UNIVERSIDAD DE COSTA RICA

FACULTAD DE CIENCIAS ECONÓMICAS

Escuela de Administración de Negocios

Trabajo final de graduación para optar por el grado de Licenciatura en Contaduría Pública

Propuesta de fortalecimiento de control interno para el Comité Cantonal de Deportes y Recreación de Alajuela (CODEA) basado en COSO, integrando COBIT 5 para el componente de Información y Comunicación

Daniela María Arrieta Arrieta

Marilyn María Castro Quesada

Jesús Alberto Murillo Vargas

Yerlin María Navarro Brenes

Ciudad Universitaria Rodrigo Facio

San Pedro de Montes de Oca

2022

UNIVERSIDAD DE COSTA RICA
FACULTAD DE CIENCIAS ECONÓMICAS

Acta # 07-2022

Acta de la Sesión 07-2022 del Comité Evaluador de la Escuela de Administración de Negocios, celebrada el 28 de junio de 2022, por medio de la Plataforma Zoom, con el fin de proceder a la Exposición del Trabajo Final de Graduación de **Daniela María Arrieta Arrieta, carné B50689, Marilyn María Castro Quesada, carné B41634, Jesús Alberto Murillo Vargas, carné B44858 y Yerlin María Navarro Brenes, carné B44893,** quienes optaron por la modalidad de Seminario de Graduación.

Presentes: Carlos Castro Umaña, quien presidió; Rony Yusnel Cordero Vargas, Tutor; Juan José Castro Palma, Lector; Felipe Antonio Bonilla Agüero, Representante del Sector Docente de la Escuela de Administración de Negocios, quien actuó como Secretario de la Sesión.

Artículo 1

El Presidente informa que los expedientes de las personas postulantes, contienen todos los documentos que el Reglamento exige. Declara que han cumplido con los requisitos del Programa de la Carrera de Licenciatura en Contaduría Pública.

Artículo 2

Hicieron la exposición del Trabajo Final: ***Propuesta de fortalecimiento de control interno para el Comité Cantonal de Deportes y Recreación de Alajuela (CODEA) basado en COSO, integrando COBIT 5 para el componente de Información y Comunicación.***

Artículo 3

Terminada la disertación, los miembros del Comité Evaluador, interrogaron a quienes expusieron, en el tiempo reglamentario. Las respuestas fueron satisfactorias, en opinión del Comité.

Artículo 4

Concluido el interrogatorio, el Tribunal procedió a deliberar

Artículo 5

Efectuada la votación, el Comité Evaluador consideró el Trabajo Final de Graduación Satisfactorio, y lo declaró Aprobado.

Artículo 6

El Presidente del Comité Evaluador comunicó en público el resultado de la deliberación y les declaró: *Licenciadas en Contaduría Pública.*

Se les indicó la obligación de realizar las gestiones para el Acto de Juramentación más próximo. Luego se dio lectura al acta que firmaron los miembros del Comité y el grupo de estudiantes.

CARLOS ENRIQUE CASTRO UMAÑA (FIRMA)
Firmado digitalmente por CARLOS ENRIQUE CASTRO UMAÑA (FIRMA)
Fecha: 2022.06.30 11:44:49 -06'00'

Carlos Castro Umaña
Representante Director, Escuela Administración de Negocios

DANIELA MARIA ARRIETA ARRIETA (FIRMA)
Firmado digitalmente por DANIELA MARIA ARRIETA ARRIETA (FIRMA)
Fecha: 2022.07.01 07:56:42 -06'00'

Daniela María Arrieta Arrieta
Carné B50689

RONY YUSNEL CORDERO VARGAS (FIRMA)
Firmado digitalmente por RONY YUSNEL CORDERO VARGAS (FIRMA)
Fecha: 2022.06.30 12:07:01 -06'00'

Rony Yusnel Cordero Vargas
Tutor

MARILYN MARIA CASTRO QUESADA (FIRMA)
Firmado digitalmente por MARILYN MARIA CASTRO QUESADA (FIRMA)
Fecha: 2022.06.30 21:42:11 -06'00'

Marilyn María Castro Quesada
Carné B41634

JUAN JOSE CASTRO PALMA (FIRMA)
Firmado digitalmente por JUAN JOSE CASTRO PALMA (FIRMA)
Fecha: 2022.06.30 13:22:21 -06'00'

Juan José Castro Palma
Lector

JESUS ALBERTO MURILLO VARGAS (FIRMA)
Firmado digitalmente por JESUS ALBERTO MURILLO VARGAS (FIRMA)
Fecha: 2022.07.01 08:22:03 -06'00'

Jesús Alberto Murillo Vargas
Carné B44858

YERLIN MARIA NAVARRO BRENES (FIRMA)
Firmado digitalmente por YERLIN MARIA NAVARRO BRENES (FIRMA)
Fecha: 2022.07.01 08:14:28 -06'00'

Yerlin María Navarro Brenes
Carné B44893

Sigifredo Garro Contreras
Lector

FELIPE ANTONIO BONILLA AGUERO (FIRMA)
Firmado digitalmente por FELIPE ANTONIO BONILLA AGUERO (FIRMA)
Fecha: 2022.07.01 22:13:18 -06'00'

Felipe Antonio Bonilla Agüero
Secretario

Según lo establecido en el Reglamento de Trabajos Finales de Graduación, artículo 39 "... En caso de trabajos sobresalientes; si así lo acuerdan por lo menos cuatro de los cinco miembros del Comité, se podrá conceder una aprobación con distinción".

(X) Se aprueba con Distinción

Observaciones: _____

FJHS

El presente documento es la versión final, ha sido aprobado y revisado por el tutor del trabajo.

RONY YUSNEL CORDERO VARGAS (FIRMA)

Firmado digitalmente por RONY YUSNEL CORDERO VARGAS (FIRMA)
Fecha: 2022.07.08 20:45:41 -06'00'

MBA. Rony Yusnel Cordero Vargas

2. Derechos de Propiedad Intelectual

3. Agradecimientos

A Dios por brindarnos discernimiento espiritual y fortaleza para culminar este proceso.

Al Comité Cantonal de Deportes y Recreación de Alajuela (CODEA) por su amplia colaboración y disposición en ayudarnos.

Al profesor coordinador y a los profesores tutores por su guía y apoyo.

Al equipo de trabajo por su persistencia, disciplina y esfuerzo demostrado.

Y a todas las personas que nos ofrecieron sus consejos y sabiduría en las distintas etapas que se requirieron para completar este proceso.

4. Dedicatoria

A mi familia por su apoyo y confianza; mi madre por mantenerme siempre presente en sus oraciones, mi padre por mostrarme los caminos que debo evitar, a mis hermanos: Cristian por el cariño y amor que siempre me brindó, Yeison por su ejemplo y su mano que nunca dejó de ayudarme, Richer por demostrarme que con esfuerzo y valentía se pueden conseguir grandes cosas, Emileny y a Liseth por la motivación y consejos que siempre me han brindado, a mis sobrinos: Evans, Kenneth, Naihara y Dereck porque con su sola existencia me llenan de alegría.

Así como a Mario por su amor, paciencia y cariño que me han ayudado a crecer en esta etapa de mi vida.

Finalmente, a Saki porque su presencia siempre me brinda paz.

Daniela Arrieta Arrieta

Dedico este trabajo a mi madre por sus palabras de aliento y oraciones, a mi padre por su amor y confianza, a mi hermana Tifany por su cariño, apoyo incondicional y consejos, a Maikol por su motivación, paciencia, comprensión, apoyó en mis decisiones y amor.

Y finalmente, a mi bisabuelo Antonio y a Paulina, ya que, sin ellos en mi vida, no sería la persona que soy y la que busco ser.

Marilyn Castro Quesada

A Dios por guiar mis pasos y por darme fortaleza en todo momento.

A mi madre Ruth Mary que desde el cielo me ilumina para avanzar con mis proyectos, por sus consejos y resilencia que me enseñó, por su amor incalculable y sus palabras que guardo en mi corazón. A ti te debo lo que soy.

A mi padre Orlando, y mis hermanos María Paula y Jeffry por su apoyo en los momentos difíciles, por sus palabras de aliento, y por la compañía incondicional.

Finalmente, a mi primo Ronny por ser un ejemplo de lucha y perseverancia para alcanzar los objetivos.

Jesús Murillo Vargas

Primeramente, a Dios quien ha sido mi guía, fortaleza y me ha acompañado en todos mis pasos hasta el día de hoy. A mi madre quien con amor, paciencia y esfuerzo me ha forjado e instado a cumplir cada uno de mis sueños y con este uno más, gracias por inculcar en mí el ejemplo de esfuerzo y valentía, de siempre ir más allá. A todas mis hermanas porque con sus oraciones, consejos y palabras de aliento hicieron de mí una mejor persona y de una u otra forma me acompañan en todos mis sueños, metas y proyectos. Finalmente quiero dedicar esta tesis a Juan Carlos por apoyarme cuando más lo necesito, por impulsarme a lograr todo aquello que me proponga, por extender su mano en momentos difíciles y por el amor brindado cada día.

Yerlin Navarro Brenes

5. Índice general

Contenido

6. Índice de figuras

7. Índice de tablas

Lista de siglas y abreviaturas

APO: *Align, Plan and Organise* (Alinear, Planificar y Supervisar)

ASF: Auditoría Superior de la Federación

AI: *Acquire and implement* (Adquirir e Implementar)

BAI: *Build, Acquire and Implement* (Construir, Adquirir e Implementar)

BMIS: Model for Information Security Information Security

CCDR: Comités Cantonales de Deportes y Recreación

CGR: Contraloría General de la República

CODEA: Comité Cantonal de Deportes y Recreación de Alajuela

COSO: Committee of Sponsoring Organizations of the Tradeway Commission (en inglés)

COBIT: Control Objetives for Information and Related Technology

DS: *Deliver and Support* (Entregar y Dar Soporte)

DSS: *Deliver, Service and Support* (Entrega, Servicio y Soporte)

EDM: *Evaluate, Direct ,Monitor* (Evaluar, Orientar y Supervisar)

ERP: Enterprise Resource Planning

ICODER: Instituto Costarricense del Deporte y la Recreación

INTOSAI: Organización Internacional de Entidades Fiscalizadoras Superiores

ITGI: IT Governance Institute

ITAF: IT Assurance Framework

ISACA: Information Systems Audit and Control Association

ME: *Monitor and Evaluate* (Monitorear y Evaluar)

MEA: *Monitor, Evaluate and Assess* (Supervisar, Evaluar y Valorar)

MEP: Ministerio de Educación Pública

NICSP: Normas de Contabilidad del Sector Público

NIIF: Normas Internacionales de Información Financiera

PAO: Plan Anual Operativo

PGR: Procuraduría General de la República

PO: *Plan and Organize* (Planear y Organizar)

SIPP: Sistema de Información sobre Planes y Presupuestos

SICOP: Sistema Integrado de Compras Públicas

SEVRI: Sistema Específico de Valoración de Riesgo

TI: Tecnología de Información

UCR: Universidad de Costa Rica

Resumen ejecutivo

El presente documento corresponde a la memoria del trabajo final de graduación, realizado bajo la modalidad de seminario de graduación, en el Comité Cantonal de Deportes y Recreación de Alajuela (CODEA) durante el año 2021 y hasta junio de 2022. El cual consiste en una Propuesta de fortalecimiento de control interno para el Comité Cantonal de Deportes y Recreación de Alajuela (CODEA) basado en COSO, integrando COBIT 5 para el componente de Información y Comunicación.

Para la elaboración de la propuesta, en primer lugar, se realizó un diagnóstico del control interno del CODEA, tomando como referencia los marcos de buenas prácticas COSO 2013 y COBIT 5, para lo cual se realizó una revisión exhaustiva de ambos marcos, una homologación de los principios de COSO 2013 y las prácticas de gestión de COBIT 5, así como revisión de información complementaria. Dicha fase también incluyó la realización de entrevistas a funcionarios clave, estructuradas de acuerdo con los cinco componentes de control interno para la identificación de las principales deficiencias y determinar sus niveles de desarrollo. Finalmente se analizaron los resultados y se contrastó con el marco de referencia. Con lo anterior, se identificaron las oportunidades de mejora para la organización.

Posterior a obtener los resultados, se diseñó la propuesta de fortalecimiento de control interno para el componente con menor nivel de desarrollo, el cual corresponde a Evaluación de Riesgos la propuesta se compone de una herramienta automatizada en la web llamada “Sistema de Gestión de Valoración de Riesgos Transitoria (SGVRT)” para la gestión de riesgos con sus diversas fases; identificación, análisis, respuesta y comunicación de resultados. Aunado a lo anterior, se documentó una metodología que corresponde a la guía paso a paso para la ejecución del proceso de gestión que el CODEA deberá, como recomendación, ejecutar mínimo una vez al año.

Introducción

Actualmente, en Costa Rica existen diferentes instituciones con miras a satisfacer intereses colectivos de la ciudadanía. Dentro de este contexto, se encuentra el Comité Cantonal de Deportes y Recreación de Alajuela (CODEA), cuya finalidad es el desarrollo y habilitación de espacios para la práctica de actividades deportivas en el cantón de Alajuela. El CODEA se creó gracias a la definición de "comités cantonales" que establece el Código Municipal, Ley N.°7794. En este mismo código se establecen las funciones que deben desempeñar estas instituciones y el origen de los recursos que tendrán a cargo para el logro de sus objetivos.

Sobre este último punto, el código establece que la principal fuente de financiamiento de los comités cantonales serán las transferencias de recursos por parte de la municipalidad correspondiente. Además, cada comité tiene la opción de administrar recursos provenientes de otras fuentes, como transferencias del Instituto Costarricense del Deporte y Recreación (ICODER) y la administración de recursos o ingresos propios.

Cabe resaltar que los comités cantonales tienen a cargo la administración y ejecución de recursos públicos, los cuales están sujetos a rendición de cuentas tanto a la ciudadanía como a diferentes órganos fiscalizadores. Por ende, con el fin de obtener una mayor transparencia y calidad de los procesos en la práctica, se debe contar con un sistema de control interno efectivo, que permita que los procesos se ejecuten con eficiencia y eficacia y que faciliten una adecuada gestión de los riesgos institucionales.

Sin embargo, el funcionamiento del CODEA presenta varios puntos de mejora relacionados al control interno. Según lo indicado en el reciente informe de auditoría de la Municipalidad de Alajuela 10-2020, se indican áreas de mejora en cuanto a: a) el alineamiento entre la planificación estratégica y la regulación interna, b) los comités comunales de deportes y la rendición de cuentas, c) la concentración de funciones incompatibles con una óptima

segregación de tareas, d) las actividades de revisión y autorización, e) la delegación de funciones, f) las instalaciones del archivo, g) el Sistema Específico de Valoración de Riesgos (SEVRI) del CODEA, h) el perfeccionamiento de la reglamentación del CODEA, i) el archivo del Comité Cantonal de Deportes y Recreación del CODEA, j) el Manual de Clases de Puestos, k) las sobre actas de la Junta Directiva.

De lo anterior, se concluye que "(...) se evidencia la falta de un Sistema de Control Interno eficiente y efectivo que le permita proporcionar al Comité Cantonal de Deportes y Recreación de Alajuela un nivel de seguridad razonable en el cumplimiento de los objetivos que asevere la exactitud y veracidad en el accionar diario de la unidad" (Municipalidad de Alajuela, 2020, p.31).

Por otra parte, mediante el Informe 08-2020, la auditoría interna de la Municipalidad de Alajuela señaló debilidades en materia de tecnologías de información, indicando que "(...) el cumplimiento a la normativa, seguridad y soporte es deficiente, lo que ocasiona que el Comité se vea expuesto a pérdidas de información y recursos, daños en los equipos tecnológicos, así como posibles responsabilidades por parte de los encargados del CODEA, debido a los aparentes incumplimientos de la normativa de TI" (Municipalidad de Alajuela, 2020, p.18).

En razón de esto, se llega a la conclusión de que la formulación de una guía de control interno que tome como referencia el marco del Comité de Organizaciones Patrocinadoras de la Comisión Treadway (COSO, por sus siglas en inglés) del año 2013 y lo complemente con el marco de Objetivos de Control para las Tecnologías de la Información y Relacionadas (COBIT, por sus siglas en inglés) versión 5 y su implementación por parte del CODEA pueden fortalecer el Sistema de Control Interno de esta institución y alcanzar altas expectativas en cuanto a eficiencia y eficacia en sus procesos y resultados.

Así las cosas, este Trabajo Final de Graduación presenta la aproximación al marco teórico que aborda los fundamentos teóricos sobre el control interno en las instituciones y el marco de buenas prácticas de gestión de las tecnologías de información llamado COBIT 5. Aunado a esto, se desarrolla el marco contextual, el cual se aborda mediante una descripción de los comités cantonales de deportes y recreación en Costa Rica y una descripción general del CODEA.

Posteriormente, se encuentra el marco metodológico, en donde se justifica el paradigma, el enfoque, el tipo de investigación, las fuentes de información, la población, el instrumento de recolección y análisis de información, construcción de la propuesta y, por último, se presentan las conclusiones y recomendaciones, la bibliografía y los anexos.

Justificación

De acuerdo con la herramienta de diagnóstico denominada “Modelo de Madurez del Sistema de Control Interno” (Contraloría General de la República, s.f.), el CODEA cuenta con un control interno que puede ser catalogado como incipiente, lo cual significa que la entidad ha realizado esfuerzos aislados para el establecimiento de un control interno.

Aunado a esto, cabe señalar que según el Sistema de Información sobre Planes y Presupuestos (SIPP) de la CGR, el CODEA administra recursos de origen público de alrededor de 1300 millones de colones anuales, de los cuales un 70% corresponde a transferencias corrientes del sector público y el 30% restante a ingresos propios y financiamiento. Además, de estos recursos, un 42% son destinados al Programa Deportivo y Recreativo y un 2% al Programa de Comités Comunales, ambos programas con incidencia directa sobre la población del cantón de Alajuela.

De lo anterior se infiere la gran responsabilidad del CODEA en administrar estos recursos de forma eficiente, cumpliendo con los objetivos del comité y el ordenamiento legal vigente. Dado lo anterior, se requieren medidas necesarias que permitan garantizar el fortalecimiento del Sistema de Control Interno.

La necesidad del fortalecimiento del actual Sistema de Control Interno por parte del CODEA, ha sido señalada por la Municipalidad de Alajuela en los últimos informes de auditoría interna (Informe 08-2019 (2019) e Informe 10-2020 (2020)), en los cuales se indicaron debilidades en temas de planificación estratégica, normativa interna desactualizada, actividades de control insuficientes para la totalidad de procesos del CODEA y debilidades en los mecanismos de información.

En línea con lo anterior, en el Informe 08-2019 se señalan recomendaciones hacia CODEA para llevar a cabo esfuerzos de mejora en los controles de las plataformas y sistemas de información que utiliza, ya que su seguridad es deficiente; además, se alertó sobre incumplimientos de la normativa de TI que exponen al Comité a riesgos como pérdidas de información o recursos y daños en los equipos tecnológicos (Municipalidad de Alajuela, 2019). Cabe indicar que este informe se refiere al Sistema Integrado de Gestión Administrativa (SYGA), el cual es utilizado por el CODEA para las labores de ejecución, control y seguimiento de las tareas administrativas; sin embargo, actualmente este sistema se está mirando hacia otro denominado SAP CODEA, con el cual se llevarían a cabo las mismas funciones de forma mejorada.

Por otra parte, en el Informe 10-2020, el cual es el último realizado, también se establecen una serie de recomendaciones que exponen los puntos mencionados en el Informe 08-2019, los cuales abarcan los componentes del Control Interno y dejan en evidencia la importancia de su fortalecimiento. En este informe se recomienda al comité: a) Elaborar un diagnóstico de los requerimientos del Comité Cantonal de Deportes y Recreación de Alajuela, b) diseñar e implementar los mecanismos de control necesarios para que los comités comunales de deportes remitan oportunamente los informes de los que dispone la normativa, c) establecer claramente las actividades generales de los cargos y separar las responsabilidades asignadas en las diversas actividades que intervienen en los diferentes procesos y d) implementar en la administración del CODEA el Sistema de Valoración de Riesgos Institucional (SEVRI), de manera que se dé cumplimiento con la normativa sobre el Sistema de Control Interno (Municipalidad de Alajuela, 2020, p.34).

En relación con lo anterior y ante las deficiencias de control detectadas, tanto en el Sistema de Control Interno y específicamente en los sistemas de información, se determina que existe concordancia entre las recomendaciones establecidas en los últimos informes de auditoría interna (Informe 08-2019 y 10-2020) y el propósito de este proyecto, pues en ambos se destaca la necesidad de contar con una herramienta que permita implementar controles y proporcionar una seguridad razonable sobre la consecución de los objetivos institucionales y la salvaguarda de los recursos patrimoniales, así como una alineación con las regulaciones legales.

Es por estas razones que el presente trabajo propone el fortalecimiento del control interno en el Comité Cantonal de Deportes de Alajuela. Para ello, en primer lugar, se realizará una evaluación de las deficiencias de control interno del Comité y, posteriormente, se diseñará una propuesta de fortalecimiento de control interno basado en los marcos COSO 2013 y COBIT 5 para el gobierno y la gestión de las tecnologías de información. De esta manera, se pretende cumplir con la normativa legal vigente, específicamente con la Ley General de Control Interno N.° 8292, y contribuir con la buena gobernanza y toma de decisiones por parte de la junta directiva, la consecución de los objetivos institucionales y la salvaguarda de los recursos públicos.

Objetivo general:

Diseñar una propuesta de fortalecimiento de control interno para el Comité Cantonal de Deportes y Recreación de Alajuela (CODEA) por medio de un diagnóstico previo comparando la situación existente, contra los criterios establecidos por COSO 2013 y COBIT 5 para el componente de información y comunicación, con el fin de garantizar la eficiencia y eficacia en sus procesos, en la consecución de sus objetivos y sus metas estratégicas.

Objetivos específicos:

1. Describir la base teórica relacionada con las buenas prácticas del control interno y de las tecnologías de información.

2. Describir la historia, estructura organizativa y funcionamiento del Comité Cantonal de Deportes y Recreación de Alajuela, contextualizando el entorno en el que opera.

3. Diagnosticar la situación actual del control interno del Comité Cantonal de Deportes y Recreación de Alajuela, para identificar las deficiencias de control presentes y sus riesgos asociados, así como las acciones aplicadas por el comité.

4. Diseñar una propuesta de fortalecimiento del control interno sobre la gestión del Comité Cantonal de Deportes y Recreación de Alajuela, que garantice razonablemente la eficiencia y eficacia en sus procesos y operaciones para la consecución de sus objetivos y metas, con base en el marco COSO 2013 e integrando COBIT 5 para el componente de Información y Comunicación.

5. Elaborar conclusiones y recomendaciones, de acuerdo con los resultados obtenidos, para promover el fortalecimiento del control interno en el Comité Cantonal de Deportes y Recreación de Alajuela.

Capítulo 1

Fundamentación teórica sobre las buenas prácticas de control interno y tecnologías de información, en el contexto nacional e internacional

1.1 Fundamentos teóricos sobre el control interno

Para la elaboración y fundamentación teórica de este proyecto de investigación es esencial establecer los elementos teóricos esenciales sobre el control interno, los cuales se indican a continuación.

1.1.1 Control interno

De acuerdo con lo establecido por la Organización Internacional de Entidades Fiscalizadoras Superiores (INTOSAI, por sus siglas en inglés) (2004) el control interno se entiende como:

> Un proceso integral efectuado por la gerencia y el personal, y está diseñado para enfrentarse a los riesgos y para dar una seguridad razonable de que, en la consecución de la misión de la entidad, se alcanzarán los siguientes objetivos gerenciales:
>
> - Ejecución ordenada, ética, económica, eficiente y efectiva de las operaciones.
> - Cumplimiento de las obligaciones de responsabilidad.
> - Cumplimiento de las leyes y regulaciones aplicables.
> - Salvaguarda de los recursos para evitar pérdidas, mal uso y daño. (p.6)

Es decir, el control interno consta de una serie de acciones que dan acompañamiento de forma continua a las diferentes actividades de la entidad, esto con el fin de brindar un control integral que asegure de forma razonable la consecución de los objetivos.

1.1.2 Importancia del control interno

Un sistema de control interno tiene como propósito principal la protección de los activos de las organizaciones y evitar actividades fraudulentas o situaciones que impidan alcanzar los objetivos. El control interno brinda apoyo a la administración para que pueda ejecutar sus tareas y alcanzar el fin propuesto. Es decir, el control interno establece la forma de llegar a la meta por medio del seguimiento de pasos propuestos y acoplados por cada entidad, sin perder de vista el objetivo.

1.1.3 Características de control interno

Es importante señalar que el sistema de control interno reúne un conjunto de características que permiten comprender su objetivo en una organización. A continuación, se describen algunas de ellas.

1.1.3.1 Seguridad razonable en el control interno. González (2005) afirma que el control interno da un alto grado de aseguramiento en la obtención de los objetivos propuestos, mas no es un aseguramiento absoluto.

1.1.3.2 Costo-beneficio del control interno. Es una de las características que debe cumplir el control interno, ya que "las actividades de control deben presentar una relación satisfactoria de costo-beneficio, de manera que su contribución esperada al logro de los objetivos sea mayor que los costos requeridos para su operación" (Contraloría General de la República [CGR], 2009, p.14).

1.1.3.3 Limitaciones del control interno. Según lo establecido por la INTOSAI (2004) "el control interno no puede por sí mismo asegurar el logro de los objetivos generales definidos anteriormente" (p.13). Es decir, el control interno puede ser afectado por diversos factores en su forma de operar, por ende, es importante destacar que el control interno únicamente brinda una seguridad razonable en la consecución de los objetivos y no una seguridad absoluta.

1.1.4 Enfoques de control interno

Conforme las empresas van adquiriendo mayor experiencia en el tema de la administración, el enfoque del control interno ha ido evolucionando paralelamente, es por esto que a continuación se presentan los enfoques que se le han dado al control interno:

1.1.4.1 Enfoque tradicional. El enfoque tradicional se considera como la primera generación de control interno, el cual se basa principalmente en los controles contables y administrativos, y se considera como poco profesional, debido a la falta de especialización por parte de los encargados de los sistemas de control interno.

1.1.4.2 Enfoque contemporáneo. Según Rivas (2011), el enfoque contemporáneo se ha desarrollado en dos etapas: la segunda y tercera generación. La segunda generación añade la necesidad del cumplimiento regulatorio, principalmente en el sector público; sin embargo, carece de calidad técnica apropiada. La tercera generación amplía el alcance de control interno en la gestión de riesgos, confiabilidad de la información financiera, cumplimientos normativos y regulatorios, desarrollo del talento humano, y la protección de los recursos y el desempeño.

1.1.5 Modelos contemporáneos de control interno

A continuación, se presentan algunos de los modelos en los cuales el control interno ha sido contextualizado:

1.1.5.1 Modelo COSO (USA-1992). El modelo COSO es un marco de buenas prácticas desarrollado por el Comité de Organizaciones Patrocinadoras de la Comisión Treadway (COSO, por sus siglas en inglés), esta es una comisión voluntaria que se encarga de desarrollar las mejores prácticas en temas de fraude, gestión de riesgo empresarial y control interno.

1.1.5.2 Evolución del modelo COSO. A continuación, se describe la evolución del modelo COSO:

1.1.5.2.1 COSO I. La comisión COSO publicó en 1992 "Internal Control-Integrated Framework" donde establece la guía para el diseño de control interno, conformado por cinco componentes: 1) ambiente de control, 2) evaluación de riesgos, 3) actividades de control, 4) información y comunicación y 5) monitoreo. Estos se encuentran "alineados a las operaciones, la información financiera y el cumplimiento de normas en las unidades de negocio de la organización" (Castañeda, 2018, p.36).

1.1.5.2.2 COSO II ERM. En el año 2004, COSO publicó el Marco Integrado de Gestión Empresarial. De acuerdo con lo expuesto por Abella (2006), este se conforma de ocho componentes: a) ambiente interno, 2) establecimiento de objetivos, 3) identificación de acontecimientos, 4) evaluación de riesgos, 5) respuesta al riesgo, 6) actividades de control, 7) información, y comunicación, 8) supervisión.

1.1.5.2.3 COSO III 2013. COSO III fue publicado en el año 2013. De acuerdo con el resumen ejecutivo facilitado por COSO (2013), este marco se enfoca en considerar elementos del mercado global y en ampliar el alcance de la información financiera y no financiera, tanto interna como externa. Considera 17 principios de control interno, categorizados en cinco componentes de control interno de COSO los cuales deben operar de manera conjunta: 1) entorno de control, 2) evaluación de riesgos, 3) actividades de control, 4) información y comunicación y 5) actividades de supervisión.

1.1.5.2.4 COSO ERM 2017 (COSO IV). También conocido como COSO ERM 2017, fue publicado por COSO en el año 2017 y consiste en una actualización del Marco de Gestión Empresarial COSO 2004, el cual incluye la importancia de la administración del riesgo con respecto a las expectativas de las partes interesadas, la anticipación al riesgo por los posibles cambios del entorno y las tendencias futuras. Los componentes que lo integran son: a) gobierno y cultura, b) estrategia y establecimiento de objetivos, c) desempeño, d) evaluación y revisión, e) información, comunicación y reporte. Contempla 20 principios.

1.1.6 Componentes según COSO 2013

En este trabajo final de graduación se hará énfasis en COSO 2013. Este marco define sus componentes de la siguiente manera:

1.1.6.1 Entorno de control. De acuerdo con COSO (2013) "el entorno de control es el conjunto de normas, procesos y estructuras que constituyen la base sobre la que desarrollar el control interno de la organización" (p.4). Es decir, este componente proporciona un direccionamiento básico a las organizaciones, por lo que su calidad afecta a los restantes cuatro componentes. Es importante indicar que este componente se ve afectado por factores internos y externos como los valores, el mercado y la competencia.

El entorno de control se conforma de la integridad y valores éticos, la estructura organizacional, asignación de autoridad y responsabilidades, el compromiso con atraer y retener personal competente, la evaluación del desempeño y los incentivos (COSO, 2013). La importancia de los factores mencionados anteriormente debe ser establecida desde la junta directiva y la administración debe reforzar su relevancia hacia todos los niveles de la organización.

1.1.6.2 Evaluación de riesgos. COSO (2013) indica que "la evaluación del riesgo implica un proceso dinámico e interactivo para identificar y evaluar los riesgos de cara a la consecución de los objetivos. Dichos riesgos deben evaluarse en relación a unos niveles preestablecidos de tolerancia" (p.4). Este proceso resulta de gran relevancia para cualquier organización de cualquier índole, esto debido a que la existencia de riesgos es inevitable y estos pueden surgir tanto de fuentes externas como internas.

1.1.6.3 Actividades de control. Este componente se define como "las acciones establecidas a través de políticas y procedimientos que contribuyen a garantizar que se llevan a cabo las instrucciones de la dirección para mitigar los riesgos con impacto potencial en los objetivos" (COSO, 2013, p. 4). Estas acciones deben llevarse a cabo en toda la organización y en todos sus procesos, de manera que permita generar una seguridad razonable sobre el cumplimiento de sus objetivos.

1.1.6.4 Información y comunicación. De acuerdo con COSO (2013) la información es aquella necesaria para que una institución pueda llevar a cabo su responsabilidad de control interno y para el logro de los objetivos. Y la comunicación es un proceso continuo e iterativo de proporcionar, compartir y obtener información (p. 5). Este componente resulta de gran relevancia, ya que permite generar información que cumple con diferentes metas, por ejemplo: proveer información de apoyo a la toma de decisiones, generar información histórica, documentar procesos, entre otras. Así mismo, la comunicación oportuna también agrega valor en términos de eficiencia.

1.1.6.5 Actividades de supervisión. Debido a que el control interno es un proceso dinámico, debe de adaptarse continuamente a los riesgos y cambios a los que se enfrenta la institución, por consiguiente, es por esto que COSO (2013) indica que las actividades de supervisión son fundamentales para "determinar si cada uno de los cinco componentes del

control interno, incluidos los controles para cumplir los principios de cada componente, están presentes y funcionan adecuadamente" (p.5).

1.1.7 Principios y puntos de enfoque según componentes del COSO 2013

A continuación, se describen los diecisiete principios asociados a los cinco componentes de control interno, según lo propone COSO 2013 Marco Integrado.

Principio 1.1: La organización demuestra compromiso con la integridad y los valores éticos. Hace referencia al compromiso que tiene la entidad con el establecimiento de las normas de conducta, adhesión a las mismas y seguimiento de las desviaciones, como base para un control interno adecuado. La línea de referencia de este principio consiste en que la integridad y los valores éticos de las personas que participan en el control interno son la base para su adecuación, además de ser esenciales para que funcionen los demás componentes (COSO, 2013).

Principio 1.2: El consejo de administración demuestra independencia de la dirección y ejerce la supervisión del desempeño del sistema de control interno. Hace referencia a la supervisión e independencia, las cuales son responsabilidad de la alta dirección. Ante ello, COSO 2013 establece los puntos de enfoque relevantes para este principio, y se centra en el establecimiento de la responsabilidad de supervisión, la experiencia relevante, las funciones de independencia y la supervisión del control interno. La supervisión de la que se habla en este componente debe ser apoyada por las estructuras y procesos señalados en los niveles de ejecución del negocio, es decir, la persona que funge como directora ejecutiva y la alta dirección son responsables del desarrollo e implementación del sistema de control interno (COSO, 2013).

Principio 1.3 La dirección se establece con la supervisión del consejo, las estructuras, las líneas de reporte y los niveles de autoridad y responsabilidad apropiados para la consecución de los objetivos. Alude a aspectos dentro de la organización que fortalecen el control interno a nivel de estructura, detallado en los puntos de enfoque COSO 2013, En este documento se afirma que se deben considerar las estructuras de la entidad y el establecimiento de las líneas de reporte; así como definir, asignar y delimitar las autoridades y responsabilidades. Cabe señalar en este punto que la administración tiene la responsabilidad de diseñar, revisar y evaluar las líneas de reporte, de manera que la información fluya, haya transparencia y se logren los objetivos y metas por las cuales se propusieron (COSO, 2013).

Principio 1.4 La organización demuestra compromiso para atraer, desarrollar y retener a profesionales competentes, en concordancia con los objetivos de la organización. El cuarto principio se enfoca en el capital humano, parte relevante del control interno, ya que son quienes realizan las actividades de control de la entidad. Dado que el personal es parte fundamental de la organización, COSO 2013 establece puntos de enfoque que ayudan a valorar la adecuación de este aspecto, como lo son el establecimiento de prácticas y políticas, la evaluación de las competencias y la corrección de las deficiencias, atracción y desarrollo del personal idóneo, así como la preparación adecuada para sucesión (COSO, 2013).

Principio 1.5 La organización define las responsabilidades de las personas a nivel de control interno para la consecución de los objetivos. Se enfoca en la consecución de los objetivos, por lo que la administración se centra en disponer de personas capaces y hacerlas responsables para cumplir con las responsabilidades y obligaciones de control interno. En este principio se evalúa el desempeño, recompensas y disciplina de los individuos (COSO, 2013).

Principio 2.1 La organización define los objetivos con suficiente claridad para permitir la identificación y evaluación de los riesgos relacionados. Se refiere al proceso de formular un plan estratégico ordenado y coherente, con todos los esfuerzos para lograr la consecución de los objetivos (operacionales, financieros, internos, externos) con el fin de identificar y evaluar de mejor manera los riesgos que se presenten (COSO, 2013).

Principio 2.2 La organización identifica los riesgos para la consecución de sus objetivos en todos los niveles de la entidad y los analiza como base sobre la cual determina cómo se deben gestionar. Busca identificar los riesgos para analizar y determinar la respuesta a los mismos. Se deben analizar tanto los factores internos como los externos (COSO, 2013).

Principio 2.3 La organización considera la probabilidad de fraude al evaluar los riesgos para la consecución de los objetivos. Para este principio, la administración debe considerar la posibilidad de que ocurra cualquier tipo de fraude o acto de corrupción que pueda afectar la consecución de los objetivos. El principal objetivo de esta acción es que se identifique y analice la mejor manera de enfrentar estas situaciones (COSO, 2013).

Principio 2.4 La organización identifica y evalúa los cambios que podrían afectar significativamente al sistema de control interno. Establece la necesidad de la empresa de evaluar los diferentes cambios tanto a lo interno como a lo externo de la organización, que podrían generar algún impacto en el negocio en marcha. Algunos de los cambios a considerar que se establecen mediante los puntos de enfoque son: cambios en el entorno externo, en el modelo regulatorio, en el modelo comercial y en el liderazgo (COSO, 2013).

Principio 3.1 La organización define y desarrolla actividades de control que contribuyen a la mitigación de los riesgos hasta niveles aceptables para la consecución de los objetivos. Consiste en establecer una serie de actividades de control alineadas con el

entorno, la complejidad, naturaleza y alcance de las operaciones de la entidad. Para poder determinarlas, se debe esclarecer cuáles son los procesos de negocio relevantes de la entidad, de esta forma se obtiene un panorama general que permite identificar qué tipo de actividad debe aplicarse y la manera en que debe ser aplicada (COSO, 2013).

Principio 3.2 La organización define y desarrolla actividades de control a nivel de entidad sobre la tecnología para apoyar la consecución de los objetivos. En la actualidad, la tecnología es aprovechada por muchas organizaciones para la automatización de las actividades de control, es por esto que se debe determinar cuál es la relación existente entre los procesos de negocio y los controles automatizados. En este mismo orden de ideas, surge la necesidad de generar actividades de control de infraestructura tecnológica que garanticen la efectividad de los controles establecidos, así como controles de seguridad que permitan la continuidad de los diferentes procesos. Por último, este principio establece la importancia de generar actividades de control sobre los procesos de adquisición, desarrollo y mantenimiento de TI (COSO, 2013).

Principio 3.3 La organización despliega las actividades de control a través de políticas que establecen las líneas generales del control interno y procedimientos. Para llevar a cabo las actividades de control, COSO 2013 establece que la organización debe establecer políticas y procedimientos que respalden su implementación, así mismo se deben establecer responsabilidades y procesos de rendición de cuentas, tomar acciones correctivas, asignar personal competente para estas actividades y revisar periódicamente las actividades de control con el fin de determinar si deben ser actualizadas o no (COSO, 2013).

Principio 4.1 La organización obtiene o genera y utiliza información relevante y de calidad para apoyar el funcionamiento del control interno. Hace referencia a la forma en que la información permite el funcionamiento de los componentes de control. En primera instancia, COSO 2013 establece que se deben definir los requisitos de información que permitan identificar las fuentes de información internas y externas que sean relevantes, confiables e íntegras. Los sistemas de información son parte fundamental de la información, ya que permiten obtener, capturar y procesar datos de las fuentes internas y externas (COSO, 2013).

Principio 4.2 La organización comunica la información internamente, incluidos los objetivos y responsabilidades que son necesarios para apoyar el funcionamiento del sistema de control interno. Se enfoca en cómo la organización define e implementa políticas y procedimientos para lograr una comunicación interna eficaz, pues la información debe fluir en toda la organización por medio de diferentes canales. También se deben considerar los métodos de comunicación para la comprensión del mensaje para los destinatarios. En la información comunicada internamente entre la junta directiva, la administración y el personal debe destacar la importancia, la relevancia y los beneficios del control interno, así como los roles y responsabilidades para el diseño y la ejecución adecuada de los controles (COSO, 2013).

Principio 4.3 La organización se comunica con los grupos de interés externos sobre los aspectos clave que afectan al funcionamiento del control interno. La información también fluye desde las fuentes externas. Es decir que la organización define e implementa políticas y procedimientos para promover una comunicación externa eficaz con el fin de obtener y recibir información de las diversas partes interesadas de la entidad, por lo que se debe desarrollar e implementar controles para facilitar la comunicación externa, que faciliten la

comprensión de las circunstancias que puedan afectar el funcionamiento de la entidad o el cumplimiento de los objetivos (COSO, 2013).

Principio 5.1 La organización selecciona, desarrolla y realiza evaluaciones continuas y/o independientes para determinar si los componentes del sistema están presentes y funcionando. El seguimiento se puede realizar mediante evaluaciones continuas, evaluaciones independientes o una combinación de ambas, con el fin de determinar si los cinco componentes de control están presentes y funcionando. Permiten comprender cómo la administración ha diseñado e implementado el sistema de control interno (COSO, 2013).

Principio 5.2 La organización evalúa y comunica las deficiencias de control interno de forma oportuna a las partes responsables de aplicar medidas correctivas, incluyendo la alta dirección y el consejo, según corresponda. Las actividades de supervisión permiten identificar asuntos que requieran de atención, como deficiencias potenciales o reales en relación con el control interno, que puedan impedir el cumplimiento de objetivos. Las deficiencias de control identificadas se deben comunicar a la junta directiva, administración o reportarse a entidades reguladoras o de supervisión si existe normativa legal que así lo requiera. En otras palabras, las deficiencias de control deben informarse a las partes responsables para tomar acciones correctivas (COSO, 2013).

A continuación, se presenta una tabla resumen con los cinco componentes del control interno con sus diecisiete principios asociados según lo propone COSO 2013 Marco Integrado:

Tabla 1: *Principios y puntos de enfoque de control interno según componentes, COSO 2013*

Componente	*Principios*	*Punto de enfoque*
1. Entorno de control	1.1 La organización demuestra compromiso con la integridad y los valores éticos.	1.1.1 Establece el tono en la cima
		1.1.2 Establece normas de conducta
		1.1.3 Evalúa la adhesión a normas de conducta
		1.1.4 Aborda desviaciones de manera oportuna
	1.2 El consejo de administración demuestra independencia de la dirección y ejerce la supervisión del desempeño del sistema de control interno.	1.2.1 Establece responsabilidades de supervisión
		1.2.2 Aplica la experiencia relevante
		1.2.3 Funciona de forma independiente
		1.2.4 Supervisa el sistema de control interno
	1.3 La dirección establece con la supervisión del Consejo, las estructuras, líneas de reporte y los niveles de	1.3.1 Considera todas las estructuras de la entidad

	autoridad y responsabilidad apropiados para la consecución de los objetivos.	1.3.2 Establece líneas de reporte
		1.3.3 Define, asigna y limita autoridades y responsabilidades
	1.4 La organización demuestra compromiso para atraer, desarrollar y retener a profesionales competentes, en concordancia con los objetivos de la organización.	1.4.1 Establece políticas y prácticas
		1.4.2 Evalúa las competencias y corrige las deficiencias
		1.4.3 Atrae, desarrolla y retiene individuos
		1.4.4 Planifica y se prepara para la sucesión
	1.5 La organización define las responsabilidades de las personas a nivel de control interno para la consecución de los objetivos.	1.5.1 Hace cumplir la rendición de cuentas mediante estructuras, autoridad y responsabilidad
		1.5.2 Establece medidas de desempeño, incentivos y recompensas
		1.5.3 Evalúa las medidas de desempeño, incentivos y recompensas para relevancia continua

		1.5.4 Considera presiones excesivas
		1.5.5 Evalúa el desempeño y recompensa o disciplina a los individuos
2. Evaluación de riesgos	2.1 La organización define los objetivos con suficiente claridad para permitir la identificación y evaluación de los riesgos relacionados.	2.1.1 Objetivos operacionales
		2.1.2 Objetivos de reporte financiero externo
		2.1.3 Objetivos de reporte no financiero externo
		2.1.4 Objetivos de reporte interno
		2.1.5 Objetivos de cumplimiento
	2.2 La organización identifica los riesgos para la consecución de sus objetivos en todos los niveles de la entidad y los analiza como base sobre la cual determina cómo se deben gestionar.	2.2.1 Incluye entidad, subsidiaria, división, unidad operativa y niveles funcionales
		2.2.2 Analiza los factores internos y externos
		2.2.3 Involucra a niveles adecuados de la administración

		2.2.4 Estima la importancia de los riesgos identificados
		2.2.5 Determina cómo responder a los riesgos
	2.3 La organización considera la probabilidad de fraude al evaluar los riesgos para la consecución de los objetivos.	2.3.1 Considera varios tipos de fraude
		2.3.2 Evalúa incentivos y presiones
		2.3.3 Evalúa oportunidades
		2.3.4 Evalúa las actitudes y las racionalizaciones
	2.4 La organización identifica y evalúa los cambios que podrían afectar significativamente al sistema de control interno.	2.4.1 Evalúa los cambios en el entorno externo
		2.4.2 Evalúa los cambios en el modelo de negocio
		2.4.3 Evalúa los cambios en el liderazgo
3. Actividades de control	3.1 La organización define y desarrolla actividades de control que contribuyen a la mitigación de los riesgos hasta niveles aceptables para la consecución de los objetivos.	3.1.1 Integración con la evaluación de riesgos
		3.1.2 Considera los factores específicos de la entidad

		3.1.3 Determina los procesos empresariales relevantes
		3.1.4 Evalúa una mezcla de tipos de actividades de control
		3.1.5 Considera en qué nivel se aplican las actividades
		3.1.6 Toma en cuenta la segregación de funciones
	3.2 La organización define y desarrolla actividades de control a nivel de entidad sobre la tecnología para apoyar la consecución de los objetivos.	3.2.1 Determina la dependencia entre el uso de TI en los procesos del negocio y los controles generales de TI
		3.2.2 Se establecen actividades de control relevantes a la infraestructura de TI
		3.2.3 Se establecen actividades de control relevantes para el proceso de gestión de seguridad
		3.2.4 Se establecen actividades de control relevantes para los procesos de adquisición, desarrollo y mantenimiento de TI

	3.3 La organización despliega las actividades de control a través de políticas que establecen las líneas generales del control interno y procedimientos.	3.3.1 Se establecen políticas y procedimientos para permitir la implementación de las directrices de la administración
		3.3.2 Establece la responsabilidad y rendición de cuentas por la ejecución de las políticas y los procedimientos
		3.3.3 Se realiza de forma oportuna
		3.3.4 Se toma acción correctiva
		3.3.5 Se lleva a cabo usando personal competente
		3.3.6 Se evalúan las políticas y los procedimientos
4. Información y comunicación	4.1 La organización obtiene o genera y utiliza información relevante y de calidad para apoyar el funcionamiento del control interno.	4.1.1 Identifica los requisitos de la información
		4.1.2 Captura fuentes internas y externas de datos
		4.1.3 Transforma datos relevantes en información
		4.1.4 Mantiene la calidad a lo largo del procesamiento

		4.1.5 Considera los costos y los beneficios
	4.2 La organización comunica la información internamente, incluidos los objetivos y responsabilidades que son necesarios para apoyar el funcionamiento del sistema de control interno.	4.2.1 Se comunica información de control interno
		4.2.2 La administración se comunica con el consejo directivo
		4.2.3 Proporciona líneas de comunicación independientes
		4.2.4 Selecciona métodos relevantes de comunicación
	4.3 La organización se comunica con los grupos de interés externos sobre los aspectos clave que afectan al funcionamiento del control interno.	4.3.1 Se comunica a partes externas
		4.3.2 Permite comunicaciones entrantes
		4.3.3 Se comunica con el consejo directivo
		4.3.4 Proporciona líneas de comunicación independientes
		4.3.5 Selecciona métodos relevantes de comunicación

5. Actividades de supervisión	5.1 La organización selecciona, desarrolla y realiza evaluaciones continuas y/o independientes para determinar si los componentes del sistema están presentes y funcionando.	5.1.1 Considera una mezcla de evaluaciones permanentes y separadas
		5.1.2 Considera la velocidad del cambio
		5.1.3 Establece una comprensión básica
		5.1.4 Utiliza personal experto
		5.1.5 Se integra con los procesos del negocio
		5.1.6 Se ajusta el alcance y la frecuencia
		5.1.7 Se evalúa objetivamente
	5.2 La organización evalúa y comunica las deficiencias de control interno de forma oportuna a las partes responsables de aplicar medidas correctivas, incluyendo la alta dirección y el consejo, según corresponda.	5.2.1 Evalúa los resultados
		5.2.2 Comunica las deficiencias
		5.2.3 Monitorea las acciones correctivas

Fuente: Elaboración propia basado en *COSO 2013.*

1.1.8 Control interno según la Ley General de Control Interno N° 8292

La ley busca establecer los criterios mínimos de control interno, que deben implementar las diferentes instituciones en Costa Rica. Esta ley contempla una serie de elementos con el fin de apoyar la gestión de las organizaciones; entre ellos se encuentran: el ambiente de control, la evaluación del riesgo, los sistemas de información, las actividades de control y el seguimiento, los cuales se detallaron en el apartado sobre COSO III. En los apartados siguientes se describen otros aspectos que contempla la ley.

1.1.8.1 Obligatoriedad de establecimiento de control interno. Según lo establece la Ley General de Control Interno N° 8292 de 2002 en el artículo 7: "Los entes y órganos sujetos a esta Ley dispondrán de sistemas de control interno, los cuales deberán ser aplicables, completos, razonables, integrados y congruentes con sus competencias y atribuciones institucionales" (p. 5).

Cabe indicar que, la Ley Orgánica de la Contraloría General de la República N° 7428 de 1994 en su artículo 4 menciona que los sujetos privados, que sean administradores, por cualquier título, de los fondos y actividades públicos, deben de acatar la normativa técnica aplicable en relación con el control interno que emita la Contraloría General de Costa Rica, por lo que el incumplimiento es causal de responsabilidad administrativa.

Así mismo, la Ley General de Control Interno N° 8292 de 2002 señala que la jerarca o las personas titulares subordinadas deben cumplir con medidas correctivas ante desviaciones e irregularidades, implementar recomendaciones de órganos de fiscalización y velar que el sistema de control interno sea razonable y congruente con sus competencias y atribuciones institucionales.

1.1.8.2 Componentes orgánicos del control interno. Se establecen dos componentes orgánicos dentro del control interno, que consisten en la definición de dos grupos de la administración, los cuales se encuentran inmersos en sus procesos. Seguidamente, se puntualizan estos componentes:

1.1.8.2.1 Administración activa. La Ley General de Control Interno N° 8292 de 2002 en el artículo N° 2, define la administración activa desde dos puntos:

Desde el punto de vista funcional como la función decisoria, ejecutiva, resolutoria, directiva u operativa de la Administración y desde el punto de vista orgánico como el conjunto de órganos y entes de la función administrativa, que deciden y ejecutan; incluyen al jerarca, como última instancia (p. 3).

1.1.8.2.2 Auditoría interna. La auditoría interna busca garantizar una seguridad razonable sobre la actuación de los funcionarios y que esta sea acorde con el marco legal, las mejores prácticas y los criterios técnicos, según lo expresa la Ley General de Control Interno N° 8292 de 2002 en el artículo N° 21:

La auditoría interna es la actividad independiente, objetiva y asesora, que proporciona seguridad al ente u órgano, puesto que se crea para validar y mejorar sus operaciones. Contribuye a que se alcancen los objetivos institucionales, mediante la práctica de un enfoque sistémico y profesional para evaluar y mejorar la efectividad de la administración del riesgo, del control y de los procesos de dirección en las entidades y los órganos sujetos a esta Ley. (p.13)

1.1.8.3 Componentes funcionales del control interno. La Ley General de Control Interno N° 8292 de 2002 en el capítulo III, establece cinco componentes funcionales para el funcionamiento de control interno, los cuales son: ambiente de control, valoración de riesgo, actividades de control, sistemas de información, y seguimiento del sistema de control interno.

1.1.8.4 Autoevaluación de control interno. La autoevaluación del control interno será un deber de la administración activa, este debe realizarse al menos una vez al año para identificar desvíos de la organización para el cumplimiento de los objetivos y para la mejora continua (Ley General de Control Interno N° 8292, 2002).

Esta autoevaluación permite a las entidades determinar la razonabilidad de los procesos de gestión y riesgos de su institución. Para llevar a cabo esta autoevaluación, la CGR establece las Directrices Generales para el Establecimiento y Funcionamiento del Sistema Específico de Evaluación de Riesgo Institucional (SEVRI). De acuerdo con estas directrices, el objetivo del SEVRI es "producir información que apoye la toma de decisiones orientada a ubicar a la institución en un nivel de riesgo aceptable y así promover, de manera razonable, el logro de los objetivos institucionales" (CGR, 2006, p.10).

Por ende, cada institución deberá establecer una metodología basada en SEVRI que permita identificar el nivel de riesgo de cada uno de sus procedimientos y, asimismo, identificar oportunidades de mejora y fortalecer la toma de decisiones, con el fin de que se alcance una seguridad razonable del cumplimiento de sus objetivos.

1.1.9 Modelo de madurez de control interno según Contraloría General de la República

El control interno es un mecanismo estratégico para el cumplimiento de los objetivos institucionales, por lo que conocer su nivel de funcionamiento en la organización es importante. El modelo de madurez de control interno es una herramienta que permite comprender e

identificar el estado actual de esta variable, por lo que tiene una función de diagnóstico debido a que la administración identifica las debilidades en esta área; al mismo tiempo, es el insumo que permite establecer acciones correctivas, y con ello fortalecerla. Además, facilita el seguimiento del grado de avance de la institución a lo largo del tiempo y con ello la mejora continua del sistema.

El modelo permite determinar el grado de compromiso de la administración y de los demás niveles de la organización, el nivel de funcionamiento y las medidas a seguir para la mejora continua del control interno. Con base en lo anterior, permite detectar cinco posibles estados de madurez del control interno, los cuales pueden ser: incipiente, novato, competente, diestro y experto.

Figura1: *Niveles del modelo de madurez de control interno*

Fuente: Elaboración propia adaptado de *Modelo de Madurez de Control Interno, Contraloría General de la República*.

1.2 Buenas prácticas de control y supervisión de las tecnologías de información: marco COBIT

En el siguiente apartado, se abordarán aspectos relacionados con el marco COBIT, entre los cuales destacan la definición y elementos teóricos fundamentales, que se abordarán a continuación.

1.2.1 Definición conceptual del marco COBIT

COBIT corresponde al acrónimo de "Objetivos de control para tecnologías de la información y relacionadas" (Control Objectives for Information and Related Technology, en inglés). Este un modelo para el buen gobierno y la gestión de las tecnologías de información y la tecnología de la empresa, el cual está basado en cinco principios claves para el gobierno y la gestión. De acuerdo con COBIT 5 Implementación, estos principios son: 1) satisfacer las necesidades de las partes interesadas, 2) cubrir a la empresa de extremo a extremo, 3) aplicar un marco de referencia único integrado, 4) hacer posible un enfoque holístico y 5) separar el gobierno de la gestión (Information Systems Audit and Control Association [ISACA], 2012b).

Asimismo, COBIT 5 se define como:

> ". . . un marco de referencia de Gobierno de TI y un conjunto de herramientas de soporte que permite a los gerentes reducir la brecha entre los requerimientos de control, los temas técnicos y los riesgos del negocio. Además, permite el desarrollo de una política clara y una buena práctica para el control de TI en las organizaciones" (Saavedra & Torres, 2012, p.25).

Es por esto que se seleccionó COBIT 5 como el marco idóneo para reforzar las respuestas que se vayan a dar a las necesidades del Comité Cantonal de Deportes y Recreación de Alajuela (CODEA). Además, ofrece la ventaja de ser un marco genérico que se adecúa a las necesidades de todas las organizaciones ya sea sector privado o público, con o sin fines de lucro, pero sobre todo de cualquier tamaño.

1.2.2 Importancia de COBIT

COBIT es un modelo que integra materia de control, auditoría, gestión y gobierno para ofrecer guías actualizadas en el aseguramiento de la gestión de TI. Es por esto que la misión que busca COBIT y, por ende, su importancia, se basa en que este modelo "contempla aspectos puntuales, como niveles de riesgo aceptables, continuidad, disponibilidad, cumplimiento legal (regulaciones) y políticas internas" (Hernández, 2018, p. 7).

Además, según Hernández (2018, p. 7) COBIT tiene ciertas ventajas y beneficios para ofrecer a la seguridad de la información, por ejemplo:

1. Disminuye la complejidad y aumenta la rentabilidad, generando un crecimiento en la satisfacción del usuario y permitiendo una mejor toma de decisiones basada en la matriz de riesgo definida.
2. Mejora la prevención, detección y recuperación de amenazas, lo que se traduce en una reducción del impacto en los incidentes de seguridad.
3. Mejora la comprensión de la información en toda la organización.
4. Proporciona orientación específica relacionada con los habilitadores.

COBIT funciona como un marco de seguridad donde las empresas pueden definir las responsabilidades y estructuras requeridas para funcionar adecuadamente. Es una herramienta

que logra optimizar la gestión de la tecnología, para que las organizaciones generen valor y buenas prácticas en el manejo de estos recursos; en pocas palabras, mantiene un equilibrio entre la generación de beneficios, la optimización de los niveles de riesgo y el uso de los recursos.

También hay que destacar que COBIT, al reunir cinco principios que permiten a la organización formar un marco efectivo de gobierno y administración basado en una serie holística de siete habilitadores, también logra que se optimicen las inversiones en tecnología e información, así como que se genere un beneficie a las partes interesadas que lo utilicen.

1.2.3 Evolución del COBIT

Desde sus inicios el COBIT ha tenido como fin funcionar como un marco que ayude a las entidades a cumplir sus obligaciones regulatorias, alinear actividades de manera interna e incrementar el valor, todo esto asociado a las tecnologías de información.

A pesar de ello, COBIT ha pasado por diversas etapas o enfoques: auditoría de TI, control, gestión de TI, gobierno de TI, hasta el enfoque holístico de gobierno corporativo de TI en su versión actual, COBIT 5. Esto se visualiza de mejor manera en la figura 2:

Figura 2: *Evolución de COBIT*

Fuente: Elaboración propia con base en el *Modelo de Gobierno de TI como apoyo al proceso de transformación digital en empresas de la industria editorial* (Saavedra, J., & Torres, A , 2012, p.25).

1.2.3.1 COBIT 4.1. En este apartado se desarrollará COBIT 4.1 de forma general, con el fin de marcar diferencias y la importancia de su evolución con respecto a COBIT 5.

La primera publicación de COBIT se dio en 1996 y desde entonces ha sufrido varias actualizaciones: ha pasado de ser una herramienta para auditoría a un marco que abarca tanto la gestión como el gobierno corporativo de las empresas.

El COBIT 4.0 fue publicado en noviembre de 2005 y fue la primera gran actualización que marcó el COBIT, comparado con sus anteriores versiones, como el COBIT 3. Las actualizaciones que trajo COBIT 4.0 y COBIT 4.1 fue la de incluir la racionalización de los objetivos de control y controles de aplicación, la mejora de proceso controles y una mayor explicación de la medición del desempeño. Además, el COBIT 4.1 se compone de cuatro dominios, treinta y cuatro procesos y doscientos veinte objetivos de control.

1.2.3.1.1 Dominios. Para poder determinar los riesgos y las actividades, se necesita administrarlos correctamente, es por esto que COBIT 4.1 define sus actividades de TI en un modelo de 34 procesos, los cuales se agrupan en un total de 4 dominios: planear y organizar (PO), adquirir e implementar (AI), entregar y dar soporte (DS) y monitorear y evaluar (ME) (IT Governance Institute [ITGI], 2007).

El primer dominio lo que busca es la forma en la que TI pueda mejorar el logro de los objetivos, el segundo dominio se encarga de identificar y desarrollar las soluciones, el tercero es el responsable de la entrega y prestación del servicio solicitado y, por último, el cuarto dominio se encarga de evaluar de forma constante la calidad y el cumplimiento de los requerimientos.

1.2.3.1.2 Controles del negocio y controles de TI. Uno de los objetivos del negocio es el de fijar un nivel de dirección ejecutiva y es con base en esto que los controles de TI se guían. Los controles de negocio son a nivel de procesos y actividades específicas de negocio; los controles de TI son proporcionados para soportar dichos procesos (ITGI, 2007).

1.2.3.1.3 Generadores de mediciones. Las empresas deben saber medir dónde se encuentran y dónde requieren mejorar, es por esto que COBIT responde a estas preguntas utilizando el modelo de madurez, las metas y mediciones, y las metas de actividades (ITGI, 2007).

El modelo de madurez logra que la empresa identifique el desempeño real, el estatus real de la industria y el objetivo de mejora. Este modelo inicia con el nivel 0, el cual es llamado "no existente", ya que la empresa ni siquiera conoce que existe un problema; luego sigue el nivel 1 "inicial", donde la empresa ya identificó un problema pero no hay procesos sino enfoques; el nivel 2 "repetible", donde existen procesos pero no comunicación de ellos; nivel 3 "definido", donde hay procedimientos estandarizados, se documentan, pero el individuo es el que elige utilizarlos; el nivel 4 "administrado", donde ya es posible monitorear y medir el cumplimiento, además de una constante mejora que proporciona buenas prácticas; y por el último el nivel 5 "optimizado", el cual se basa en los resultados de la mejora continua y en un modelo de madurez con otras empresas (IT Governance Institute, 2007).

1.2.3.2 COBIT 5.0: En cuanto a COBIT 5, la razón de utilizarlo como marco base para el componente de información y comunicación en CODEA, se debe a que se encuentra completamente alineado a estándares globales los cuales son utilizados y conocidos de manera generalizada, pero principalmente el hecho de que se adecúa a cualquier institución.

1.2.3.2.1 Principios COBIT 5. Dado que esta última versión de COBIT está enfocada en el Gobierno Corporativo de IT, la institución requiere asumir responsabilidades necesarias para la implementación del mismo, las cuales irán en línea con los principios de este marco.

Saavedra y Torres (2012), identifican las siguientes ideas de los cinco principios básicos de COBIT 5 que se detallan a continuación:

1. **Satisfacer las necesidades de las partes interesadas:** Este principio está enfocado completamente a la razón de ser del marco dentro de una entidad o institución, necesidades alineadas con los objetivos empresariales específicos, objetivos de TI y objetivos habilitadores, optimizando el uso de los recursos al momento de obtener los beneficios con un nivel aceptable del riesgo.

2. **Cubrir a la empresa de extremo a extremo**: El marco establece los siete habilitadores de COBIT, con el fin de que la empresa respalde sus áreas de forma que queden cubiertas de extremo a extremo.

3. **Aplicar un marco de referencia único integrado**: COBIT 5 integra los mejores marcos de ISACA como Val IT, Risk IT, Business Model for Information Security (BMIS) e IT Assurance Framework (ITAF). Además, como se indicó en puntos anteriores, está completamente alineado con estándares globales, por lo que se garantiza la homogeneidad de los lineamientos.

4. **Posibilitar un enfoque holístico**: Hace énfasis en que tanto el Gobierno de TI como la Gestión de TI operen bajo el mismo fin, para ello establece los habilitadores, los cuales son clasificados en 7 categorías.

5. **Separar el gobierno de la gestión**: El marco COBIT 5 establece una separación entre Gobierno de TI y Gestión de TI, de esta manera el primero se encarga de evaluar, dirigir y monitorear, y el segundo de planificar, construir, ejecutar y monitorear.

1.2.3.2.2 Catalizadores COBIT 5. Los facilitadores, habilitadores o catalizadores de COBIT 5, son los elementos que logran que los procesos y las políticas de las organizaciones se realicen de manera más sencilla, para lograr un rendimiento y cumplimiento de los objetivos de forma óptima.

ISACA (2012a) hace mención de 7 catalizadores que deben interactuar entre sí (esta interacción se aprecia en la figura 3). Estos elementos son:

1. Principios, políticas y marcos de referencia: traducen el comportamiento deseado.
2. Procesos: conjunto de prácticas y actividades para alcanzar los objetivos.
3. Estructuras organizacionales: son los entes de toma de decisiones.
4. Cultura, ética y comportamiento: características de los individuos que forman la empresa.
5. Información: toda la información producida y utilizada en la organización.
6. Servicios, infraestructura y aplicaciones: infraestructura, tecnología y aplicaciones que posee la organización.
7. Personas, habilidades y competencias: está relacionada propiamente con las personas, el cual es de suma importancia para la toma de decisiones y evaluar que se pueden satisfacer todas las actividades.

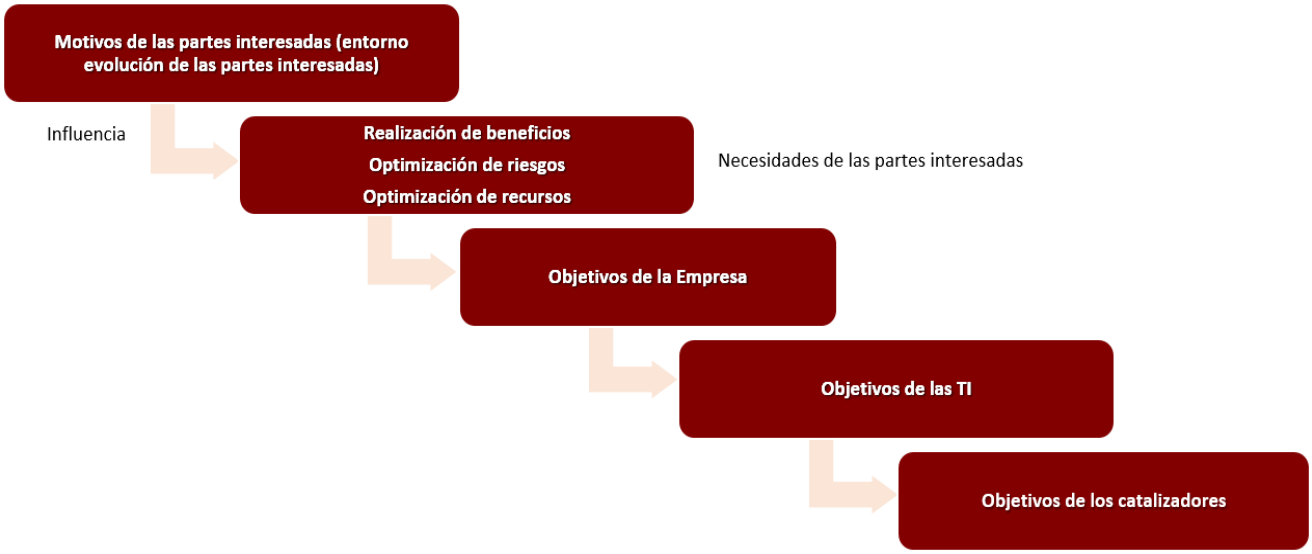
Figura 3: *Catalizadores COBIT 5*

Fuente: Elaboración propia adaptado de *COBIT 5 Un marco de negocio para el gobierno y la gestión de las TI de la empresa* (ISACA, 2012a, p. 27).

1.2.3.2.3 Cascada de metas (técnica COBIT 5). De acuerdo con COBIT 5 Procesos Catalizadores, la cascada de metas ". . . es el mecanismo para traducir las necesidades de las partes interesadas en metas corporativas específicas, practicables y personalizadas, metas de TI y metas de los catalizadores. Esta traducción permite establecer metas específicas a cualquier nivel y en toda área de la empresa como apoyo a las metas globales y los requerimientos de las partes interesadas" (ISACA, 2012c, p.13).

Con la anterior definición de una cascada de metas, se entiende que esta herramienta o mecanismo permite a las diversas organizaciones establecer prioridades en el proceso de mejora e implementación del Gobierno de TI, ya que establece las metas de manera estratégica, así como la relación e importancia de los catalizadores, esto se puede observar en la figura 4:

Figura 4: *Catalizadores COBIT 5*



Fuente: Elaboración propia adaptado de *COBIT 5 procesos catalizadores* (p.14), por ISACA, 2012c.

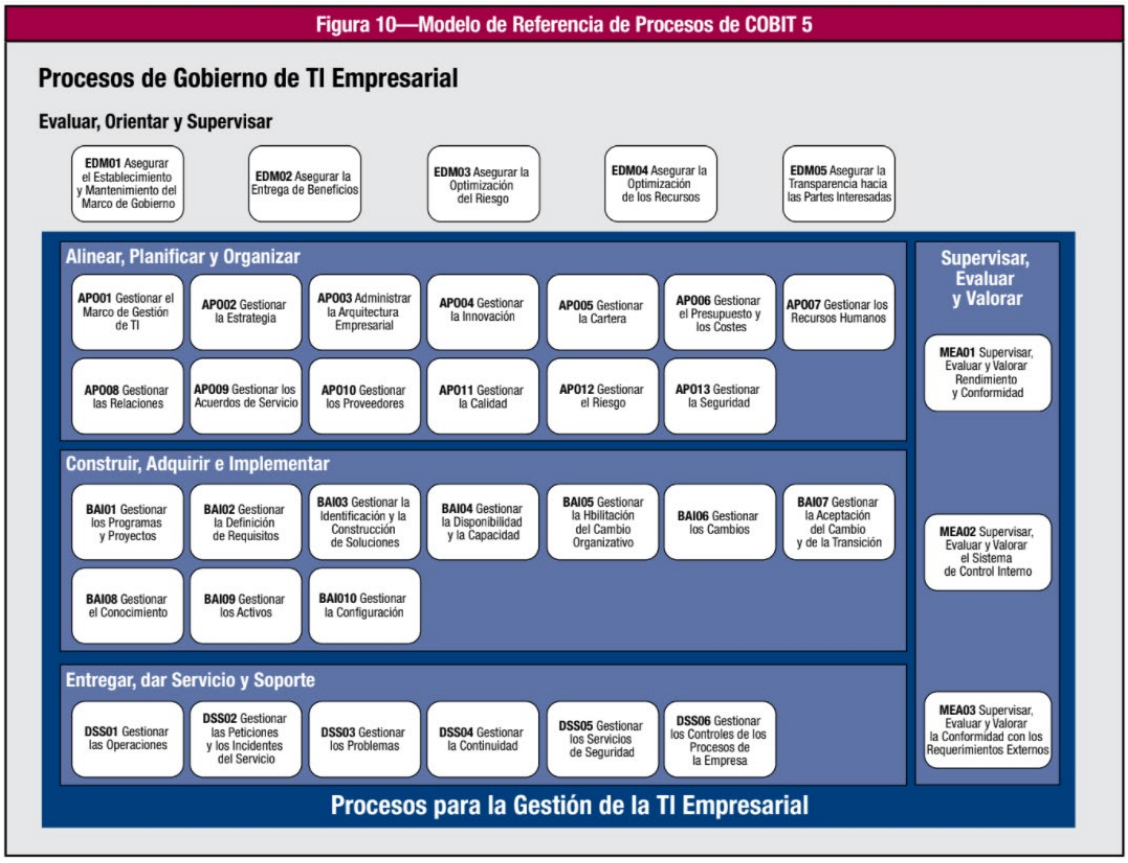
Tal y como se muestra en la figura 4, a continuación, se expone en qué consiste cada uno de esos pasos:

- Paso 1: conocer que los motivos de las partes interesadas pueden estar influenciadas por las necesidades, tales como el entorno del negocio, nuevas tecnologías, etc.
- Paso 2: identificar que las necesidades de las partes interesadas pueden estar relacionadas con un conjunto de metas genéricas corporativas y que dichas metas representan una lista que las empresas utilizan comúnmente.
- Paso 3: se refiere a que el logro de las metas empresariales requiere un número de resultados relacionados con las tecnologías de información.
- Paso 4: reconocer el objetivo o la razón por la cual las tecnologías de información forman parte importante en el proceso y el cual va de la mano con el último paso.

- Paso 5: alcanzar las metas relacionadas con las tecnologías de información, requiere la implementación satisfactoria junto con el uso de varios de los catalizadores.

1.2.3.2.4 Procesos de COBIT 5. En esta sección se detallan los procesos de gobierno de TI empresarial de COBIT 5: a) evaluar, orientar y supervisar (EDM), b) alinear, planificar y supervisar (APO), c) construir, adquirir e implementar (BAI), d) entregar, dar servicio y soporte (DSS) y e) supervisar, evaluar y valorar (MEA). Cada uno de ellos se detallan en la figura 5.

Figura 5: *Conjunto completo de procesos de gobierno y gestión de COBIT 5.*



Fuente: Tomado de *COBIT 5 procesos catalizadores* (p.27), por ISACA, 2012c.

A continuación, se explican más detalladamente los procesos mencionados en el apartado anterior:

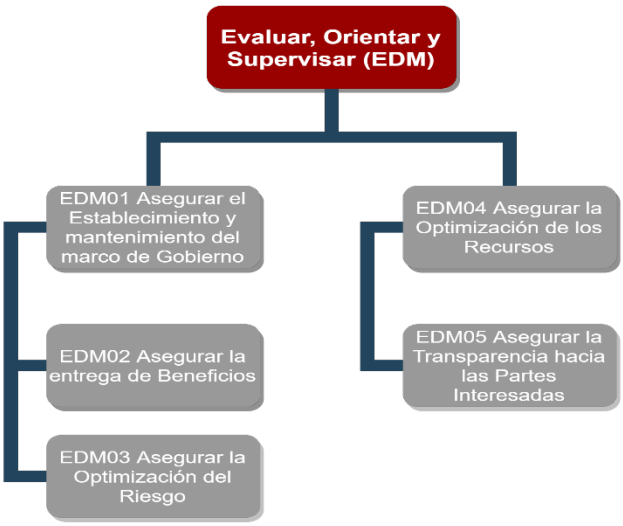
1. Evaluar, orientar y supervisar (EDM): Este dominio está compuesto por 5 procesos y 15 prácticas de gestión, y es el primer dominio en los procesos de COBIT 5.

   Por medio de este dominio, los procesos aseguran que la entidad defina el camino para la consecución de los objetivos, por medio de la evaluación de las necesidades de los interesados, así como marcar la ruta para orientarlos y supervisarlos.

   Dentro de los procesos que presenta se encuentran analizar los requerimientos que necesita el gobierno de TI de la empresa, supervisar las estructuras y los procesos, evaluar las prácticas para que logren de mejor manera los objetivos, optimizar el valor del negocio, asegurarse que la tolerancia y el apetito de riesgo de la empresa lo conozcan todos y sea el adecuado, tiene presente las capacidades y su objetivo es dar una ruta para brindar soluciones a la entrega de servicios.

   A continuación, se detallan los procesos y prácticas de gestión:

Figura 6: *Evaluar, orientar y supervisar*



Fuente: Elaboración propia adaptado de *COBIT 5 Procesos Catalizadores* (p.24), por ISACA, 2012c.

2. Alinear, planificar y supervisar (APO): Este dominio está compuesto por 13 procesos y 72 prácticas de gestión.

   En *COBIT 5 procesos catalizadores*, se indica que se debe considerar la implementación de mecanismos y autoridades para la gestión de la información y uso de TI.

   Además, se debe establecer un plan estratégico que contenga una visión holística del negocio actual y del entorno de TI.

   Debe establecerse una

   > ". . . arquitectura común compuesta por los procesos de negocio, la información, los datos, las aplicaciones y las capas de la arquitectura tecnológica de manera eficaz y eficiente para la realización de las estrategias de la empresa y de TI mediante la creación de modelos clave y prácticas que describan las líneas de partida y las arquitecturas objetivo." (ISACA, 2012c, p. 63)

   Además, este dominio también contiene el tema de la gestión de la innovación como un proceso, en el establece que las entidades deben "mantener un conocimiento de la tecnología de la información y las tendencias relacionadas con el servicio, identificar las oportunidades de innovación y planificar la manera de beneficiarse de la innovación en relación con las necesidades del negocio." (ISACA, 2012c, p. 68).

   Por otra parte, también se indica que se debe gestionar debidamente el portafolio de proyectos, esto debido a que cada una de las inversiones realizadas en TI deben estar alineadas con la visión de la arquitectura empresarial. En línea con lo anterior, se deben gestionar debidamente las actividades financieras que se relacionen con las TI, por ende

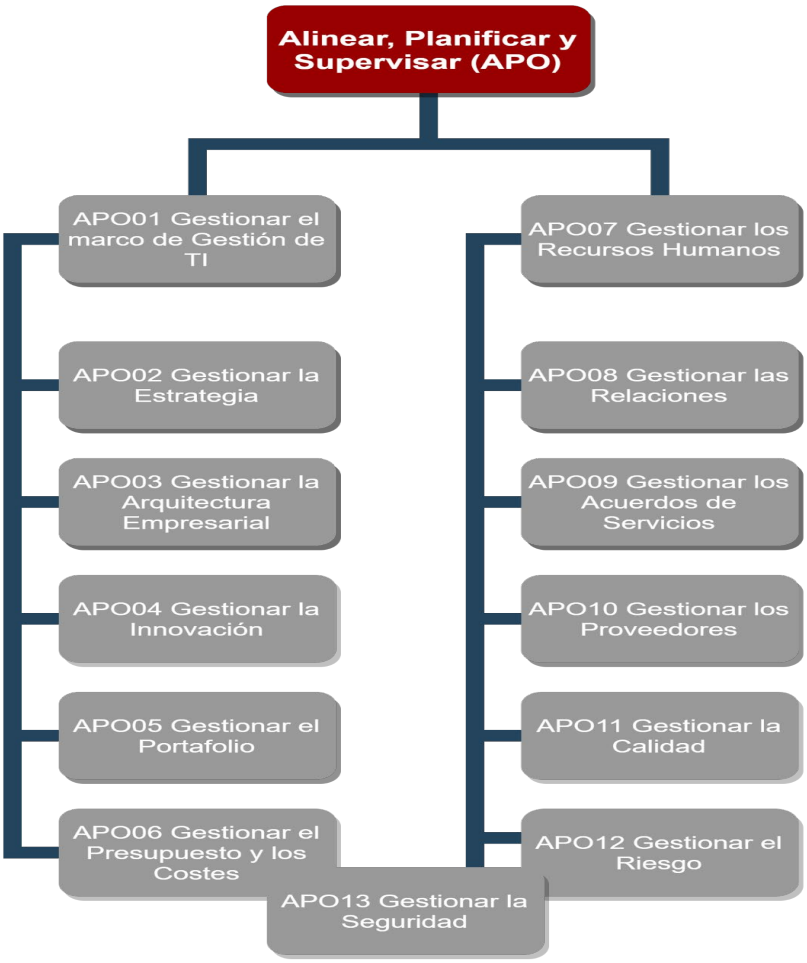
se debe identificar y controlar los costes originados por estás actividades e implementar prácticas contables y presupuestarias formales.

Por otra parte, la entidad debe gestionar debidamente los recursos humanos, esto incluye establecer y comunicar las funciones a cada uno de los funcionarios, así como mantener una debida gestión de las habilidades y competencias junto con evaluaciones de desempeño.

También, se establece la importancia de mantener debidamente gestionadas todas aquellas relaciones del negocio y acuerdos de servicio que la empresa posea, así como las relaciones con los proveedores.

Finalmente, es importante "definir y comunicar los requisitos de calidad en todos los procesos, procedimientos y resultados relacionados de la organización, incluyendo controles, vigilancia constante y el uso de prácticas probadas y estándares de mejora continua y esfuerzos de eficiencia" (ISACA, 2012c, p.101). Además, es importante mantener una constante evaluación de los riesgos relacionados con TI y un sistema para la gestión de la seguridad de la información.

Figura 7: *Alinear, planificar y supervisar*



Fuente: Elaboración propia adaptado de *COBIT 5 Procesos Catalizadores* (p. 24), por ISACA, 2012c.

3. Construir, adquirir e implementar (BAI): El dominio BAI, por sus siglas en inglés (*Build, Acquire and Implement*), se compone de 10 procesos con un objetivo y propósito definido, el cual se describe a continuación:

   COBIT 5 establece que gestionar programas y proyectos del portafolio de inversiones relacionadas con los sistemas de información se debe alinear con la estrategia organizacional, con el fin de obtener beneficios de negocio. Para cumplir con ello se

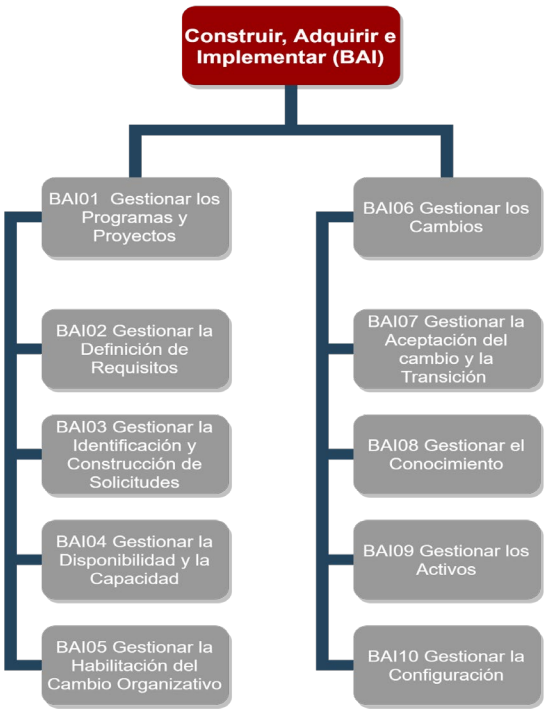
debe gestionar la definición de requisitos, el cual busca analizar requerimientos que cumplan con las necesidades de la entidad para su arquitectura empresarial, para minimizar el riesgo. Dichas inversiones requieren compras y contrataciones que sean rentables y que permitan darle soporte a la estrategia de la organización por medio de la gestión por medio de la identificación y construcciones de soluciones (ISACA, 2012c).

Debido a que la dinámica del entorno y la disponibilidad de los servicios y de tecnologías de información son fundamentales para el cumplimiento de los objetivos, es necesario gestionar su disponibilidad y capacidad, para comprender las capacidades actuales y futuras de acuerdo con un análisis de riesgos que soporte la toma de decisiones. Por lo anterior, la entidad debe de procesar los cambios organizativos previendo las respuestas a las necesidades futuras con un enfoque que permita a las partes interesadas lograr una implementación exitosa, de forma rápida y minimizando el riesgo. Por ende, gestionar la aceptación del cambio y la transición permite preparar a la entidad por medio de una serie de etapas planificadas para lograr soluciones exitosas.

Aunado a lo anterior, gestionar el conocimiento facilita la toma de decisiones, ya que el personal cuenta con las herramientas necesarias para realizar sus actividades con la experiencia adquirida a lo largo de los años. Para cumplir con los objetivos y gestionar la disponibilidad es importante que los activos generen un valor y costo óptimo, por ello administrar los activos los protege físicamente y apoya el cumplimiento de objetivos.

Por lo anterior se concluye que el dominio de "construir, adquirir e implementar" comprende una serie de subprocesos relevantes para que una entidad pueda cumplir con los objetivos por medio de la alineación estratégica.

Figura 8: *Construir, adquirir e implementar*



Fuente: Elaboración propia adaptado de *COBIT 5 Procesos Catalizadores* (p. 24), por ISACA, 2012c.

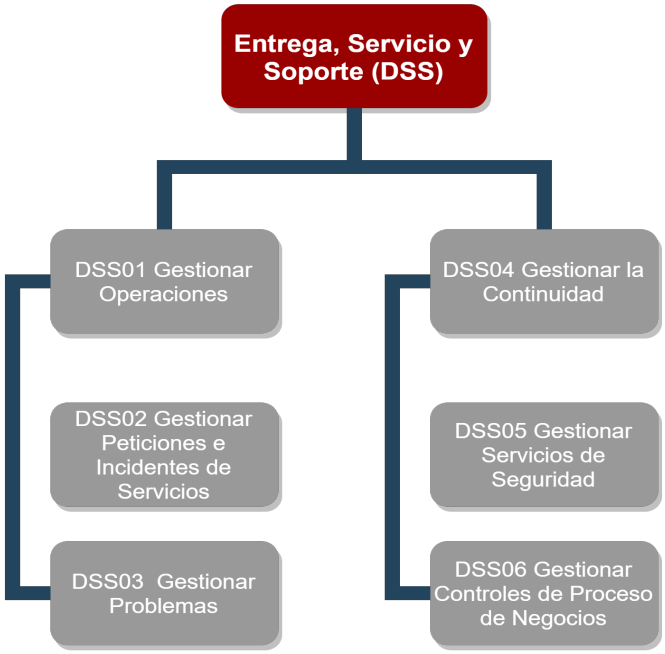
4. Entrega, servicio y soporte (DSS): Este dominio está compuesto por 6 procesos y 38 prácticas de gestión, en los procesos de COBIT 5.

   En este dominio se realiza la entrega de los servicios requeridos y se da soporte a los usuarios del servicio en la información, incluida la seguridad de esta. Es decir, su principal meta es la de lograr que los servicios se entreguen de acuerdo con las prioridades que presenta la empresa, pero considerando costos, confidencialidad y que todo el proceso sea seguro para todas las partes involucradas (ISACA, 2012c).

Por lo que dentro de sus procesos se coordinan realizar actividades para la entrega de TI, tener las respuestas adecuadas en las consultas que realizan los usuarios, diagnosticar, tener disponibilidad de información y tener controles adecuados para asegurar la integridad y la seguridad de la información.

A continuación, se detallan los procesos y prácticas de gestión:

Figura 9: *Entrega, servicio y soporte*



Fuente: Elaboración propia adaptado de *COBIT 5 Procesos Catalizadores* (p.24), por ISACA, 2012c.

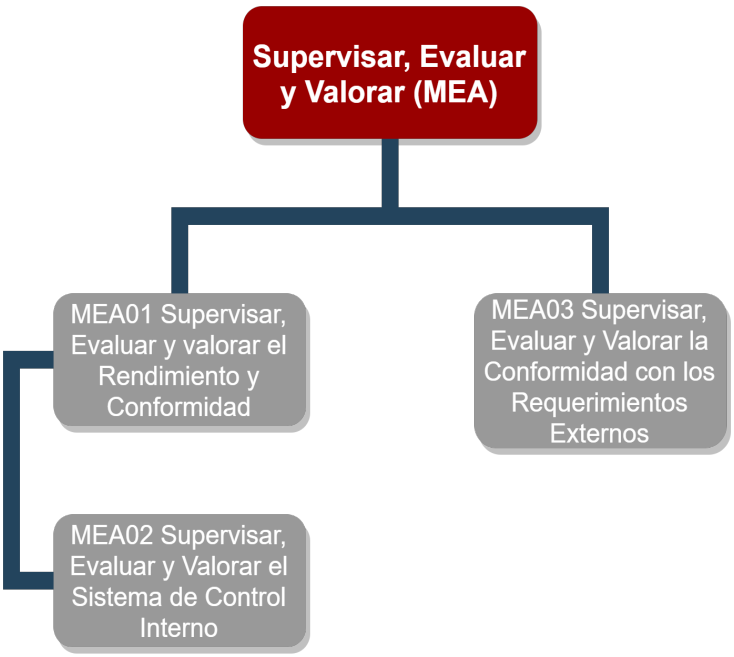
5. Supervisar, evaluar y valorar (MEA): Este dominio está compuesto por 3 procesos y 13 prácticas de gestión, se trata del último dentro de las áreas de gestión de COBIT.

   Por medio de estos procesos la entidad controla que los métodos se están efectuando acorde al rendimiento esperado y a los objetivos y métricas determinadas, mediante este proceso además es que se proporcionan informes de forma sistemática y planificada.

Adicionalmente, a través de la evaluación es que la entidad identifica las deficiencias en el control, direccionando las actividades a realizar para solventarlas. Por otra parte, por medio de estos procesos la entidad evalúa que el cumplimiento de los requisitos regulatorios y contractuales esté acorde a los requerimientos de externos.

En línea con lo anterior es que se concluye que por medio de los procesos MEA la entidad proporciona a sus actividades transparencia y los mantiene en línea con el logro de los objetivos, además asegura la adecuación del control interno y reafirma el cumplimiento de todos los requisitos externos aplicables. A continuación, se detallan los procesos y prácticas de gestión:

Figura 10: *Supervisar, evaluar y valorar*



Fuente: Elaboración propia adaptado de *COBIT 5 Procesos Catalizadores* (p.24), por ISACA, 2012c.

Capítulo 2

Entorno, historia, estructura organizativa y funcionamiento del Comité Cantonal de Deportes y Recreación de Alajuela

2.1 Comités Cantonales de Deportes y Recreación en Costa Rica

Los Comités Cantonales de Deportes y Recreación (en adelante CCDR), son los órganos de cada cantón costarricense, encargados de brindar espacios y recursos de deportes y recreación a las comunidades, con el fin de dar acceso a oportunidades para el desarrollo de destrezas tanto físicas como mentales.

A continuación, se presenta un recuento histórico sobre la creación de los Comités Cantonales de Deportes y Recreación realizado por la Unión Nacional de Gobiernos Municipales, la cual indica que:

> Nacieron a la vida jurídica como órganos dependientes de la Dirección General de Educación Física y Deportes (según Ley Orgánica de la Dirección General de Educación Física y Deportes, N° 3656 del 6 de enero de 1966), la cual a su vez era parte del Ministerio de Educación Pública. Su fin únicamente era la administración de instalaciones deportivas y recreativas.
>
> Posteriormente, mediante Ley N° 6890 del 14 de setiembre de 1983, se adicionó al entonces Código Municipal (Ley No. 4574 de 4 de mayo de 1970), el Artículo 186, en el cual se regulaba la participación de las municipalidades en la integración de los Comités. Se coordinaba con las municipalidades las obras e inversiones del cantón, pero los Comités se mantenían sujetos a los planes nacionales del deporte y recreación elaborados por la Dirección General de Educación Física y Deportes.

> A partir de ese momento, con la derogatoria del Artículo 6 de la Ley Orgánica de la Dirección General de Educación Física y Deportes, N° 3656, que autorizaba la creación y funcionamiento de los Comités para la promoción del deporte en cada localidad, éstos se acercaron más a la estructura municipal. Sin embargo, fue hasta la promulgación del actual Código Municipal (Ley N° 7794 del 26 de abril de 1998.), cuando expresamente se dispuso la adscripción y sujeción de tales comités a los entes locales. (Unión Nacional de Gobiernos Locales, 2013, p.183)

En el artículo N°173 del Código Municipal se establece la creación de los CCDR e indica que debe existir uno en cada cantón y que cada uno deberá estar adscrito a cada municipalidad respectiva. Además, se establecen como entes con personalidad jurídica instrumental, lo cual les da potestad para desarrollar proyectos deportivos y recreativos, así como para construir, administrar y mantener instalaciones (Código Municipal N°7794, 1998).

Respecto a la personalidad jurídica, la Procuraduría General de la República, mediante el Dictamen C-062-2018 de 04 de abril de 2018, indica que:

> Este tipo de personalidad en definitiva no puede considerarse como equivalente a la creación de entes descentralizados, sino que más bien se trata de una "personalidad parcial, no plena, que les permite a los órganos actuar en un ámbito restringido (desconcentrado) como si fueran personas jurídicas diferentes al ente público al que pertenecen (. . .). En el caso de los comités cantonales, estos órganos ostentan tal personalidad en virtud de que cuentan con fondos limitados para realizar determinados actos de gestión, referentes a la construcción, administración, y manutención de las instalaciones deportivas de su propiedad u otorgadas en administración. (Procuraduría General de la República [PGR], 2018, p. 4)

Por otra parte, en cuanto a su conformación, el Código Municipal en el artículo N°174 indica que estos comités están integrados por cinco residentes del cantón: dos personas miembros de nombramiento del Concejo Municipal, dos personas miembros de las organizaciones deportivas y recreativas del cantón y una persona de las organizaciones comunales restantes y cada una de estas personas son electas cada dos años. La elección de los miembros del comité cantonal se rige a partir de los lineamientos dictados por la municipalidad respectiva y se asumen como funcionarios de la municipalidad. Tienen un período de dos años en sus cargos y no devengan ningún tipo de remuneración (Código Municipal N°7794, 1998).

En lo que respecta al financiamiento de los CCDR, en el artículo N°173 del Código Municipal se establece que cada municipalidad deberá asignarle a cada comité un mínimo de 3% de sus ingresos ordinarios anuales (Código Municipal N°7794, 1998). Esto con el fin de que lleven a cabo las actividades necesarias para el cumplimiento de sus objetivos. Respecto a lo anterior, la Contraloría General de la República mediante el oficio DFOE-DL-0162, del 12 de febrero de 2021 indica que:

> Las Municipalidades deben cumplir con el precepto legal del artículo 173 tantas veces referenciado para el destino correcto de los fondos; también a efectos presupuestarios esa transferencia debe reflejarse en los presupuestos de las Municipalidades, y es responsabilidad de la Municipalidad la ejecución de esos recursos por parte del CCDR. (CGR, 2021, p. 6)

Así mismo, cabe señalar que el Instituto Costarricense del Deporte y la Recreación (ICODER), también cede sus instalaciones y transfiere recursos a estas entidades. Un ejemplo de ello es que, según el Sistema de Información sobre Planes y Presupuestos (SIPP) de la CGR, el ICODER presupuestó en el 2019, para 22 CCDR del país, un monto de 215 mil millones de colones, con el fin de promover la realización de proyectos recreativos presentados por CCDR

en cantones seleccionados[1].

En otro orden de ideas, es importante rescatar la relación existente entre los CCDR y los Consejos Municipales. Según el Código Municipal en el artículo N°181, cada primera semana de julio de cada año, los CCDR deberán someter "a conocimiento de los Concejos Municipales sus programas anuales de actividades, obras e inversión, antes de aprobarse los presupuestos ordinarios de la municipalidad" (Código Municipal N°7794, 1998, p. 103).

Finalmente, existe la figura del comité comunal, este se establece a partir del artículo N° 175 del Código Municipal, donde se indica que:

> El comité comunal estará integrado por siete miembros residentes en la comunidad respectiva, nombrados en la asamblea general, convocada para tal efecto por el comité cantonal. La asamblea general estará conformada por dos representantes de cada una de las organizaciones deportivas, recreativas y de desarrollo comunal existentes en la comunidad. (Código Municipal N° 7794, 1998, p. 100)

Los comités comunales son órganos que perciben sus recursos a través de los CCDR. Su ámbito de acción es menor en comparación con los CCDR, pero tienen una gran importancia, debido a que sus acciones se desarrollan a nivel comunal lo cual pretende cubrir la mayor parte posible del cantón.

[1] Datos extraídos del Sistema de Información sobre Planes y Presupuestos (SIPP), específicamente del Plan Operativo Institucional 2019 del ICODER y Detalle de Transferencias.

A continuación, se presentan algunas de las características más destacables de los CCDR:

Figura 11: *Características de los Comités Cantonales de Deportes y Recreación*

Fuente: Contraloría General de la República (2017). Informe de auditoría de carácter especial acerca de la actividad del Comité Cantonal de Deportes y Recreación de Paraíso.

De igual forma, se suma como parte de sus características más relevantes la administración de recursos públicos que llevan a cabo. En esta línea, según el SIPP, para el período 2020, un total de 79 CCDR del país llegaron a presupuestar montos que oscilan entre los 15 millones de colones y los 13.983 millones de colones, sumando un total de 74.378 millones de colones para ese periodo.

En la tabla 2 se muestra la distribución por estratos del total presupuestado para el 2020 y la cantidad de CCDR incluidos en cada uno.

Tabla 2: *Monto total presupuestado por estrato, período 2020*

Número de estrato	Límites	Cantidad de CCDR	* Monto total presupuestado por estrato
1	0- 1.000	60	₡19.880
2	1.001-2.000	12	₡17.732
3	2.001-3.000	2	₡4.522
4	3.001-4.000	1	₡3.531
5	4.001-5.000	2	₡8.612
6	5.001-6.000	0	₡0
7	6.001-7.000	1	₡6.116
8	7.001-8.000	0	₡0
9	8.001-9.000	0	₡0
10	9.001-10.000	0	₡0
11	10.001-11.000	0	₡0
12	11.001-12.000	0	₡0
13	12.001-13.000	0	₡0
14	13.001-14.000	1	₡13.984
Totales:		**79**	**₡74.378**

Nota. Montos en millones de colones.

Fuente: Elaboración propia, con datos del Sistema de Información sobre Planes y Presupuestos (SIPP) de la Contraloría General de la República.

De acuerdo a la tabla anterior, se observa que del total de 79 CCDR activos para el 2020, 60 presupuestaron recursos inferiores a 1.000 millones de colones. Sin embargo, no dejan de ser importantes puesto que la sumatoria total de sus presupuestos es de 19.880,06 millones de colones.

Por otra parte, se observan dos casos particulares: uno de ellos consiste en un solo CCDR que presupuestó recursos entre 6.001 y 7.000 millones de colones, lo cual es cifra

cuantiosa en comparación con lo solicitado por los demás CCDR; el segundo corresponde a un CCDR que presupuestó un total de 13.983,58, lo cual se sale completamente del estándar, que es establecido por el Comité Cantonal de Deportes y Recreación de San José.

El CODEA se encuentra ubicado en el quinto estrato, ya que presupuestó más de 4.000 millones de colones para el periodo 2020. Dado lo expuesto, se infiere que este CCDR se encuentra entre los cinco CCDR más grandes de Costa Rica en términos de manejo de recursos.

2.2 Contextualización histórica, organizativa y funcional del CODEA

En esta sección, se contextualiza el funcionamiento del CODEA, para lo cual se describe su historia, misión, visión, instalaciones, estructura administrativa, valores y principales procesos.

2.2.1 Historia del CODEA

De acuerdo con la información brindada por el CODEA, mediante entrevista al Director Administrativo en el 2020, esta institución fue creada por el artículo 186 del Código Municipal, reformado por la ley N°6890 del 23 de setiembre de 1983. En el documento, se define como el organismo superior en el cantón central de Alajuela encargado de la atención y vigilancia de la actividad deportiva en todos sus aspectos, por medio de la promoción del deporte y la recreación, procurando el aprovechamiento del tiempo libre de sus habitantes mediante una recreación saludable. Se menciona además que este ente se regirá por las disposiciones del presente reglamento autónomo de organización. El Polideportivo Monserrat de la ciudad de Alajuela, parte de esta institución, se ubica en el barrio Monserrat y fue construido para los XI Juegos Deportivos Nacionales Alajuela de 1987. (Vargas, comunicación personal, 22 de febrero de 2020).

2.2.2 Misión

De acuerdo con el marco estratégico del CODEA, su misión se define de la siguiente manera:

> Promover el deporte y la recreación a través de la administración, construcción y mantenimiento de infraestructura deportiva y políticas públicas que contribuyan al desarrollo y bienestar integral de los habitantes de Alajuela. (Vargas, comunicación personal, 22 de febrero de 2020).

2.2.3 Visión

El CODEA define su visión de la siguiente forma:

> Ser el Comité Cantonal de referencia nacional e internacional en la adecuada promoción del deporte, la recreación y la actividad física a través de programas inclusivos, innovadores e integrales para niños, jóvenes, personas con discapacidad, adultos mayores y atletas de alto rendimiento. (Vargas, comunicación personal, 22 de febrero de 2020).

2.2.4 Valores

Los principios generadores de compromiso establecidos por el CODEA para el desarrollo de sus acciones corresponden a cinco valores: respeto, trabajo en equipo, disciplina, profesionalismo y solidaridad.

2.2.5 Escudo y colores

Los colores oficiales del deporte del cantón de Alajuela son el blanco, rojo y negro.

Imagen 1: *Escudo del CODEA*

Fuente: Comité Cantonal de Deportes y Recreación de Alajuela (CODEA)

2.2.6 Funciones del CODEA

El Código Municipal N°7794 en el artículo 173, establece entre las funciones generales de los CCDR: “desarrollar planes, proyectos y programas deportivos y recreativos cantonales, así como construir, administrar y mantener las instalaciones deportivas de su propiedad o las otorgadas en administración” (Código Municipal N°7794, 1998, p. 99).

Para llevar a cabo lo anterior, el CODEA estableció una variedad de programas deportivos: programa de juegos deportivos nacionales y escuelas deportivas, programa de comités comunales de deportes, programa de adultos mayores, programa de adultos jóvenes, programa deporte adaptado, programa de deporte y recreación para personas con capacidades especiales, programa de zumba para todos y programa de ejercicios funcionales (nivel avanzado y básico). De estos programas se extraen los siguientes objetivos generales:

- Ejecutar el programa de promoción y competición deportiva para los jóvenes del cantón.
- Mejorar los hábitos de actividad física y la calidad de vida de las personas del cantón

de Alajuela.

- Brindar un espacio de aprendizaje, recreación, salud y competitividad para la población en situación de discapacidad en diferentes disciplinas deportivas y actividades recreativas.
- Aumentar la oferta deportiva a los adultos y mejorar los ingresos mensuales del CODEA utilizando infraestructura y capacidad instalada del Polideportivo Monserrat en algunas franjas horarias accesibles para la población trabajadora.

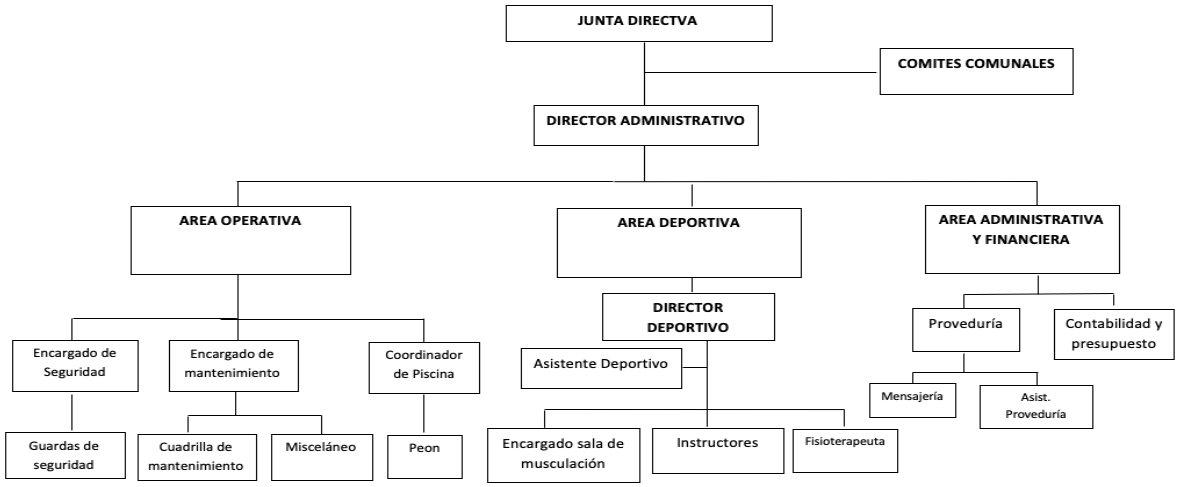
2.2.7 Estructura organizativa

Según el organigrama del CODEA (ver figura 12), actualmente su estructura organizacional se divide en tres áreas: 1) operativa, 2) deportiva y 3) administrativa y financiera. Estas tres áreas están conformadas por 35 funcionarios en total y son administradas por una persona en el rol de directora administrativa que rinde cuentas a la junta directiva del comité.

El área deportiva se encarga del desarrollo de las personas atletas. En cuanto al área operativa, se encarga de mantener y mejorar las obras que posee el CODEA y sus principales actividades son mantener la seguridad y el mantenimiento de las instalaciones. Por último, se encuentra el área administrativa y financiera, la cual está conformada por dos departamentos: contabilidad y presupuesto, por un lado, y proveeduría, por otro (Municipalidad de Alajuela, 2011).

Las actividades del CODEA giran en torno al funcionamiento conferido en el Reglamento para la Organización y Funcionamiento del Comité Cantonal de Deportes y Recreación de Alajuela el cual se apega de forma estricta a lo establecido por el Código Municipal.

Figura 12: *Organigrama del CODEA 2021*



Fuente: Elaboración propia.

2.2.8 Instalaciones

Dentro de la normativa del CODEA, el Reglamento para la Organización y Funcionamiento del Comité Cantonal de Deportes y Recreación de Alajuela, establece en su artículo 51 lo siguiente:

> "El Comité Cantonal será el administrador general de las instalaciones deportivas inscritas a nombre de la Municipalidad de Alajuela y podrá ceder Instalaciones Deportivas a los Comités Comunales, los que deberán estar debidamente inscritos y a la vez deben contar con todos los requisitos que para su funcionamiento exige el presente Reglamento para su administración y mantenimiento, sin que por esta razón ceda su responsabilidad." (Municipalidad de Alajuela, 2011, p. 29).

De acuerdo con lo anterior, el Comité administra un complejo deportivo compuesto por: un terreno con una extensión de 3 hectáreas, un boulevard, un sendero, cinco canchas de fútbol, dos canchas de tenis, una pista de atletismo, una piscina olímpica, un gimnasio, un aula de capacitaciones, un aula de entrenamiento de ajedrez, vestidores ubicados en la piscina, dos

canchas de béisbol, dos canchas de baloncesto bajo techo, un parque infantil, dos canchas de voleibol de playa y dos sodas.

Además, a nivel comunal, registra 43 canchas de fútbol y otras instalaciones en los 14 distritos del cantón. A continuación, se presenta el detalle del distrito, nombre del comité comunal y la instalación, respectivamente:

Tabla 3: *Instalaciones del CODEA por distritos de Alajuela*

Distrito	Comité comunal	Instalación
Alajuela	Brasil (Maracaná)	Cancha de fútbol municipal
	Canoas	Cancha de fútbol municipal y salón multiuso
	El Carmen	Cancha de fútbol municipal
	El Llano	Cancha de fútbol municipal
	Montecillos	Cancha de fútbol INVU
	Plaza Acosta	Cancha de fútbol municipal y soda
	Plaza Iglesias	Cancha de fútbol municipal
	Villa Bonita	Salón comunal que se utiliza como multiuso y cancha de fútbol de la asociación de desarrollo

Carrizal	Carrizal	Cancha de fútbol ADI, planché y salón multiuso CODEPLAN
	Comité Comunal Pavas Carrizal	Cancha de fútbol y salón multiuso
Desamparados	Fátima	Planché multiuso municipal
	Desamparados	Cancha de fútbol municipal
	INVU Las Cañas	Cancha de fútbol propiedad del INVU
	Mondovi	Cancha de fútbol ADI, salón comunal y parque infantil
Guácima	Guácima Abajo	Cancha de fútbol municipal
	Guácima Arriba	Cancha de fútbol municipal
	San Francisco	Cancha de fútbol municipal
	Santiago Oeste COCO	Cancha de fútbol municipal
Garita	La Garita	Cancha de fútbol y salón multiuso de la Asociación Integral de la Garita
Río Segundo	Barrio San José	Cancha de fútbol municipal
	Río Segundo	Cancha de fútbol finca sin dueño

	La California	Cancha de fútbol municipal
Sabanilla	Fraijanes	Cancha de fútbol de la asociación de desarrollo y soda
	Poasito	Cancha de fútbol Manuel Emilio Avendaño
	Sabanilla Los Ángeles	Salón de la iglesia
	San Luis	Cancha de fútbol municipal
San Antonio	El Roble	Cancha de fútbol municipal
	San Antonio Del Tejar *	Cancha de fútbol municipal y parque con aros de baloncesto
	La Pradera	Planché municipal
San Isidro	Pilas	Cancha de fútbol y salón comunal de la ADI
	Itiquis	Cancha de fútbol municipal y salón multiuso de la asociación de desarrollo
	San Isidro	Cancha de fútbol de la finca la Emilia / hermanos Vargas
	San Martin (pertenece a la ADI)	Cancha de fútbol de la asociación de desarrollo

San José	Los Jardines	Cancha de fútbol 5 y planché Zeledón e hijos
	Pueblo Nuevo	Cancha de fútbol municipal y parque con máquinas de la municipalidad
San Rafael	San Rafael	Cancha de fútbol municipal
Sarapiquí	Corazón de Jesus	Cancha de fútbol municipal
	Paraíso	Cancha de fútbol municipal
	San Miguel Sarapiquí	Cancha de fútbol municipal
Turrucares	Cebadilla	Cancha de fútbol
	San Miguel	Cancha de fútbol y planché municipal
	Turrucares	Cancha de fútbol ADI
Tambor	Cacao	Cancha de fútbol y planché municipal, gimnasio AD y soda
	Tuetal Norte	Cancha de fútbol municipal y soda
	Tambor	Cancha de fútbol temporalidad de la iglesia católica

Fuente: Elaboración propia con información suministrada por el Director Administrativo del CODEA.

El uso de las instalaciones está a disposición del público en general, y las tarifas por su uso son de cobro obligatorio y son establecidas anualmente por el Comité Cantonal. El ingreso por cobro de uso de instalaciones debe ser presupuestado anualmente y deben destinarse a las siguientes actividades y en los siguientes porcentajes: 65% para mantenimiento de las instalaciones, 15% para programas de promoción deportiva, 10% para ligas menores de la jurisdicción y 10% para gastos administrativos del comité comunal (Municipalidad de Alajuela, 2011, p. 30-32).

En el uso de las instalaciones deportivas existentes, los comités deben fomentar la participación a todos los grupos deportivos y recreativos, como adultos mayores, personas con discapacidad y cualquier agrupación de personas sin discriminación de ningún tipo.

2.2.9 Infraestructura tecnológica del CODEA

Anteriormente el sistema informático que soportaba las operaciones del CODEA se llamaba SYGA-CODEA, el cual presentaba una diversidad de problemas operativos que impedían su óptimo funcionamiento, que habían sido señalados en informes de auditoría de la Municipalidad de Alajuela[2]. Por ello, el año 2020 se empezó el proceso de licitación para migrar hacia una nueva plataforma tecnológica que le permitiera desempeñar sus procesos de la mejor manera.

A partir de octubre de 2020, el sistema informático fue adjudicado a la empresa FCS International Consultant Group, para el desarrollo e implementación del paquete empresarial ERP (Enterprise Resource Planning) llamado SAP Business One, con el objetivo de alinear las

[2] INFORME 08-2019: Evaluación sobre el uso, seguridad y controles del sistema informático que utiliza el Comité Cantonal de Deportes y Recreación de Alajuela.

INFORME 10-2020: Estudio de carácter especial sobre la administración del Comité Cantonal de Deportes y Recreación de Alajuela,período 2019.

estrategias del CODEA con sus procesos clave. Dentro de los beneficios obtenidos se destacan: operación en tiempo real, la integración de las diferentes áreas que apoyan en la ejecución del plan estratégico, la centralización y el control de la información para la toma de decisiones.

La plataforma tecnológica permite integrar los módulos de gestión de tesorería, inventarios, recepción y emisión de facturas, proveeduría, control de actas, contabilidad y presupuesto con base en las Normas de Contabilidad del Sector Público (NICSP) y un módulo que permite una conexión directa con el Sistema Integrado de Compras Públicas (en adelante SICOP), respetando la normativa y marco jurídico costarricense, en especial atención a la Ley de Control de Interno, Ley General de Administración Pública, Ley de Presupuestos Públicos, Ley de Contratación Administrativa y todos sus reglamentos.

Además del ERP, también se contará con una página web integrada con SAP Business One, con elementos que permitan el desarrollo y optimización de procesos del CODEA, tales como: la venta de productos y servicios, alquiler de instalaciones, cursos y capacitaciones por medio un nuevo proceso de *e-commerce*, la transparencia gubernamental con publicación de estados financieros, los presupuestos y actas, encuestas para satisfacción de los usuarios, información sobre los programas deportivos e institucionales, noticias referentes al CODEA, entre otras funcionalidades.

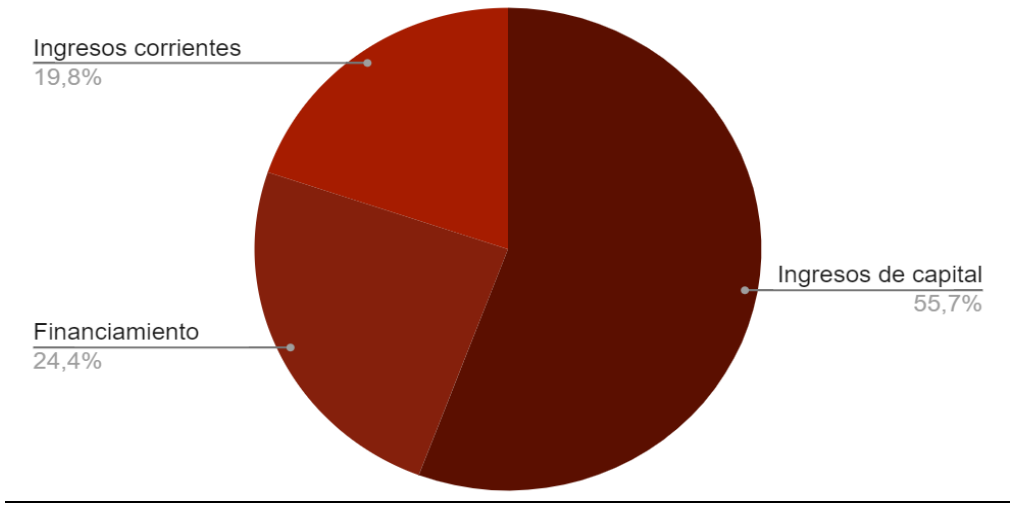
El cambio en la plataforma permitirá al CODEA lograr un avance en el tema tecnológico, lograr mejorar el sistema de control interno, alinearse a los criterios técnicos de las diversas normativas a las que está sujeto, así como en procura de la transparencia.

2.2.10 Recursos y presupuesto

Como se había mencionado anteriormente, mediante el artículo N°173 del Código Municipal, se establece que las municipalidades deben destinar al menos 3% de los ingresos anuales ordinarios a los CCDR. Además de esto, el CODEA puede percibir ingresos de diferentes fuentes: mediante donaciones, convenios, ingresos por alquiler de las instalaciones y otros generados por la administración.

El presupuesto del CODEA para el 2021 se dividió de las siguiente forma, de acuerdo con el SIPP: de un total de 1.432 millones de colones un 55,73% correspondió a ingresos capital en lo que respecta a transferencias de capital del sector público, un 24,43% a financiamiento por medio de préstamos de Instituciones Públicas Financieras y, finalmente, un 19,84% a ingresos corrientes, de este último un 90,58% corresponde a venta de bienes y servicios, un 7,07% a ingresos no tributarios y un 2,36% a la renta de activos no financieros.

Figura 13: *Gráfico presupuesto del CODEA 2021: composición de ingresos*

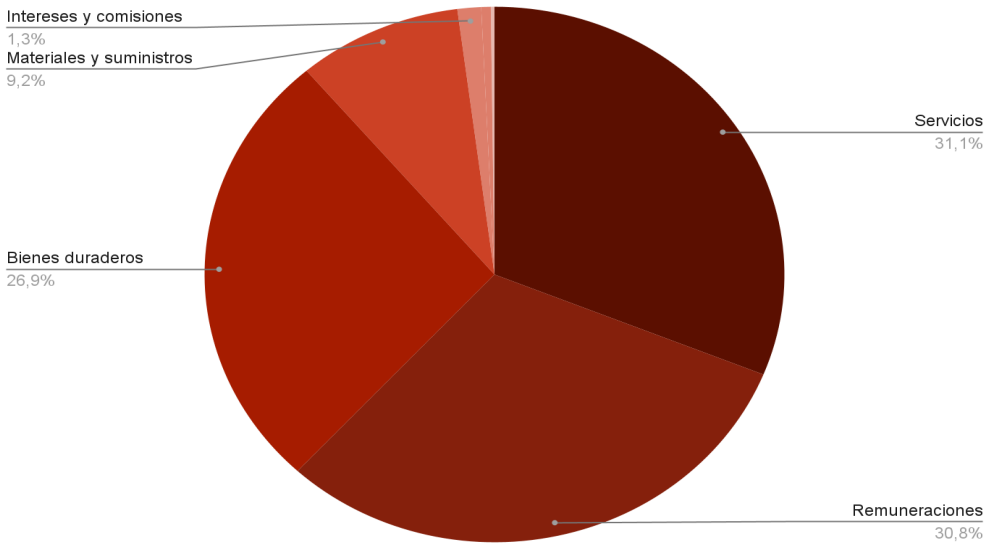


Fuente: Elaboración propia a partir de datos del Sistema de Información sobre Planes y Presupuestos (SIPP), Contraloría General de la República (2021).

En cuanto a los egresos presupuestados, un 31,09% corresponde a servicios, rubro que se compone principalmente de servicios gestión y apoyo en cuanto a servicios médicos y de laboratorio y servicios en ciencias económicas y sociales; un 30,79% de los egresos corresponden a remuneraciones de los cuales corresponden principalmente a remuneraciones básicas e incentivos salariales. Por otra parte, la partida de bienes duraderos equivale a un 26,88% del total de egresos, compuesta por la cuenta de construcciones, adiciones y mejoras y por la cuenta de maquinaria, equipo y mobiliario.

Seguidamente, se ubica la partida de materiales y suministros equivale a un 9,18% del total de egresos, compuesta principalmente por la subpartida útiles, materiales y suministros diversos. Por último, el restante 2,05% del total de egresos se compone por las partidas de intereses sobre préstamos, amortización de préstamos y prestaciones legales.

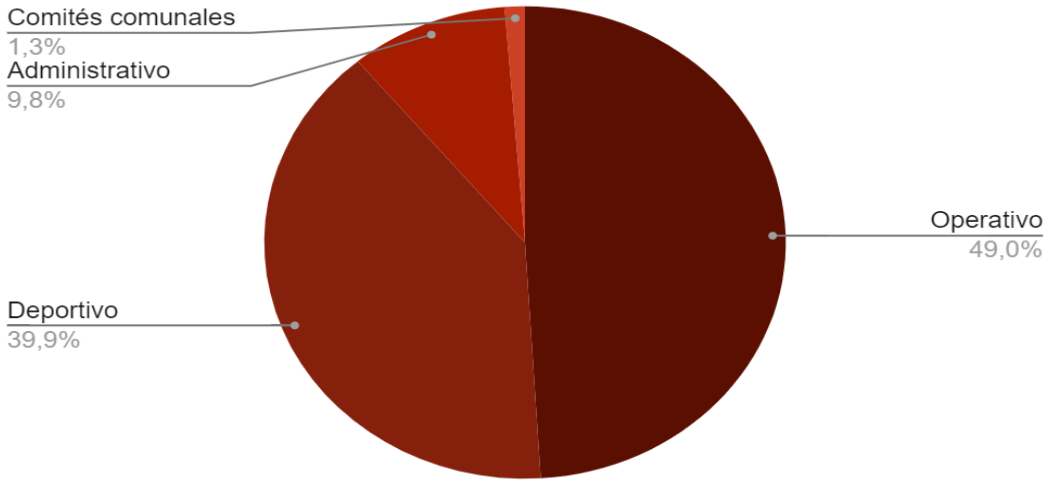
Figura 14: *Gráfico distribución de gastos por partida presupuestaria*



Fuente: Elaboración propia a partir de datos del Sistema de Información sobre Planes y Presupuestos (SIPP), Contraloría General de la República (2021).

Finalmente, al clasificar los egresos por programa, se identifica que el programa operativo es el que consume una mayor cantidad de recursos, para un total de 49,04% del total presupuestado para el 2021, seguidamente el programa deportivo con un 39,88%, el administrativo con un 9,83% y comités comunales con un 1,25%.

Figura 15: *Gráfico de distribución de gastos por programas*



Fuente: Elaboración propia a partir de datos del Sistema de Información sobre Planes y Presupuestos (SIPP), Contraloría General de la República (2021).

2.2.11 Procesos

Con el fin de obtener un entendimiento y contexto de la estructura del CODEA, se procede a realizar una descripción de sus principales procesos, para esto se procede a dividir la estructura de la siguiente manera: procesos estratégicos, procesos sustantivos y procesos de apoyo, esto con el fin de mantener homogeneidad dentro de las subáreas.

2.2.11.1 Procesos estratégicos. Son los procesos que incluyen las partes jerárquicas del CODEA, se encargan de la toma de decisiones, establecimiento de estrategias, políticas de acción y se encargan del tema de rendición de cuentas.

Junta directiva. De acuerdo con el Reglamento para la Organización y Funcionamiento del Comité Cantonal de Deportes y Recreación de Alajuela, la junta directiva se define como el "órgano colegiado nombrado por el Concejo Municipal y encargado de la dirección del Comité Cantonal de Deportes y Recreación de Alajuela" (Municipalidad de Alajuela, 2011, p. 5). Es decir, es el órgano de administración superior que se encarga de aprobar los proyectos y procesos más importantes del CODEA y, junto con la Dirección Administrativa, es la encargada de adjudicar los procesos de compra llevados a cabo y de establecer los límites económicos, así como de establecer sanciones y dictar las diferentes resoluciones. Por otra parte, también es la encargada de aprobar el Plan Anual Operativo (PAO) y los presupuestos del CODEA.

A continuación, de acuerdo con el artículo N°11 del Reglamento para la Organización y Funcionamiento del Comité Cantonal de Deportes y Recreación de Alajuela, se detalla un resumen de las principales funciones de la junta directiva:

- Establecer estrategias y políticas de acción.
- Proponer las prioridades del cantón en materia deportiva y recreativa y divulgar e informar sobre las actividades llevadas a cabo en línea de estas prioridades.
- Evaluar el desarrollo de los programas deportivos y recreativos a nivel cantonal.
- Establecer y mantener actualizada su estructura organizativa.
- Nombrar y remover al administrador del CODEA.
- Elegir y juramentar a los miembros de las comisiones y comités comunales.
- Celebrar convenios.
- Elaborar y proponer a la municipalidad los planes anuales y sus ajustes en concordancia

con los planteamientos estratégicos en materia deportiva y recreativa.

- Comprometer los fondos y autorizar los egresos referentes a los procesos licitatorios y convenios que excedan la responsabilidad del administrador.
- Elaborar y presentar ante el Concejo Municipal para su respectiva aprobación los reglamentos internos que promulgue el Comité Cantonal para la Organización y Funcionamiento interno de sus dependencias, así como las reformas que se promulguen a estos posteriormente.
- Rendir ante el Concejo Municipal informes anuales de ingresos y egresos de los recursos que le fueran asignados y generados. (Municipalidad de Alajuela, 2011, p.10-12)

Dirección administrativa. De acuerdo con información suministrada por el CODEA (Vargas, comunicación personal, 19 de mayo de 2021), la Dirección Administrativa lleva a cabo las siguientes funciones:

- Planear, coordinar, ejecutar y controlar la administración financiera, operativa, técnica e informática.
- Formulación del plan anual operativo del proceso y su programa de ejecución, la presupuestación respectiva, el desarrollo y aplicación de herramientas y metodologías de trabajo.
- Definir políticas de fiscalización y control y la coordinación permanente, tanto a lo interno con la totalidad de las unidades de trabajo de la organización, como con entes externos (Contraloría General de la República; Ministerio de Hacienda, Comités distritales entre otras).

- Dar fe, validez y cumplimiento del sistema de control interno, como en general, garantizar la efectiva fiscalización sobre las actividades desarrolladas por la institución, todo esto en términos de sus logros, costos y marco legal de observación.
- Planificar y desarrollar de los ingresos, incorporados a la administración del CODEA y los egresos a cargo (presupuesto, contabilidad, tesorería y proveeduría).
- Evaluar los resultados de la aplicación de esas políticas y en general el plan operativo.
- Informar frecuentemente a las autoridades del CODEA el rendimiento alcanzado por las diferentes áreas de trabajo.
- Supervisar y coordinar al personal, así como definir sus respectivos roles.

2.2.11.2 Procesos sustantivos. Estos procesos corresponden a la "razón de ser" del comité y hacen operativos los planes del CODEA.

Dentro de los procesos sustantivos del comité, se encuentran los siguientes:

Deporte y recreación. Este proceso está a cargo del Área Deportiva, que tiene dentro de sus funciones la coordinación con los entrenadores de las diferentes ramas deportivas y diferentes organizaciones relacionadas, así como con los instructores de los programas recreativos.

A la fecha, el CODEA cuenta con un total de 22 diferentes disciplinas asociadas, que sirven a una población de 1.910 personas, mediante la atención de un equipo de 76 entrenadores. Estas disciplinas pertenecen a 46 federaciones y organizaciones y cuenta con un aproximado de 92 instructores distribuidos en cada una de ellas. A continuación, se detallan las disciplinas, la cantidad de atletas y de entrenadores:

Tabla 4: *Disciplinas atletas y entrenadores del CODEA*

Disciplina	Cantidad de entrenadores	Cantidad de atletas
Ajedrez	3	118
Atletismo	3	90
Baloncesto	5	97
Balonmano	4	65
Béisbol	4	58
Boxeo	3	82
Ciclismo R/M	3	42
Fut sala	8	210
Fútbol	6	137
Gimnasia artística	1	78
Gimnasia rítmica	2	72
Halterofilia	2	26
Judo	3	70
Karate Do	2	70
Natación	5	107
Patinaje	3	59
Taekwondo	4	153
Tenis	3	104

Tenis de mesa	3	62
Triatlón	3	78
Voleibol	5	105
Voleibol de playa	1	27
Total	**76**	**1.910**

Fuente: Elaboración propia.

Todas esas disciplinas forman parte del Programa de Juegos Deportivos Nacionales, el cual es catalogado como uno de los más demandantes. Este programa va dirigido a toda la comunidad residente del cantón central de Alajuela entre el rango de edad de 6 a los 23 años.

Actividad física y salud. El CODEA también ha estado incursionando en un nuevo programa que le permita, además, generar ingresos adicionales, este programa se denomina "Plan piloto de profundización y ampliación del vínculo remunerado del CODEA (CODEA EXPERIENCE)", el mismo tiene el objetivo de atraer personas de edad adulta con actividades a un bajo costo, orientado al desarrollo integral de las personas.

Por otra parte, también se cuenta con programas de recreación, los cuales amplían el público meta y sus objetivos. A continuación, se muestra un resumen de los programas de recreación:

Tabla 5: *Programas de Recreación de Alajuela*

Nombre del proyecto	Objetivo
Programa de Adulto Mayor	Mejorar los hábitos de actividad física y la calidad de vida de los adultos mayores.
CODEA Especiales	Brindar un espacio de aprendizaje, recreación, salud y competitividad para la población en situación de discapacidad en diferentes disciplinas deportivas y actividades recreativas.
Acondicionamiento físico y ejercicios funcionales	Mejorar la condición física de los participantes mediante ejercicio de resistencia y fuerza.
Subpestaña piscina municipal y enseñanza de la natación	Promover la actividad física y el aprendizaje de la natación.
Zumba CODEA	Ejecutar el programa ZUMBA CODEA para que todos los ciudadanos del cantón puedan acceder mediante el baile, música e integración social a la práctica de una actividad recreativa que mejore su estado de salud.

Fuente: Elaboración propia.

Por otra parte, el área deportiva también cuenta con una encargada de musculación y una fisioterapeuta, que ayuda a mantener la salud y seguridad de cada uno de los integrantes de las disciplinas.

Gestión comunal. Los comités comunales son parte de la estructura organizativa del comité cantonal y son los órganos encargados de establecer el enlace entre el comité cantonal y las respectivas comunidades. De acuerdo a lo anterior, CODEA tiene un rol de supervisor en las diferentes actividades de los comités comunales.

Los procesos de CODEA en relación con los comités comunales se establecen por medio del artículo N°7 del Reglamento para la Organización y Funcionamiento del Comité Cantonal de Deportes y Recreación de Alajuela, estos se enfocan en la supervisión.

A continuación, se puntualizan algunas de las actividades de supervisión llevadas a cabo por el CODEA:

- Recibir en el mes de junio de cada año los planes de trabajo y presupuesto del año inmediatamente posterior para ser aprobados, y establecer controles durante la ejecución.
- Recibir informes de labores, de ingresos y egresos de forma mensual.
- Exigir cuando crea necesario, el archivo de gestión administrativo y financieros, en relación con informes relacionados con la gestión.
- Recibir por parte de los tesoreros de los Comités Comunales el libro de tesorería, incluyendo las facturas y comprobantes para su revisión.
- Brindar recomendaciones de las revisiones, y no realizar gestiones económicas en caso de que se presenten dudas o confusiones en dichas revisiones.

2.2.11.3 Procesos de apoyo. Las áreas de apoyo corresponden a aquellas que tienen como fin dar soporte a los procesos operativos tanto de manera administrativa en general, como en materia de mantenimiento y limpieza. A continuación, se detallan los procesos correspondientes a esta área de acuerdo con el modelo de negocios del CODEA:

Gestión administrativa. La gestión administrativa se subdivide en varios procesos, los cuales son:

1. El proceso de secretaría: El área de secretaría soporta principalmente temas administrativos y de atención al público en general, dentro de las actividades se tienen:

    - Realizar trabajos relacionados con la transcripción de documentos, administrativos y documentos de la junta directiva.
    - Redactar cartas, cuadros, informes, reportes y otros.
    - Recepción y registro de correspondencia.
    - Ordenamiento, clasificación y archivo de documentos.
    - Asistir a las sesiones de la junta y levantar las actas respectivas.
    - Administrar y custodiar toda la documentación producida y acordada por la junta.
    - Transcribir, comunicar y/o notificar los acuerdos de la junta directiva.
    - Controlar el cumplimiento de los acuerdos de la junta directiva.
    - Brindar la asistencia administrativa requerida por las distintas instancias del comité.
    - Realizar los trámites correspondientes para las renovaciones de personería jurídica del comité y de los entes deportivos.
    - Recepción, distribución y control de la correspondencia recibida y enviada al comité.
    - Controlar el uso racional de los materiales y suministros de oficina, por parte de los funcionarios.

- Aplicación de encuestas de satisfacción al cliente.
- Elaborar y foliar los expedientes producto de temas solicitados.

2. Procesos de recursos humanos: Se encarga de organizar, planificar y administrar las distintas tareas y acciones relacionadas con el personal que integra el CODEA. A continuación, se detallan las actividades de este proceso:
    - Gestionar y elaborar el pago de planillas.
    - Participar en la ejecución de labores en el campo de los recursos humanos orientadas a la apertura, actualización y custodia de los expedientes personales del recurso humano de la institución.
    - Confeccionar los carnés de identificación para los funcionarios, así como llevar los controles de los funcionarios que extravían o presentan anomalías en su uso, pasar sus reportes para llevar a cabo el debido proceso.
    - Llevar el control de asistencia y presentación personal, emitir los reportes y suministrar información para la ejecución de los diferentes procesos disciplinarios.
    - Llevar el control de las actividades relacionadas con vacaciones de los empleados.
    - Confeccionar documentos relacionados a administración de personal como constancias de salario, constancias de tiempo servido, trámite de cuenta bancaria para funcionarios de nuevo ingreso.
    - Colaborar con el área de administración de salarios en la realización de análisis, estudios y cálculos aritméticos de diversas inconsistencias de los funcionarios,

revisión de prestaciones, realización de oficios de pago de las instituciones, asistir en mantener actualizada la información del sistema de planillas, entre otras actividades técnicas que se le soliciten.

- Colaborar en la gestión de análisis estadístico y presentación de informes.
- Asistir a la dirección administrativa en actividades relacionadas con los recursos humanos.
- Rendir informes técnicos de sus labores.

Gestión financiera. Esta área de apoyo se considera una de las más relevantes para el CODEA, debido a que lleva a cabo las actividades contables y presupuestarias del comité que permiten la toma de decisiones importantes. Los siguientes corresponden a los principales subprocesos de gestión financiera:

1. Proceso de contabilidad: Las funciones de esta área consisten en llevar a cabo los registros contables y financieros del CODEA. Se considera un área relevante ya que tiene efecto sobre todas las actividades operativas, además de que la información que produce tiene efectos de cumplimiento, legales y en la toma de decisiones. A continuación, se detallan sus actividades:
    - Elaboración de planillas administrativas, servicios profesionales, y viáticos de atletas.
    - Cálculo de embargos y anualidades.
    - Elaboración de la planilla del INS, C.C.S.S. y de aguinaldos.
    - Cálculo de liquidaciones (preaviso, cesantía, vacaciones y aguinaldo).
    - Ejecución y control del registro en orden cronológico de las operaciones

contables, presupuestarias y de costos.

- Preparar los estados financieros e informes específicos, para el cumplimiento del registro contable de los ingresos y egresos.
- Análisis de las diversas cuentas del activo, pasivo y patrimonio.
- Actualización de libros contables y libro de activos.
- Dirigir, controlar y supervisar la actividad de control presupuestario.
- Recopilar, analizar y aplicar las fuentes de ordenamiento jurídico-administrativo con relación a la materia presupuestaria, contable y de contratación administrativa.
- Recopilar, analizar y aplicar las fuentes de ordenamiento jurídico-administrativo con relación a la materia contable (NICSP y NIIF).
- Determinar recursos disponibles para la distribución de los recursos en los diferentes procesos para el presupuesto ordinario.
- Velar por la adecuada asignación y ejecución de los recursos fijados por la ley.
- Elaborar informes trimestrales sobre los movimientos de los egresos presupuestarios y los remanentes.
- Garantizar el mantenimiento actualizado de los registros contables y la provisión de los estados financieros comprensibles y oportunos para la toma de decisiones.
- Implementar todas las normas vigentes, tales como NICS y NIIF.
- Archivar y controlar el consecutivo de cheques de cada mes.

- Desarrollar labores de gestión de cobro a usuarios, patrocinadores u otros.

2. Proceso de presupuesto: Las actividades que se realizan para llevar a cabo el proceso presupuestario son:

    - Cálculo de egresos, ingresos y salarios presupuestados.
    - Balance de presupuesto.
    - Cálculo de presupuesto ordinario y extraordinario.
    - Liquidación: preliquidación y liquidación de presupuestos.
    - Flujo de caja: movimiento de egresos e ingresos.
    - Reporte de ingresos y egresos por fecha y centro de costos.

    Además, el proceso de presupuesto se divide en dos, esto debido a los periodos de realización y entrega, mensual y anual:

    a. Presupuesto mensual: Se preparan los cálculos presupuestarios mensuales, así como los reportes que se envían al área de contabilidad con los resultados de dicha información.

    b. Presupuesto anual: El manejo del presupuesto se desarrolla sobre la metodología del Gobierno de Costa Rica. El presupuesto es realizado tomando como base los documentos de períodos preliminares, dentro de los cuales están las solicitudes de compra, órdenes de compra, facturas de compra, asientos manuales y pagos efectuados.

3. Procesos de tesorería: Hace referencia a los procesos ligados a órdenes de pago y compra, cheques, inversiones, liquidaciones, adelantos de viáticos, transferencias bancarias y todo lo que tiene que ver con el efectivo del CODEA. Las actividades específicas se detallan a continuación:

- Procesar mediante el sistema las órdenes de pago.
- Realizar pagos referentes al cumplimiento legal, a proveedores, de planilla, servicios públicos, proveeduría, de viáticos, etc.
- Controlar y dar seguimiento del libro de bancos.
- Seguir los movimientos de dinero y de los cheques que se emiten.
- Consultar créditos, depósitos, débitos y traslados.
- Procesar el control de la caja chica.
- Preparar y mantener un detalle diario de facturación.
- Procesar la solicitud y liquidación de viáticos.

Hay que destacar que esta última actividad tiene como objetivo cumplir con los requisitos y procedimientos para la solicitud de adelanto, pago y reintegro de gastos de viáticos, así como su liquidación, esto de acuerdo con las disposiciones del CODEA y la normativa nacional vigente.

Gestión de compras. Las compras que se realizan corresponden a las necesidades de las diferentes áreas, disciplinas deportivas o departamentos y se relacionan con insumos, como lo son implementos deportivos o de mantenimiento de las instalaciones deportivas y administrativas. Las compras locales son realizadas por medio del SICOP, a continuación, se detallan los subprocesos y actividades:

1. Procesos generales de compras:

- Mantener actualizado el sistema de control de ejecución presupuestaria que permite tomar decisiones oportunas en cuanto a compras, modificaciones u otros movimientos.
- Registro y control de órdenes de compra, contratos, recibos telefónicos, recibos eléctricos, planillas, detalles de pagos del departamento de recursos humanos y las nóminas, para la debida autorización del pago.

2. Procesos específicos de compras:

- Cada una de las unidades compradoras son las encargadas de realizar la solicitud de compra, estas pueden ser los comités comunales, junta directiva, dirección deportiva, área operativa, dirección administrativa, proyectos municipales. Las solicitudes las generan mediante un oficio (desde el SICOP) y lo envían a las personas que operativizan las compras.
- La Junta Directiva del CODEA y la Dirección Deportiva son quienes realizan la compra, operativizan la compra, y elaboran la decisión inicial, las mismas verifican si el oficio procede o no.
- En el proceso de compras está la elaboración y publicación del cartel por medio del sistema SICOP, esta actividad es realizada por las áreas de Proveeduría, Dirección Administrativa y la Dirección Deportiva.
- Tanto la Dirección Administrativa como Proveeduría, son las unidades técnicas que van a tener a cargo el estudio de las ofertas y la respectiva recepción. Cabe señalar que una vez recibidas las ofertas en la página del SICOP entran en un periodo de estudio, ese periodo de estudio lo determina el cartel de contratación publicado.
- Una vez realizado el estudio la Dirección Administrativa o Proveeduría, son las

unidades técnicas que van a tener a cargo la publicación del acto final de adjudicación.

- El área de proveeduría gestiona la recepción de los productos o servicios que se reciben de manera física en el CODEA, cuando se recibe el producto se verifica que las especificaciones técnicas del producto se cumplan.

- La orden de compra se registra desde el SICOP y se sincroniza con SAP para que el registro de esta quede en la base de datos, y luego se registra la entrada de mercadería del proveedor (si es una compra interna, se registra la factura proveedor o la cuenta por pagar; si es una compra al exterior, se registra los precios de entrega el oferente).

- Posteriormente al pago, el área de cuentas por pagar que se encuentra en contabilidad registra el proceso de pagos a proveedores desde SAP. Esto por medio de pagos efectuados.

- En el SICOP se da la opción de enviar al adjudicatario el comunicado de que se recibió el producto o servicio conforme y que por lo tanto ya se finiquita el contrato.

- Se cierra el expediente en el SICOP y el proceso queda archivado.

3. <u>Procesos de compras por caja chica:</u>

- La jefatura del departamento de finanzas crea en SAP una solicitud de compra con el detalle de artículo(s) o servicio(s) que se requiere(n).

- Primeramente, se debe crear la solicitud de compra en SAP y, posteriormente, se debe enviar a autorización, este documento requiere la autorización del Director Administrativo y en caso de no estar presente, la podrá otorgar al contador. Si se rechaza la solicitud de compra, se finaliza el proceso.

- Al autorizar la solicitud de compra, SAP notifica al solicitante para que pueda crear el

documento en firme.

- Creada la solicitud de compra, SAP notifica a la Dirección Administrativa y clasifica la compra en caja chica o por el proceso de orden de compra. Adicional establece el nivel de urgencia.
- Las compras por caja chica no afectan al inventario y la factura se envía como parte del reintegro para su registro por parte de finanzas.
- Posterior a ello viene el proceso de devolución de producto (nota de crédito).
- Cuando el producto se rechaza, el sistema SAP notifica a logística, que en el CODEA está representado por la jefatura de cada disciplina, para que realicen una transferencia de stock a la bodega de rechazado.
- Si la entrada no se ha convertido en factura y el proveedor repone el producto, entonces el encargado de logística registra la entrada como devolución, este proceso abre la orden de compra y efectúa el ingreso del nuevo producto.
- Si la factura ya está creada y el proveedor repone el producto (sin emitir una nueva factura), logística realiza una salida del producto entregado y una entrada del nuevo producto.
- Si el proveedor envía una nota de crédito, Finanzas localiza la factura y copia la nota de crédito por la cantidad que corresponda.

Gestión de mantenimiento. Está conformado por los subprocesos de mantenimiento, misceláneos y seguridad, son quienes se encargan del cuido, mantenimiento y mejora de las instalaciones del comité.

Cabe resaltar en este punto que el CODEA administra un complejo deportivo compuesto por: un terreno con una extensión de 3 hectáreas, un boulevard, un sendero, cinco canchas de fútbol, dos canchas de tenis, una pista de atletismo, una piscina olímpica, un gimnasio, un aula de capacitaciones, un aula de entrenamiento de ajedrez, vestidores ubicados en la piscina, dos canchas de béisbol, dos canchas de baloncesto bajo techo, un parque infantil, dos canchas de voleibol de playa y dos sodas, de las cuales todas requieren del área de gestión de mantenimiento para poder recibir a los atletas y público en general.

Con base en lo mencionado, a continuación, se detallan los subprocesos de cada una de las subáreas:

1. Procesos de mantenimiento: Esta área se considera de apoyo dado que su función principal es mantener todas las estructuras y espacios del CODEA en las condiciones óptimas para que se puedan realizar las actividades para las cuales han sido destinadas. Sus actividades incluyen:

a. Procesos de mantenimiento general:

- Esta área se encarga de ejecutar las actividades de construcción y mantenimiento de edificaciones y de carpintería, reparar o reconstruir y realizar cualquier actividad que permita finalizar las obras.
- Realizar diferentes actividades de mantenimiento relacionadas con la actividad de pintura y otras similares, además de mantener en adecuadas condiciones el uso del equipo y las herramientas.
- Ejecutar actividades de albañilería y carpintería.
- Instalación, reparación y mantenimiento de tuberías, hierro o tramos de redes.

- Ejecutar labores variadas y simples de electricidad e iluminación.
- Realizar trabajos en soldadura.
- Gestionar el inventario de bienes y herramientas de la bodega institucional de aprovisionamiento de materiales para labores de mantenimiento.
- Realizar informes periódicos de inventarios de herramientas y materiales.
- Realizar los traslados requeridos por medio de vehículos institucionales.
- Rendir informes a la Dirección Administrativa sobre las labores de mantenimiento, inventario y construcción de obras de la institución.
- Ejecutar labores de chapeo, limpieza y ornato de zonas verdes, calles y otros sitios públicos del polideportivo, con el fin de mantener las instalaciones limpias y libres de focos de contaminación y malos olores.
- Ejecutar labores de acarreo, empaque, carga y descarga de materiales y residuos.
- Realizar instalaciones o reparaciones varias.

b. <u>Procesos de mantenimiento de piscina:</u>

- Realizar labores de limpieza y aspirado de piscina (limpieza de los tanques de agua de la piscina).
- Operar el cuarto de filtros y máquinas de la piscina.
- Aplicación de los productos químicos para el debido mantenimiento de la piscina.
- Realizar los análisis químicos del agua de la piscina para determinar si los parámetros de los diferentes productos se encuentran en los niveles adecuados.
- Atender en cualquier momento las emergencias que se presenten con las condiciones

inadecuadas del agua de la piscina.

- El trabajo de mantenimiento debe realizarse en un horario en el cual no se utilice la piscina, por lo que son labores que se realizan durante el horario nocturno.

2. Procesos misceláneos:

- Realizar limpieza y aseo en oficinas, bodegas, edificios, así como en sus áreas adyacentes.
- Solicitar cuidar y darle el debido uso a los utensilios de trabajo que se le asignan.
- Realizar limpieza y aseo de escritorios, estantes, mostradores, y equipos de uso de las oficinas.
- Desinfectar y esterilizar baños y vestidores.
- Recoger y transportar basura y desechos.
- Suministrar información sencilla al público que visita la institución.

3. Procesos de seguridad: El área de seguridad es de gran relevancia dentro del CODEA, se considera un área de apoyo, ya que el fin principal de la misma es que tanto las personas como las estructuras no presenten alguna situación que represente algún peligro, por lo que sus principales funciones son la vigilancia y protección de los espacios del comité. A continuación, se detallan sus actividades principales:

- Realizar actividades de seguridad y vigilancia, protección de bienes, personas y mantenimiento del orden, mediante el control de acceso y salida de personas y vehículos del polideportivo, así como mediante rondas, con el fin de salvaguardar las instalaciones.

- Realizar rondas de vigilancia en los alrededores del polideportivo a pie o mediante el uso de motocicletas o bicicletas.
- Actualización y registro en bitácora de eventos destacables durante la guardia.
- Realizar monitoreo constante del conjunto de cámaras de seguridad de la institución.
- Suministrar información sencilla al público que visita en el polideportivo, tales como direcciones, horarios, lugares de atención y reglas de convivencia dentro del inmueble.
- Organizar, dirigir, inspeccionar y administrar los servicios y recursos de seguridad disponibles y el personal.
- Identificar, analizar y evaluar situaciones de riesgos que puedan afectar a la vida e integridad de las personas y al patrimonio del CODEA.
- Planificar, organizar y controlar las actuaciones precisas para la implantación de las medidas conducentes a prevenir, proteger y reducir la manifestación de riesgos de cualquier naturaleza con medios y medidas precisas, mediante la elaboración y desarrollo de los planes de seguridad aplicables al CODEA.
- Controlar el funcionamiento y mantenimiento de los planes de seguridad aplicables al CODEA.
- Controlar el funcionamiento y mantenimiento de los sistemas de seguridad.
- Validar provisionalmente, hasta la comprobación por parte de la administración, las medidas de seguridad en lo referente a su adecuación a la normativa de seguridad.
- Comprobar que los sistemas de seguridad se encuentren debidamente instalados.
- Comunicar a las fuerzas y cuerpos de seguridad competentes de las circunstancias o informaciones relevantes para la seguridad ciudadana, así como de los hechos delictivos

de los que tenga conocimiento en el ejercicio de sus funciones.

- Llevar a cabo la interlocución y enlace con la administración, especialmente con las fuerzas y cuerpos de seguridad, respecto de la función de seguridad integral de la entidad, en relación con el cumplimiento normativo sobre gestión de todo tipo de riesgos.
- Comprobar los aspectos necesarios sobre el personal que, por el ejercicio de las funciones encomendadas, precise acceder a áreas o informaciones, para garantizar la protección efectiva de su entidad y los usuarios.
- Generar protocolos institucionales de abordaje de problemáticas institucionales relacionadas con la seguridad.

Gestión de ventas. El proceso de ventas de CODEA, se compone de tres subprocesos, los cuales son ventas locales, ventas de servicios y ventas de tienda por medio de la página, los cuales se describen a continuación:

1. Proceso de ventas locales: Este proceso corresponde al proceso general que se lleva a cabo en el sistema SAP para las ventas en las tiendas o bodegas físicas del CODEA:

- El primer paso corresponde a la recepción de órdenes de compra por parte de los clientes. Para ello, la persona encargada busca al cliente en SAP; si no existe debe registrarse de acuerdo con los protocolos que dicta el Ministerio de Hacienda.
- Posterior a ello, la persona encargada de ventas en el CODEA genera una orden de venta en SAP con los artículos de inventario correspondientes.
- En el momento de crear la orden de venta, se validan las cantidades en la bodega, ya sea de la tienda o de cada disciplina deportiva. Luego, en caso de ser aceptadas, se

generará una entrega de mercancías y la factura del cliente.

- Finalmente, se registra el pago (se trabaja de contado, por ende, se registra el ingreso del dinero de inmediato a SAP, afectando bancos).

- Al final del día la persona encargada deberá generar un cierre de ventas.

2. Proceso de ventas tipo servicios: Es el proceso que considera la venta de servicios. El proceso se inicia cuando algún cliente realiza una adquisición de servicios que genera una orden de ventas. Seguidamente la persona encargada de la tienda debe verificar que cada cliente se encuentra registrado en el sistema SAP Business con los campos obligatorios para la emisión de la factura electrónica, o bien proceder a su registro. Cuando se acepta la orden de venta se genera la entrega del artículo y al mismo tiempo se produce la factura del cliente para el registro contable en SAP y el auxiliar de ventas. Finalmente, al terminar la jornada laboral la persona encargada de ventas debe generar un cierre de caja de las ventas realizadas.

3. Proceso de ventas locales en tienda: Es el proceso que contempla las ventas por medio del comercio electrónico, en este caso, utilizando la página web del CODEA. El proceso se inicia cuando algún cliente realiza una compra por medio de la web de la entidad, para lo cual la persona usuaria debe estar previamente registrada. Posterior a ello, el encargado de la tienda debe verificar que cada cliente se encuentra registrado en el sistema SAP Business con los campos obligatorios para la emisión de la factura electrónica, o bien proceder a su registro. Luego de lo anterior, se genera una orden de ventas en el sistema y se valida la cantidad solicitada contra la registrada en la bodega de la tienda o de cada disciplina. Cuando se acepta la orden de venta, se genera la entrega del artículo, y al mismo tiempo se genera la factura del cliente para el registro contable en SAP y en el auxiliar de ventas. Finalmente, al finalizar la jornada laboral el

encargado de ventas debe generar un cierre de caja de las ventas realizadas.

4. Proceso de caja chica: Este proceso comprende tres niveles, cada uno de los cuales se detalla a continuación:

- Nivel 1: En él, se crean los vales de caja iniciales asignados a un empleado, dicha creación comprende 2 autorizaciones.
- Nivel 2: Corresponde al proceso de liquidación y es por medio del cual se desglosan las facturas de gastos asociadas al vale de caja creado en el nivel 1. En este nivel el proceso requiere de dos jerarquías de autorización y un nivel de aprobación.
- Nivel 3: Este nivel hace referencia a los reintegros de caja chica en el cual se desglosan aquellas liquidaciones autorizadas y aprobadas correctamente. Las liquidaciones se agrupan y se crea un reintegro, luego se genera el pago correspondiente. Tiene un nivel de autorización.

5. Proceso de liquidación: En este proceso se crean las facturas de gastos asociadas a los vales de caja. Si se va a crear una liquidación sin carga de vale de caja asociado, se debe iniciar con el llenado de la información requerida, que son el proyecto, cuenta presupuestaria de gastos y el empleado a quien se le asignará la carga de facturas.

Una vez listo el proceso de vales de caja se procede a generar los documentos ligados a la factura (PDF y XML de la factura). Después, se realiza el envío a Hacienda del XML de la factura electrónica que corresponda. Cabe señalar que, si la respuesta de Hacienda es numérica, el documento fue aceptado y aprobado, pero si la respuesta es diferente de la numérica, entonces hubo un error en el proceso con Hacienda.

El envío del XML para Hacienda puede hacerse en cualquier momento antes de la aprobación definitiva del documento de liquidación. Una vez autorizada y aprobada la

liquidación, el proceso estará completo.

6. Proceso de reintegros de caja chica: En el sistema existe una sección de reintegros, la cual contiene las liquidaciones autorizadas y aprobadas, listas para ser asociadas a un reintegro.

Inicialmente, se deben asociar las liquidaciones con un reintegro por medio del sistema y posteriormente se envía la petición de autorización. Una vez aprobado, se crea el asiento que corresponde y el número de pago asociado, con lo cual se completa el reintegro. Luego, se realiza el pago por medio de cheque, el cual emite el contador.

7. Procesos de contabilidad: Se emiten los reportes referentes a los activos, saldos mensuales de ingresos y egresos, así como la preparación de asientos contables y estados de información financiera. Los procesos específicos se detallan a continuación:

- Asientos de diario.
- Procesos.
- Conciliación bancaria.
- Registro de activos.
- Cierres.
- Estados financieros.
- Consultas por cuentas, movimientos por cuenta y consecutivos de asientos.

Gestión de proveeduría. Proveeduría es la unidad encargada de generar todos los reportes relacionados con proveedores y procesos administrativos (trámites, adjudicaciones por tipo, presupuesto ejecutado en la parte de proveeduría y detalle de compras realizadas). Esta es una lista detallada de las actividades de esta área:

- Registro de proveedores.
- Registro de procesos de contratación administrativa por tipo de contratación.
- Registro de decisión inicial del proceso de contratación administrativa.
- Seguimiento del proceso de contratación administrativa.
- Establecimiento de rubros de calificación particularizadas para cada proceso de contratación administrativa.
- Calificación de ofertas.
- Adjudicación de ofertas.
- Registro de archivos externos, como garantías de las compras o facturas.

Debido a la naturaleza de sus funciones, también se incluye el subproceso de inventario y el subproceso de pago a proveedores:

1. Proceso de inventario: Consiste en la gestión de las bodegas administrativas y deportivas del CODEA, en relación con los movimientos de entradas, salidas y traslados de artículos. Algunas de las actividades que se realizan en este proceso son:

- Control de entradas de inventario.
- Control de salidas de inventario.
- Traslados de inventario.

- Conteo físico de unidades.
- Solicitud de material nuevo.
- Ajustes de inventario.
- Creación de códigos de artículos.

2. Proceso de pago a proveedores: Se encarga de la administración de los pagos con los proveedores de bienes y servicios para controlar los egresos y permitir generar información oportuna y veraz sobre las obligaciones contraídas por CODEA. Dentro de este proceso se llevan a cabo las siguientes actividades:

- Pagos parciales, y totales, adelantos de pago.
- Conciliaciones de proveedores.

Capítulo 3

Marco metodológico, presentación y análisis de los resultados del trabajo de campo

3.1 Metodología de la investigación

Esta investigación se desarrolló bajo la modalidad de seminario de graduación y diseñó una propuesta de fortalecimiento del control interno del CODEA con base en mejores prácticas internacionales. A continuación, se muestra la estructura de la investigación.

3.1.1 Paradigma de la investigación

El paradigma de la investigación se expone de forma sociocrítica, debido a que analiza la situación particular del CODEA y la comprende mediante una postura crítica, para proponer las mejoras pertinentes. Para ello, se utilizan de referencia dos marcos internacionales de buenas prácticas y comprensión del funcionamiento del control interno que mantiene el comité.

3.1.2 Enfoque de la investigación

La investigación presenta un enfoque mixto con preponderancia cualitativa (cuan-cual). Es importante recalcar que este enfoque se escogió por la necesidad de la institución de fortalecer su sistema de control interno, por lo cual se considera importante realizar un acercamiento primario desde una perspectiva cualitativa utilizando por un lado técnicas de recolección de datos como la observación, la revisión de documentos y las entrevistas, para proceder al análisis de datos e interpretar los resultados de la contextualización del entorno de CODEA.

3.1.3 Tipo y diseño de investigación

El presente estudio se fundamenta por medio de una investigación descriptiva de carácter aplicado, ya que no se va a enfocar solo en la parte teórica, sino también en integrar los conocimientos adquiridos, para diseñar la propuesta de fortalecimiento que se le va a proponer al CODEA.

Para Sampieri et al (2014), la investigación descriptiva "busca especificar las propiedades, las características y los perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis" (p. 92). Es decir, lo que se pretende es describir cómo son y cómo se manifiestan diferentes fenómenos o situaciones.

En cuanto al concepto de investigación aplicada, Tomayo y Tomayo (2003) manifiestan que: ". . . busca confrontar la teoría con la realidad. Es el estudio y aplicación de la investigación a problemas concretos, en circunstancias y características concretas" (p. 43). En resumen, lo que se quiere es transformar un problema concreto por medio de la puesta en práctica de la teoría.

3.1.4 Técnicas de recolección de información

Para el desarrollo de este trabajo se utilizaron las siguientes técnicas:

- Entrevista en línea: se realizó una reunión con el Director Administrativo del CODEA, utilizando un entorno virtual para videollamada. Para llevar a cabo la misma se definió una guía de preguntas.
- Encuesta: la encuesta consistió en la aplicación de una serie de preguntas mediante formularios en línea, que tuvieron como fin recopilar información que sirviera de insumo para el análisis y diagnóstico de las necesidades actuales del CODEA en cuanto al fortalecimiento del control interno.

3.1.4.1 Fuentes de información. Las fuentes primarias de información que se utilizaron son: las leyes y reglamentos que rigen a la entidad, informes de auditorías realizadas al CODEA, así como información de entrevistas y consultas al personal. Dentro de las fuentes secundarias se incorporaron libros, artículos, revistas, indicadores económicos e información de la Contraloría General de la República.

3.1.5 Metodología de recolección de información

La metodología de recolección de información hace referencia al proceso desarrollado para captar la información de interés, en donde se define la unidad de estudio, población de interés, análisis teórico de los marcos de referencia y construcción del instrumento por utilizar, incluyendo la técnica de su aplicación.

3.1.5.1 Unidad de estudio. La unidad de estudio corresponde al sujeto de interés de la investigación, en este caso se trata de la unidad de Control Interno actual del CODEA, debido a que es de donde se requiere información y de la cual se obtienen los datos.

3.1.5.2 Población de interés. Se determinó que la población de interés está compuesta por los funcionarios de la Dirección Administrativa, del Área Administrativa y Financiera, la jerarca del Área Operativa y las personas jerarcas del Área Deportiva.

Debido a ello, se realizó un censo, para cuantificar la población impactada. En él, los sujetos informantes correspondieron a las mismas personas funcionarias de la población de interés. La técnica de recolección fue el uso de cuestionarios en la plataforma de formularios de Google[3].

[3] Es un software gratuito de administración de encuestas ofrecido por Google. Permite crear encuestas en línea junto con otros colaboradores y la información recopilada se guarda automáticamente en una hoja de cálculo de Google.

3.1.5.3 Fases del trabajo de campo. Las fases del trabajo de campo se constituyeron en 8 de la siguiente manera:

1. Primera fase: Se realizaron reuniones preliminares con funcionarios del CODEA y el intercambio de información.
2. Segunda fase: Se llevó a cabo la indagación de los informes de la entidad.
3. Tercera fase: Se revisaron las fuentes primarias y secundarias para obtener el marco teórico y contextual.
4. Cuarta fase: Se comprendió el diseño de las encuestas y entrevistas.
5. Quinta fase: Se aplicaron los instrumentos de recolección de información.
6. Sexta fase: Se realizó el procesamiento y análisis de los datos obtenidos.
7. Séptima fase: Se realizaron las conclusiones basadas en la información obtenida.
8. Octava fase: Se utilizaron las conclusiones del trabajo de campo para formular la estrategia de mejora de control interno para CODEA.

3.1.5.4 Instrumento de recolección de información. Se planteó la elaboración y aplicación de cuestionarios estructurados de acuerdo con los cinco componentes de control interno: 1) entorno de control, 2) evaluación de riesgos, 3) actividades de control, 4) información y comunicación y 5) actividades de supervisión. Además, se contemplaron procesos y prácticas de gestión establecidas en COBIT 5.

Se dirigieron a funcionarios seleccionados de forma específica de acuerdo con la naturaleza de cada uno de los formularios.

Para su elaboración y aplicación se llevaron a cabo las siguientes actividades: a) análisis de COSO 2013 y COBIT 5, b) creación de preguntas por principios de COSO y prácticas de gestión COBIT, c) revisión de preguntas acorde a la finalidad del proyecto y d) aplicación del instrumento de recolección de información.

a) Análisis COSO 2013 y COBIT 5. Tanto el Marco de Trabajo Integrado para Control Interno COSO 2013 como COBIT 5, son marcos internacionales de buenas prácticas que ayudan y orientan a cualquier entidad a fortalecer sus sistemas de control interno, con lo cual COBIT 5 brinda un refuerzo en la gestión de las tecnologías de información.

A raíz de la pandemia del COVID 19, muchas entidades se vieron obligadas a modificar sus procesos tradicionales por procesos que involucraban mucho más las tecnologías de información, como lo es el cambio de reuniones presenciales a reuniones virtuales, uso de espacios en la web de trabajo colaborativo, uso de herramientas en línea de seguimiento de cargas de trabajo, ventas y compras en línea y demás.

En esta línea, el CODEA es una institución que se encuentra en proceso de cambio, ya que recientemente inició con el proceso de migración de sus sistemas informáticos hacia otro ERP (Entreprise Resource Planning), esto implica capacitaciones de personal, asignaciones de roles, aseguramiento de la información y traslado de la información.

Aunado a esto, existen los señalamientos realizados por parte de la Auditoría Interna[4] de la Municipalidad de Alajuela sobre diversas debilidades de la entidad, como por ejemplo en

[4] INFORME 08-2019: Evaluación sobre el uso, seguridad y controles del sistema informático que utiliza el Comité Cantonal de Deportes y Recreación de Alajuela.

INFORME 10-2020: Estudio de carácter especial sobre la administración del Comité Cantonal de Deportes y Recreación de Alajuela, periodo 2019.

temas de planificación estratégica, normativa interna desactualizada, actividades de control insuficientes para la totalidad de procesos del CODEA y debilidades en los mecanismos de información. Todo esto hace que COSO 2013 y COBIT 5 sean dos marcos oportunos de aplicación en el CODEA para su fortalecimiento.

En consecuencia, se realizó un análisis de ambos marcos, tanto del COSO 2013, como de las siguientes lecturas de ISACA: 1) COBIT 5: Un marco de negocio para el gobierno y la gestión de las TI de la empresa y 2) COBIT 5: Procesos catalizadores.

Asimismo, para establecer la metodología de análisis se tomaron como referencia los conocimientos adquiridos mediante una capacitación internacional virtual, coordinada por el programa Capacita e-Learning[5], llamada "COSO relacionado con COBIT y las normas ISO 27001 de Seguridad de la Información para las 3 líneas de defensa en la Organización".

A continuación, se explica la metodología de análisis desarrollada:

1. Análisis de los procesos COBIT y sus prácticas de gestión: consistió en recorrer la Guía de Procesos Catalizadores de COBIT 5 con el fin de determinar la relevancia de cada uno de los procesos de gobierno de TI empresarial establecidos en dicho documento, para su aplicación en el CODEA, tomando como base el conocimiento adquirido a raíz del análisis realizado de las lecturas descritas anteriormente y la capacitación recibida.

[5] Empresa dedicada al diseño de programas de formación consultiva en Auditoría Interna, prevención de fraude, cumplimiento, control interno y auditoría de TI.

Para ello, en primera instancia se identificaron los cinco dominios establecidos en COBIT 5: 1) evaluar, orientar y supervisar (EDM), 2) alinear, planear y organizar (APO), 3) construir, adquirir e implementar (BAI), 4) entregar, dar servicio y soporte (DSS), y, por último, 5) supervisar, evaluar y valorar (MEA). A partir de ellos, se realizó un entendimiento de los procesos propuestos en cada uno y sus prácticas de gestión.

2. Entendimiento de los procesos de COBIT 5 y sus prácticas de gestión: en este primer paso se extraen las partes claves de cada proceso según COBIT 5, las cuales se detallan a continuación:

- Nombre del proceso: cada dominio posee un proceso asignado para cada uno. COBIT 5 da una breve descripción general y su propósito.
- Área del proceso: se establece si el proceso corresponde al área de gestión o de gobierno. En COBIT 5 Procesos Catalizadores de ISACA, se considera un proceso de gobierno como aquel que está alineado con los objetivos de gobierno de las partes interesadas. Incluye entrega de valor, optimización del riesgo y de recursos, además de prácticas y actividades orientadas a evaluar opciones estratégicas. Por otro lado, proceso de gestión es aquel que está alineado con la definición de gestión, las prácticas y actividades de los procesos que cubren las áreas de responsabilidad TI de la empresa y proporcionan cobertura de TI extremo a extremo (ISACA, 2012).
- Nombre del dominio: el nombre del dominio es el prefijo o la sigla (EDM, APO, BAI, DSS, MEA) y adicional el número correspondiente.
- Descripción del proceso: corresponde a la visión general de lo que hace el proceso y una visión a alto nivel de cómo él mismo lleva a cabo su propósito para conseguir su fin inmediato.

- Declaración del propósito del proceso: hace referencia a una completa descripción del propósito general.
- Información de la cascada de metas: este punto es la referencia y descripción de las metas TI relacionadas que son soportadas principalmente por el proceso y métricas para medir el logro de las metas TI relacionadas.
- Metas y métricas del proceso: corresponden al conjunto de metas del proceso y número de métricas asignadas.
- Matriz RACI: corresponde a la asignación sugerida del nivel de responsabilidad para prácticas de proceso a diferentes roles y estructuras.
- Entradas y salidas: otra parte importante de los procesos corresponden a las entradas y salidas, estas hacen referencia a las descripciones detalladas del proceso. Los procesos contienen, en el ámbito de las prácticas de gobierno y gestión entradas y salidas.

3. Identificación de procesos clave aplicables al CODEA: una vez determinados y estudiados los procesos establecidos en COBIT 5, se procedió a realizar una matriz con el fin de facilitar el análisis y mapear los procesos que estuviera directamente relacionados con el CODEA, tomando en cuenta las partes más relevantes señaladas en el punto anterior y descritos en COBIT 5.

   Cabe mencionar que la selección de los procesos claves para el CODEA, se realizó con base en el conocimiento de la entidad y su entorno, como las regulaciones, cambios relevantes debidos a COVID-19, informes de periodos anteriores de la Auditoría Interna de la Municipalidad de Alajuela, metas y objetivos planteados en el Plan Anual Operativo (PAO), así como entrevistas a la dirección.

Adicionalmente, el análisis se realizó tomando en cuenta las proporciones del CODEA como entidad, además de su capacidad de recursos para poder ajustarse a algunos de los requerimientos de COBIT 5.

Para ello, se coloca el nombre del dominio, el subproceso, las métricas del proceso, las actividades, las entradas y salidas en una matriz (ver anexo G). En dicha matriz es donde, una vez determinados los procesos aplicables al CODEA se enlistan con el fin de tener una base para continuar con el siguiente paso en el cual se homologarán con los principios de COSO, según sea su relación en cuanto al tema de control interno.

4. Identificación componentes y principios de COSO 2013: Esta identificación corresponde al proceso de tabular dentro una matriz (ver anexo H) cada uno de los componentes de este marco asociados a los 17 principios respectivos. La finalidad de dicha matriz es establecer de manera ordenada una relación entre los procesos de COBIT 5 y los cinco componentes COSO 2013.

Al realizar el análisis de COBIT 5 se identificó que varios de sus procesos podían complementar los componentes de COSO 2013, por lo que se decidió aplicar este marco como referencia de análisis para todos los componentes de COSO 2013 y no únicamente para el componente de información y comunicación. De esta forma, el análisis que se procede a realizar a cada uno de los componentes posee un fundamento mayor al ser basado en dos marcos internacionales de buenas prácticas de control.

De acuerdo con lo anterior, en esta etapa se procede a realizar un análisis de los procesos de COBIT 5 determinados como relevantes para el CODEA y a homologar ambos marcos y establecer una relación lógica entre los procesos de COBIT 5 y los componentes de COSO 2013, tomando en cuenta las características de control sobre las prácticas de gestión y los

principios que guardan relación entre ellas.

Una vez terminado el proceso anterior, en la matriz realizada se coloca el número del punto de enfoque del componente que mantienen la relación, con base en el entendimiento y conocimiento adquirido en las etapas anteriores.

Para la selección de los dominios y procesos de COBIT 5, aplicables al CODEA, se estableció una escala del 1 al 3 para asignar una calificación; siendo 1 el menos relevante para el CODEA y 3 el más relevante para el CODEA, de acuerdo con la siguiente tabla:

Tabla 6: *Escala de relevancia para la sección de procesos relevantes de CODEA*

Descripción	Escala
No relevante	1
Medianamente relevante	2
Muy relevante	3

Fuente: Elaboración propia.

Para definir esta calificación, se realizaron sesiones en equipo que tuvieron como fin discutir el dominio y proceso de acuerdo con el contexto preliminarmente analizado del CODEA. Se consideraron las métricas y actividades aplicables al CODEA, así como el componente de COSO, el objetivo de gobierno y gestión de TI, además de las entradas y salidas y las palabras clave.

Para finalizar el análisis, se visualizaron todos los dominios y procesos con calificación tres; seguidamente, se escogieron solo aquellos dominios con más de un proceso con calificación tres; finalmente, con esta depuración de dominios y procesos, se procedió con la

elaboración de los instrumentos.

b) Creación de preguntas por principios de COSO y prácticas de gestión COBIT. Tomando como base la matriz creada, se procedió a analizar cada uno de los principios de COSO y prácticas de gestión de COBIT, con el fin de establecer y crear una serie de preguntas, las cuales están directamente relacionadas con actividades y/o procesos de control que el CODEA podría implementar.

1. Características de las preguntas

- Se aplicaron mediante el uso de formularios de Google.
- Fueron dirigidas a funcionarios de la Dirección Administrativa, del Área Administrativa y Financiera, a la persona jerarca del Área Operativa y las personas encargadas del Área Deportiva, según las características del cuestionario.
- No se determinó una muestra, los cuestionarios fueron dirigidos a personas funcionarias seleccionadas según sus características y las características de las preguntas a aplicar.
- Correspondieron a preguntas dicotómicas de sí y no. Adicionalmente, se incluyó un espacio abierto para los casos de dudas o comentarios al respecto.
- Formuladas con base en COSO 2013 y COBIT 5.

c) Revisión de preguntas acorde con la finalidad del proyecto. Una vez creadas todas las preguntas con base en la matriz COSO-COBIT, se procedió a realizar una nueva revisión, con el fin de que la información a recopilar generará un aporte esencial para la elaboración de la propuesta de fortalecimiento del control interno del CODEA.

Para la selección de las preguntas aplicables a las prácticas de los dominios establecidos por COBIT 5, se tomaron en cuenta los siguientes aspectos: a) CODEA es una entidad adscrita

a un ente público por lo que posee ciertas limitaciones regulatorias, b) posee poca cantidad de personal y c) dependen de un presupuesto anual para poder operar que puede estar sujeto a modificaciones. Dado a lo anterior, muchas de las prácticas no fueron consideradas aptas para su aplicación en el CODEA.

Asimismo, al crear las preguntas con ambos marcos en el proceso de revisión se determinó que existía el riesgo de que se generarán preguntas que cumplieran un mismo fin inmediato, por lo que se procedió a realizar una tercera revisión de cada una de ellas, de esta manera se logra determinar su nivel de relevancia, la razón de su duplicidad y cual es más idónea para aplicar a los funcionarios del CODEA.

d) Aplicación del instrumento de recolección de información. Finalmente, se generaron y aplicaron 114 preguntas, las cuales fueron sistematizadas mediante la herramienta en línea *Google Forms*. Los formularios tuvieron el mismo orden que los componentes de COSO, es decir, primero se aplicó el formulario de las preguntas relacionadas a entorno de control, luego el de evaluación de riesgo, seguidamente el de actividades de control, el de información y comunicación y se finalizó con el formulario de actividades de supervisión. Aunado a esto, los formularios incluyeron una breve descripción en su parte inicial, donde se plasmó el objetivo de la aplicación de las preguntas y el tiempo aproximado para que las personas los respondieran.

Previo a la aplicación de estos formularios, se coordinó una reunión[6] con el Área Administrativa del CODEA y la Dirección Administrativa, la cual actualmente está conformada por cuatro funcionarios.

---

[6] Llevada a cabo de forma virtual el día viernes 5 de noviembre del 2021. Se utilizó la herramienta *Nearpod*, la cual permite realizar presentaciones interactivas. De esta forma se consultó sobre aspectos generales relacionados con el conocimiento de los marcos COSO 2013 y COBIT 5.

En la reunión realizada, se discutieron temas como el concepto de control interno, así como la Ley General de Control Interno N°8292, el concepto de COSO, el concepto de COBIT 5, la metodología de trabajo y la aplicación de los formularios.

Una vez que se le comunicó a la administración sobre el envío de los formularios, se procedió con su aplicación de la siguiente manera:

- Formulario 1: preguntas relacionadas con el componente entorno de control. Dada la naturaleza de las preguntas, fue enviado a las personas encargadas de la jefatura de todas las áreas del CODEA, personas funcionarias del área administrativa y financiera y de la dirección administrativa. En total, se aplicó a 9 funcionarios, de los cuales todos respondieron.

- Formulario 2: preguntas relacionadas con el componente evaluación de riesgo. Dada la naturaleza de las preguntas, fue enviado a personas funcionarias del área administrativa y financiera y de la dirección administrativa. En total, se aplicó a 6 funcionarios, de los cuales 4 respondieron.

- Formulario 3: preguntas relacionadas con el componente actividades de control. Dada la naturaleza de las preguntas, fue enviado a personas funcionarias del área administrativa y financiera y de la dirección administrativa. En total, se aplicó a 6 funcionarios, de los cuales 4 respondieron.

- Formulario 4: preguntas relacionadas con el componente de información y comunicación. Dada la naturaleza de las preguntas, fue enviado a personas funcionarias del área administrativa y financiera y de la dirección administrativa. En total, se aplicó a 6 funcionarios, de los cuales 5 respondieron.

- Formulario 5: preguntas relacionadas con el componente actividades de supervisión. Dada la naturaleza de las preguntas, fue enviado a funcionarios del área administrativa y financiera y de la dirección administrativa. En total, se aplicó a 6 funcionarios, de los cuales 5 respondieron.

Cabe aclarar que únicamente para la aplicación del formulario 1 se incluyeron funcionarios fuera del área administrativa y financiera y de la dirección administrativa, debido a que las preguntas de los otros formularios correspondían a consultas de únicamente de índole administrativo. De esta forma, se minimizó el riesgo de que las respuestas pudieran estar sesgadas por desconocimiento del tema consultado.

3.1.6 Criterios de rigurosidad científica

Las etapas de la investigación son dinámicas y se entrelazan, por esto es importante tener claridad sobre los criterios de rigurosidad científica, con el fin de asegurar la calidad en la investigación. Por ello se requieren estrategias para obtener validez, confiabilidad y objetividad. A continuación, se exponen los distintos criterios de rigurosidad tomados en cuenta en esta investigación:

3.1.6.1 Criterio de credibilidad. Dentro de este criterio, para el presente trabajo se utiliza el método de triangulación de las fuentes de información que permiten realizar análisis más objetivos, como lo son informes académicos, informes de la Municipalidad de Alajuela y personal académico de la Universidad de Costa Rica (UCR). Las fuentes de información diversas y bajo distintas modalidades como lo son indagaciones y estudio de documentos, permiten obtener diversos puntos de información para ser integrados de forma objetiva.

3.1.6.2 Criterio de transferibilidad. En cuanto a la transferibilidad, los resultados del estudio sólo pueden ser extrapolados parcialmente a otros comités cantonales con características similares que busquen una mejora en su control interno. Fuera de ese ámbito, la investigación no puede ser reproducida para explicar fenómenos similares en otro tipo de institución no deportiva.

3.1.6.3 Criterio de dependencia. Este criterio está vinculado con la consistencia y fiabilidad del trabajo. Para cumplir con ello, se contó con la constante supeditación del equipo asesor del trabajo final de graduación, por medio del monitoreo de los diversos procedimientos ejecutados en cada una de las etapas para satisfacer los objetivos de la investigación. Este proceso tenía el fin de evitar inconsistencias, incoherencias o desvíos en los procedimientos y resultados. Es por ello que se llevaron a cabo reuniones frecuentes para someter a análisis las fases de investigación y llevar un registro de acuerdos y resultados.

3.1.6.4 Criterio de confirmabilidad. Para el cumplimiento de este criterio, el equipo debe ser consciente de que toda información e idea que se origine a raíz del estudio debe ser completamente neutral, de forma que los resultados no sean influidos por ningún interés o inclinación personal. Siendo así, se establece como línea de control la debida y correcta documentación de cada aspecto que dé fundamento a lo que eventualmente sea señalado, esto mediante el diseño de programas que permitan referenciar los procesos llevados a cabo, con la documentación asociada. Asimismo, la evidencia fue 100% digital y se utilizó una carpeta Google Drive de respaldo para prevenir la pérdida de información.

3.2 Tabulación y análisis de los resultados de la metodología aplicada al CODEA

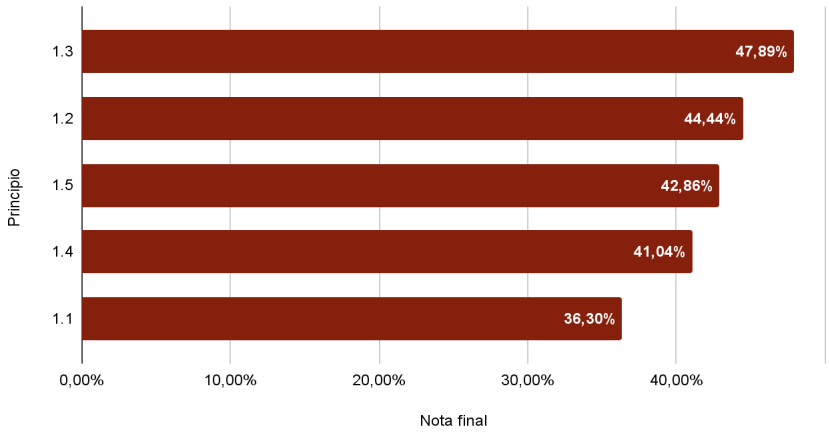
El proceso de tabulación y análisis de resultados corresponde a la etapa en la cual se detallan los resultados obtenidos de la información recabada en el proceso de investigación y estudio del CODEA. Su principal fin fue identificar los puntos de mejora más importantes.

3.2.1 Tabulación de los resultados de la información obtenida

En esta sección se procederá a detallar la tabulación de la información obtenida.

Entorno de control. El siguiente gráfico detalla los porcentajes obtenidos de acuerdo a las acciones llevadas a cabo por el CODEA relacionadas con el componente entorno de control de COSO 2013.

Figura 16: *Gráfico de porcentajes obtenidos por los principios de entorno de control según COSO 2013*



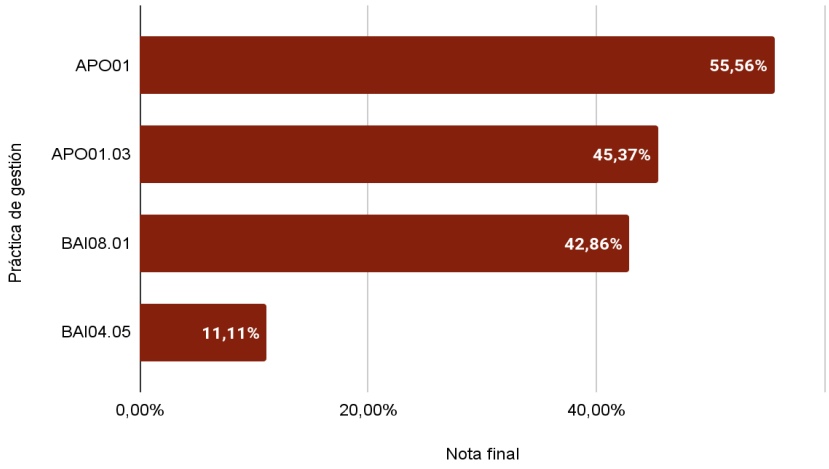
Ver Tabla 1 para la interpretación del eje vertical. Fuente: Elaboración propia.

De acuerdo al gráfico anterior, el principio de entorno de control con una mayor presencia de acciones realizadas en el CODEA es el 1.3. La dirección establece, con la supervisión del Consejo, las estructuras, líneas de reporte y los niveles de autoridad y

responsabilidad apropiados para la consecución de los objetivos, con un 47.89% para el cumplimiento de este principio. Seguidamente, sobre el principio 1.2, se puede observar que el consejo de administración demuestra independencia de la dirección y ejerce la supervisión del desempeño del sistema de control interno, con un 44.44% como resultado. En tercer lugar, se encuentra el principio 1.5, demuestra que la organización define las responsabilidades de las personas a nivel de control interno para la consecución de los objetivos, con un 42.86% como resultado. En cuarto lugar, está el principio 1.4, que habla de que la organización demuestra compromiso para atraer, desarrollar y retener a profesionales competentes, en concordancia con los objetivos de la organización, lo cual obtuvo un 41.04%. Finalmente, el principio 1.1, que indica que la organización demuestra compromiso con la integridad y los valores éticos, el cual dio como resultado un 36.30%.

Con respecto a las prácticas de gestión asociadas de COBIT 5, se obtiene lo siguiente:

Figura 17: *Gráfico de porcentajes obtenidos por práctica de gestión asociada al componente entorno de control según COBIT 5*



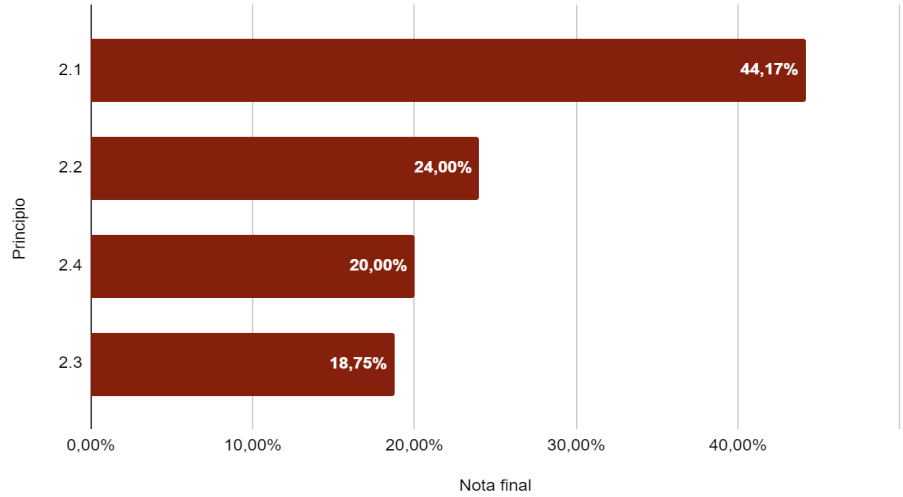
Ver Anexo K para la interpretación de eje vertical. Fuente: Elaboración propia.

De acuerdo con el gráfico anterior, se observa que en ninguna de las prácticas de gestión asociadas se obtienen resultados superiores al 75%. En su lugar, se obtiene que en el CODEA se llevan a cabo acciones en un 55.56% relacionadas con el dominio APO01: Gestionar el marco de gestión de TI, el cual consiste en "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" (ISACA, 2012, p. 51). Seguidamente se ubica la práctica clave de gobierno APO01.03: Mantener los elementos catalizadores del sistema de gestión, con un 45.37%, relacionada con "mantener los elementos catalizadores del sistema de gestión y del entorno de control de la TI de la empresa. . ." (ISACA, 2012, p. 54).

En tercer lugar, se ubica la práctica denominada BAI08.01: Cultivar y facilitar una cultura de intercambio de conocimientos, con un resultado de 42.86%, la cual consiste en "concebir e implantar un esquema para cultivar y facilitar una cultura de intercambio de conocimientos" (ISACA, 2012, p. 160). Finalmente, se ubica la práctica BAI04.05: investigar y abordar cuestiones de disponibilidad, rendimiento y capacidad, el cual consiste en "maximizar la probabilidad de la implementación exitosa en toda la empresa del cambio organizativo de forma rápida y con riesgo reducido, cubriendo el ciclo de vida completo del cambio y todas las partes interesadas del negocio y de TI" (ISACA, 2012, p.145).

Evaluación de riesgos. El siguiente gráfico detalla los porcentajes obtenidos de acuerdo con las acciones llevadas a cabo por el CODEA relacionadas con el componente evaluación de riesgos según COSO 2013.

Figura 18: *Gráfico de porcentajes obtenidos por los principios del componente evaluación de riesgos según COSO 2013*

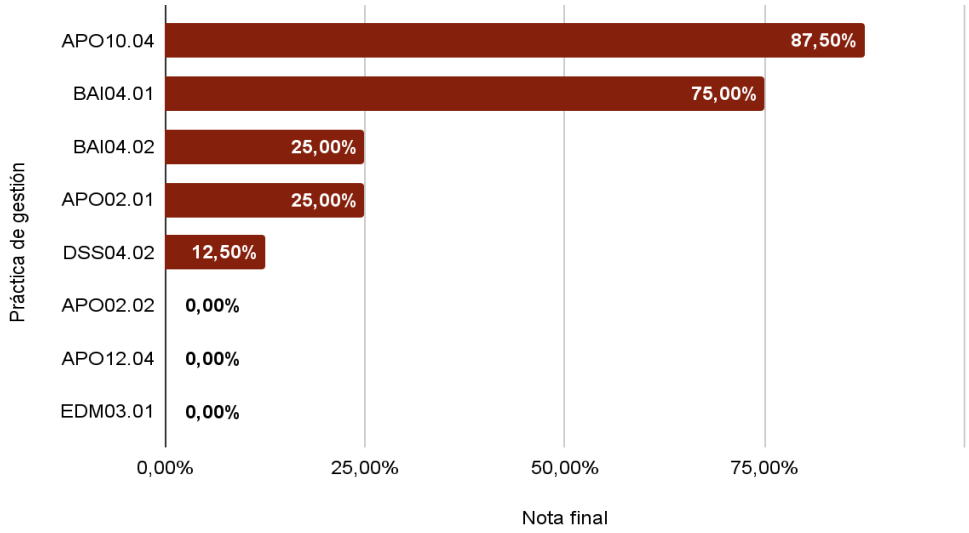


Ver Tabla 1 para la interpretación del eje vertical. Fuente: Elaboración propia.

De acuerdo con el gráfico anterior, se puede visualizar que, en relación con los principios de evaluación de riesgos, ninguno de sus cuatro principios que lo componen superan el 50%. Lo anterior indica que existen deficiencias relevantes en dicho componente. Al desglosar los resultados por principio se obtiene que el principio 2.1 el cual habla de si la organización define los objetivos con suficiente claridad para permitir la identificación y evaluación de los riesgos relacionados, se obtuvo una nota del 44,17%. En segundo lugar, se ubica el principio 2.2, que indica si la organización identifica los riesgos para la consecución de sus objetivos en todos los niveles de la entidad y los analiza como base sobre la cual determina cómo se deben gestionar, con un 24%. En tercer lugar, el principio 2.4 sobre si la organización identifica y evalúa los cambios que podrían afectar significativamente al sistema de control interno presenta una nota del 20%. Y en último lugar, se encuentra el principio 2.3 que determina si la organización considera la probabilidad de fraude al evaluar los riesgos para la consecución de los objetivos, el cual está en la última posición, con un 18,75%. Lo anterior

evidencia la necesidad de implementar acciones en relación con el fortalecimiento con los principios del componente evaluación de riesgo.

Figura 19: *Gráfico de porcentajes obtenidos por práctica de gestión asociada al componente evaluación de riesgo según COBIT 5*



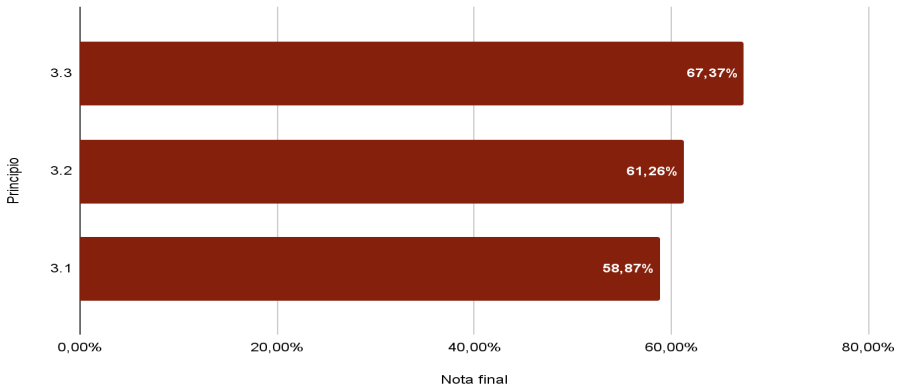
Ver Anexo K para la interpretación de eje vertical. Fuente: Elaboración propia

Del gráfico anterior, se puede observar que el cumplimiento de acciones para fortalecer las prácticas de gestión de COBIT 5 en relación con la evaluación de riesgos, las prácticas de gestión que tuvieron un porcentaje alto son tanto el APO10.04: Gestionar el riesgo en el suministro, como también BAI04.01: Evaluar la disponibilidad, rendimiento y capacidad actual y crear una línea de referencia, ambos con resultados superiores al 75%. Sin embargo, las prácticas de gestión con acciones mínimas para el cumplimiento óptimo de buenas prácticas de COBIT 5 son: BAI04.02: Evaluar el impacto en el negocio, DSS04.02: Mantener una estrategia de continuidad, APO02.01: Comprender la dirección de la empresa, APO02.0: Evaluar el entorno, capacidades y rendimiento actuales, APO12.04: Expresar el riesgo, EDM03.01: Evaluar la gestión de riesgos que presentaron porcentajes inferiores al 25%, cada uno de los

cuales tienen implicaciones sobre la dirección y continuidad de CODEA como entidad en funcionamiento. Además, sus efectos ante posibles riesgos derivados de fuentes externas o internas pueden generar una duda razonable sobre la dificultad de operar en su entorno o bien la dificultad para cumplir sus objetivos ante la falta de identificación y cuantificación de riesgos.

Actividades de control. Los siguientes gráficos detallan los resultados obtenidos de la aplicación del cuestionario relacionado con el componente actividades de control en el CODEA. Inicialmente, los porcentajes obtenidos de los resultados del análisis con base en COSO 2013 para el componente actividades de control fueron los siguientes:

Figura 20: *Gráfico de porcentajes obtenidos por los principios del componente actividades de control según COSO 2013*



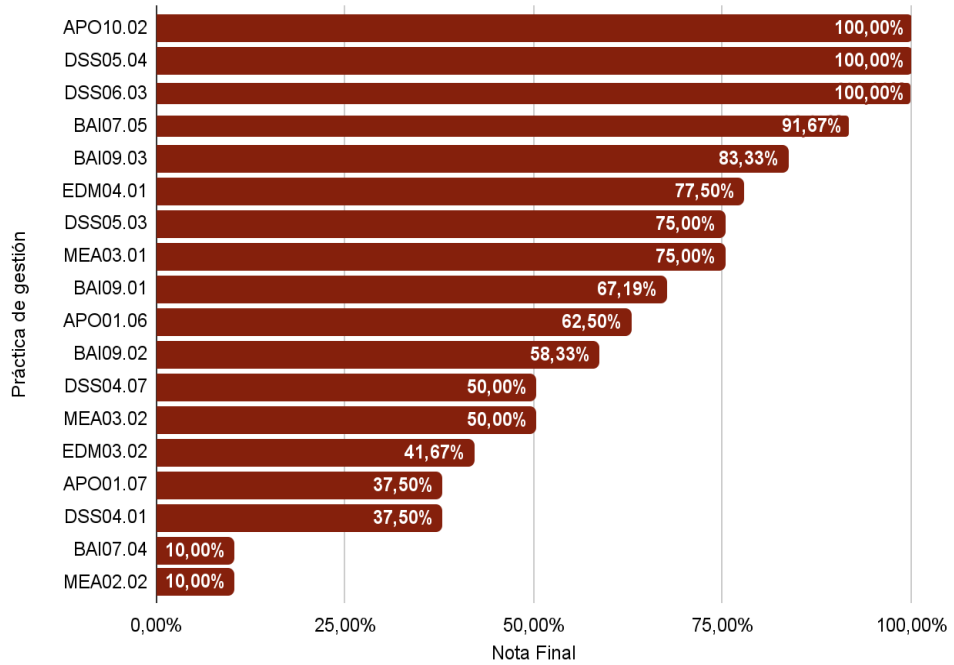
Ver Tabla 1 para la interpretación del eje vertical. Fuente: Elaboración propia.

En el gráfico anterior se aprecia que, en general, el componente actividades de control en el CODEA presenta un porcentaje de aplicación similar entre ellos para los tres principios. El principio 3.3 es el que presenta mayor grado de aplicación, con una nota del 67,37% y está relacionado con actividades de control a través de políticas que establecen las líneas generales del control interno y procedimientos. Seguidamente, se encuentra el principio 3.2, con un

61,26%, el cual hace referencia a la definición y desarrollo de actividades de control a nivel de entidad sobre la tecnología para apoyar la consecución de los objetivos. Finalmente, está el principio 3.1, con un 58,87%, que establece que la organización define y desarrolla actividades de control que contribuyen a la mitigación de los riesgos hasta niveles aceptables para la consecución de los objetivos.

Posteriormente, se tiene el detalle gráfico de los resultados porcentuales obtenidos para actividades de control con base en COBIT 5:

Figura 21: *Gráfico de porcentajes obtenidos por práctica de gestión asociada al componente actividades de control según COBIT 5*



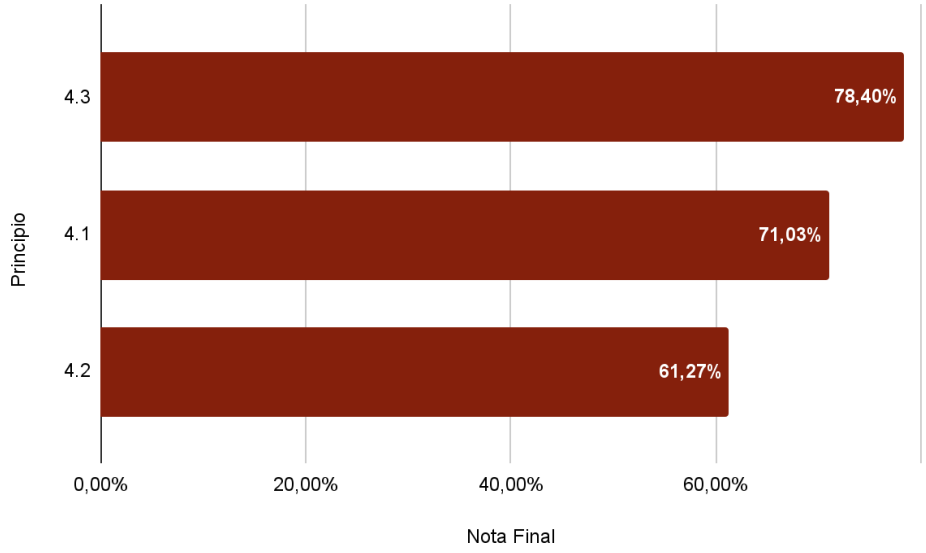
Ver Anexo K para la interpretación de eje vertical. Fuente: Elaboración propia Fuente: Elaboración propia.

En la Figura 21 se detalla cada una de las prácticas de gestión asociadas con COBIT 5 y se aprecia el porcentaje de aplicación de cada una de ellas en el CODEA. Se observa que las que tienen un mayor porcentaje de aplicación por encima del 75%, son APO10.02: Seleccionar los proveedores, DSS05.04: Gestionar la identidad del usuario y el acceso lógico, DSS06.03: Gestionar roles responsabilidades privilegios de acceso, y niveles de autorización, BAI07.05: Ejecutar pruebas de aceptación, BAI09.03: Gestionar el ciclo de vida de los activos, EDM04.01: Evaluar la gestión de recursos, DSS05.03: Gestionar la seguridad de los puestos de usuario final y MEA03.01: Identificar requisitos externos de cumplimento.

Adicionalmente, se aprecia que las que presentan aplicación por debajo del 50% son EDM03.02: Orientar la gestión de riesgo, APO01.07: Gestionar la mejora continua de los procesos, DSS04.01: Definir la política de continuidad, BAI07.04: Establecer un entorno de pruebas y MEA02.02: Revisar la efectividad de los controles sobre los procesos de negocio, dejando en evidencia puntos de mejora en tema de controles, continuidad y riesgos.

Información y comunicación. El siguiente gráfico detalla los porcentajes obtenidos de la aplicación del cuestionario relacionado con el componente de información y comunicación según COSO 2013.

Figura 22: *Gráfico de porcentajes obtenidos por los principios del componente información y comunicación según COSO 2013*

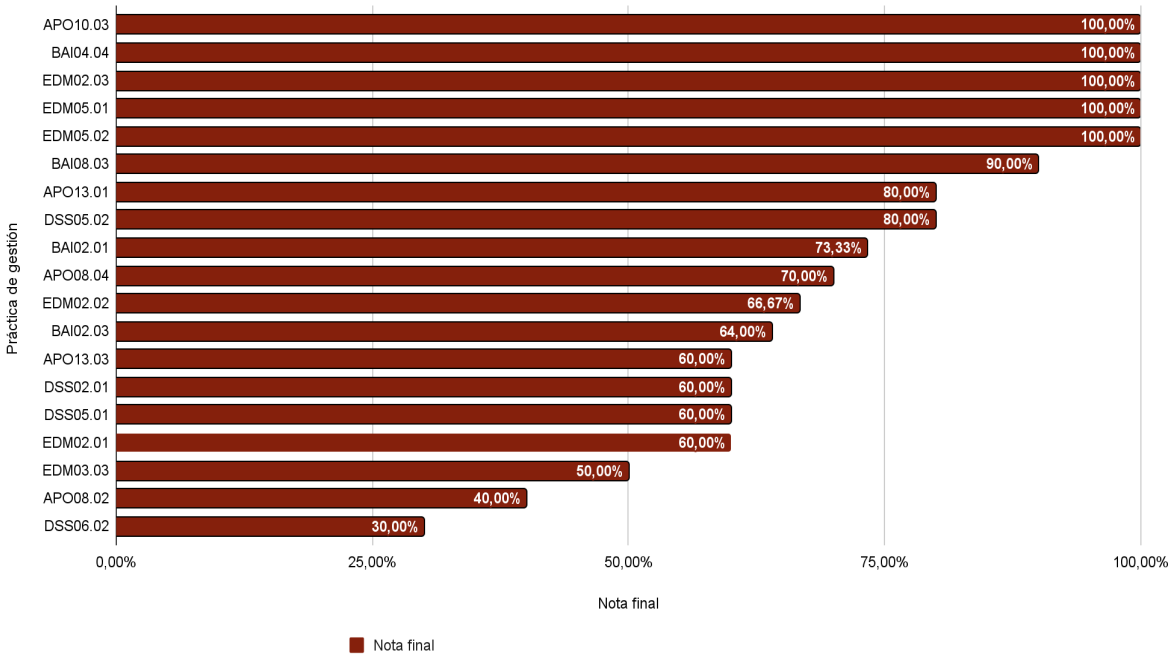


Ver Tabla 1 para la interpretación del eje vertical. Fuente: Elaboración propia.

De acuerdo al gráfico anterior, se aprecia que el principio del componente de información y comunicación con mayor aplicación en el CODEA es el principio 4.3 con un 78,40%, el cual se enfoca en la comunicación externa con los grupos de interés. Luego está el principio 4.1 con un 71.03%, el cual está relacionado con el procesamiento de la información para que esta sea de calidad y relevante. Finalmente, el principio 4.2 con 61,27%, el cual se enfoca en la comunicación interna del personal y las áreas del CODEA.

Por otra parte, el gráfico de porcentajes obtenidos para información y comunicación con base en COBIT 5 muestra los siguientes resultados:

Figura 23: *Gráfico de porcentajes obtenidos por práctica de gestión asociada al componente información y comunicación según COBIT 5*



Ver Anexo K para la interpretación de eje vertical. Fuente: Elaboración propia.

En la Figura 23, se detalla cada una de las prácticas de gestión COBIT 5 asociadas al componente de información y comunicación, en el cual se visualiza el porcentaje de cada una de ellas. Las prácticas con porcentaje de aplicación por encima del 75% son DSS05.02: Gestionar la seguridad de la red y las conexiones, APO13.01: Establecer y mantener un SGSI[7], BAI08.03: Organizar y contextualizar la información transformándola en conocimiento, EDM05.01: Evaluar los requisitos de elaboración de informes de las partes interesadas, EDM05.02: Orientar la comunicación con las partes interesadas y la elaboración de informes, EDM05.03: Supervisar la comunicación con las partes interesadas, BAI04.04: Supervisar y revisar la disponibilidad y la capacidad y el APO10.03: Gestionar contratos y relaciones con

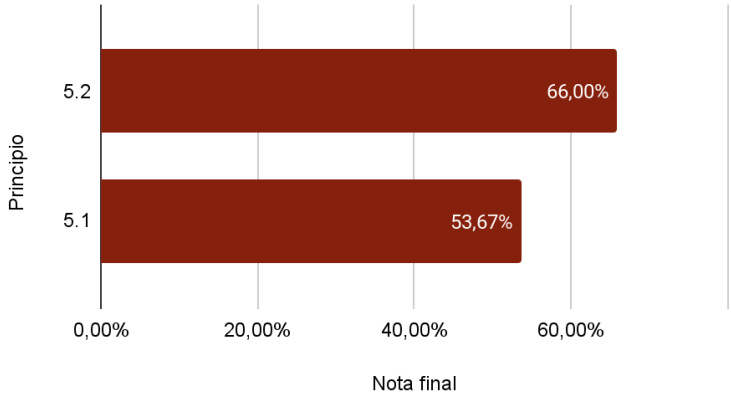
[7] Sistema de gestión de seguridad de la información.

proveedores.

Así mismo las prácticas que presentan un porcentaje igual o menor al 50% son: DSS06.02: Controlar el procesamiento de la información, APO08.02: Identificar oportunidades, riesgos y limitaciones de TI para mejorar el negocio y el EDM03.03: Supervisar la gestión de riesgos; confirmando los puntos de mejora que debe haber en los controles y los riesgos del CODEA.

Actividades de supervisión. El siguiente gráfico detalla los porcentajes obtenidos de acuerdo a las acciones llevadas a cabo por el CODEA relacionadas con el componente actividades de supervisión según COSO 2013.

Figura 24: *Gráfico de porcentajes obtenidos por los principios del componente actividades de supervisión según COSO 2013*



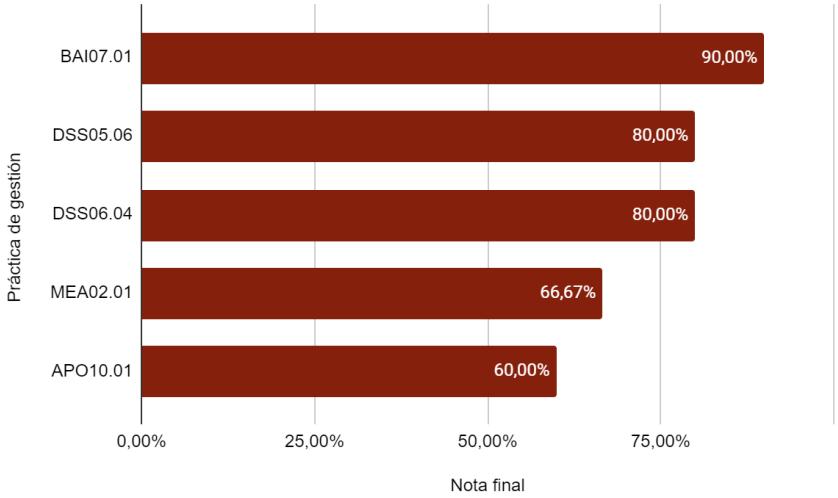
Ver Tabla 1 para la interpretación del eje vertical. Fuente: Elaboración propia.

Como se puede observar, las acciones desarrolladas en relación al principio 5.2 que indica si la organización evalúa y comunica las deficiencias de control interno de forma oportuna a las partes responsables de aplicar medidas correctivas, incluyendo la alta dirección y el consejo según corresponda, alcanzaron una nota del 66.00% y las del principio 5.1 sobre

si la organización selecciona, desarrolla y realiza evaluaciones continuas y/o independientes para determinar si los componentes del sistema están presentes y funcionando, obtuvieron un 53.67%.

Con respecto a las prácticas de gestión asociadas de COBIT 5, se observó lo siguiente:

Figura 25: *Gráfico de porcentajes obtenidos por práctica de gestión asociada al componente actividades de supervisión según COBIT 5*



Ver Anexo K para la interpretación de eje vertical. Fuente: Elaboración propia

En la figura 25, se detalla cada una de las prácticas de gestión asociadas con actividades de supervisión y se aprecia el porcentaje de aplicación de cada una de ellas en el CODEA. Se observa que las que tienen un mayor porcentaje de aplicación, por encima del 75%, son BAI07.01: Establecer un plan de implementación, con un 90%; DSS05.06: Gestionar documentos sensibles y dispositivos de salida, con un 80% y DSS06.04: Gestionar errores y excepciones con un 80%. Las que obtuvieron resultados inferiores al 75% fueron MEA02.01: Supervisar el control interno, con un 66.67% y APO10.01: Identificar y evaluar las relaciones y contratos con proveedores, con un 60%.

3.2.2 Análisis de las entrevistas y cuestionarios aplicados

A continuación, se detalla la metodología utiliza para el análisis de las respuestas de los cuestionarios aplicados y los análisis de resultados por componente de control interno:

Metodología análisis respuestas. Los formularios aplicados están compuestos por preguntas dicotómicas, es decir, respuestas cerradas de "sí" y "no" y además contaban con la opción abierta de especificar "otro". Las opciones para la opción "otro" fueron analizadas por el equipo y convertidas a una respuesta de sí o no, de esta forma, se les asignó un 1 en caso de un impacto positivo hacia el CODEA y un 0 en el caso de impacto negativo.

Posteriormente, se procedió a realizar una ponderación de las respuestas obtenidas por pregunta. Asimismo, dado que las preguntas se encuentran asociadas a principios de COSO 2013 y a componentes de COBIT 5, se enlistó las notas obtenidas por pregunta, ordenándolas por los principios y componentes asociados, generando un consolidado de las notas obtenidas y facilitando su posterior análisis mediante la creación de tablas dinámicas.

Cabe señalar que a cada una de las preguntas se les asoció un principio de COSO 2013 como "principal" y otros principios como "secundarios", esto de acuerdo con la relación del mismo con cada pregunta. El análisis de las notas obtenidas de las preguntas aplicadas se procedió a realizar por principio de COSO 2013. En este sentido, se ponderaron las notas obtenidas por principios catalogados como "principal" y luego por principios catalogados como "secundarios", para finalmente generar una nota final en la que a los principales se les asignó un peso del 80% y a los secundarios del 20%.

Los principios que no estaban asignados como "principal", fueron descartados para el cálculo de la nota final, por lo que el peso de "secundarios" fue tomado al 100%. Estos principios fueron el 1.3: La dirección establece con la supervisión del consejo, las estructuras,

líneas de reporte y los niveles de autoridad y responsabilidad apropiados para la consecución de los objetivos; el 1.5: La organización define las responsabilidades de las personas a nivel de control interno para la consecución de los objetivos; el 2.1: La organización define los objetivos con suficiente claridad para permitir la identificación y evaluación de los riesgos relacionados; el 2.3: La organización considera la probabilidad de fraude al evaluar los riesgos para la consecución de los objetivos; el 2.4: La organización identifica y evalúa los cambios que podrían afectar significativamente al sistema de control interno y el 5.1: La organización selecciona, desarrolla y realiza evaluaciones continuas y/o independientes para determinar si los componentes del sistema están presentes y funcionando.

Por otra parte, para el análisis de las respuestas obtenidas según COBIT 5, se procedió a realizar cinco tablas dinámicas en las cuales se ponderaron las notas por práctica y cada una de las tablas se filtró por componente de COSO 2013.

Finalmente, para la interpretación de los resultados obtenidos, se construyó una matriz que categoriza (columna 1) las notas de acuerdo a intervalos dados (columna 2), junto con el significado de la categoría (columna 3). A continuación, se presenta la matriz de evaluación del control interno en el CODEA según el análisis por COSO 2013 y/o a la práctica de gestión de COBIT 5:

Tabla 7: *Matriz de interpretación de resultados por categoría*

Evaluación del control interno en el CODEA		
Categoría	**Intervalo**	**Significado**
Incipiente	**0% -20%**	Existe evidencia de que la institución ha emprendido esfuerzos aislados para el establecimiento del sistema de control interno; sin embargo, aún no se ha reconocido su importancia. El enfoque general en relación con el control interno es desorganizado.
Novato	**21%-40%**	Se han instaurado procesos que propician el establecimiento y operación del sistema de control interno. Se empieza a generalizar el compromiso, pero éste se manifiesta principalmente en la administración superior.
Competente	**41%-60%**	Los procedimientos se han estandarizado y documentado, y se han difundido en todos los niveles de la organización. El sistema de control interno funciona conforme a las necesidades de la organización y el marco regulador.
Diestro	**61%-80%**	Se han instaurado procesos de mejora continua para el oportuno ajuste y fortalecimiento permanente del sistema de control interno
Experto	**81%-100%**	Los procesos se han refinado hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas y la generación de iniciativas innovadoras. El control interno se ha integrado de manera natural con las operaciones y el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, y haciendo que la organización se adapte de manera rápida.

Fuente: Elaboración propia con base en el modelo de madurez del sistema de control interno, por la Contraloría General de la República.

Análisis de los resultados. A continuación, se exponen los distintos resultados que se obtuvieron de los cuestionarios aplicados:

Resultados obtenidos para el componente Entorno de Control. En el caso del entorno de control con base en COSO 2013, al realizar la ponderación de cada uno de los principios que conforman este componente, se obtiene una nota del 37,54%. Según la matriz utilizada para el análisis, este resultado es catalogado como novato. El detalle por principio COSO es el siguiente:

Tabla 8: *Ponderación por principio del componente entorno de control según COSO 2013*

Entorno de control			
Principio	**Nota principal**	**Nota secundarios**	**Nota final**
1.1	43,52%	0,00%	34,81%
1.2	55,56%	0,00%	44,45%
1.3	0,00%	43,73%	43,73%
1.4	29,17%	48,15%	32,96%
1.5	0,00%	31,75%	31,75%
Promedio de nota final:			**37,54%**

Nota. Para el cálculo de la nota final de los principios 1.3 y 1.5, al no tener "principal" asignado, se le procede a dar un peso del 80% a la nota de "secundarios". Fuente: Elaboración propia.

Alineado con el punto anterior, el análisis realizado para las prácticas de COBIT 5 relacionados a los principios del componente de entorno de control, se revela que existen debilidades en prácticas de gestión BAI04.05, BAI08.01, APO01.03, debido que se encuentran por debajo del 50%. Estas debilidades se detallan a continuación:

- Existen debilidades en relación con la práctica de gestión BAI 04.05: Investigar y

abordar cuestiones de disponibilidad, rendimiento y capacidad, ya que se requiere mejorar la resolución rápida de emergencias en caso de interrupciones de los sistemas.

- Existen deficiencias para el cumplimiento de la práctica de gestión BAI08.01: Cultivar y facilitar una cultura de intercambio de conocimientos, debido a que no existen esquemas que permitan promover y facilitar el intercambio de conocimientos entre los colaboradores de CODEA.

- Se identifican debilidades en el cumplimiento de la práctica de gestión APO01.03: Mantener los elementos catalizadores del sistema de gestión, debido a que existe la necesidad de mejorar el trabajo en equipo y en promover una cultura de cumplimiento y mejora continua de los procesos que contribuya al cumplimiento de los objetivos.

Tabla 9: *Ponderación COBIT 5 homologado con el componente de entorno de control de COSO 2013*

Sigla	Nombre	Nota
BAI04.05	Investigar y abordar cuestiones de disponibilidad, rendimiento y capacidad	11,11%
BAI08.01	Cultivar y facilitar una cultura de intercambio de conocimientos	42,86%
APO01.03	Mantener los elementos catalizadores del sistema de gestión	45,37%

Fuente: Elaboración propia.

Por medio de los cuestionarios, se identificaron fortalezas y debilidades determinadas por principio, los cuales se explican a continuación:

1. Principio 1.1: La organización demuestra compromiso con la integridad y los valores éticos: A continuación, se detalla un listado de las fortalezas relacionadas a este principio.

    - El 100% de los colaboradores indica que existe un estatuto del funcionamiento de CODEA debidamente establecido.
    - El 89% de funcionarios respondió que los objetivos estratégicos están alineados con la misión de la entidad.
    - El 100% de personas indicó que las actas del comité de la junta directiva demuestran la discusión y revisión de asuntos relevantes que pueden impactar a CODEA.
    - El 100% de personas mencionó que se desarrollan reuniones frecuentes que permiten un control y supervisión constante de las actividades y asuntos de importancia de CODEA.
    - El 100% de personas indicó que la junta directiva, revisa y aprueba el presupuesto anual.
    - El 100% de funcionarios mencionó que existe un proceso formal y documentado para la conformación de la junta directiva, incluyendo que cumpla con las credenciales necesarias.

    En cuanto a las debilidades asociadas a este principio se encuentran:

    - El 100% de las personas indicó que no existe un código de ética documentado y difundido en los niveles de la organización, ni existe un

proceso formal de aceptación del mismo, tampoco existen medidas alternativas, que permitan asegurar la integridad y valores éticos de CODEA.

- El 100% de colaboradores respondió que no se identifican líneas de reporte que permitan realizar comunicaciones anónimas por parte de los funcionarios de CODEA.
- El 66% de los funcionarios de CODEA indicó que no se investigan y documentan las faltas a la ética.
- El 66% de las personas mencionó que no se comunican a lo interno las acciones disciplinarias ante faltas a la ética.
- El 100% de colaboradores indicó que no se identifican canales de comunicación que permitan abordar situaciones inapropiadas.
- El 100% de personas afirmó que la junta directiva no realiza supervisión de situaciones inapropiadas.

2. Principio 1.2: El consejo de administración demuestra independencia de la dirección y ejerce la supervisión del desempeño del sistema de control interno: la fortaleza identificada corresponde a que el 56% de funcionarios respondieron que la administración y la junta directiva realizan la supervisión del control interno. Para este principio no se identificaron debilidades asociadas.

3. Principio 1.3: La dirección establece con la supervisión del consejo, las estructuras, líneas de reporte y los niveles de autoridad y responsabilidad apropiados para la consecución de los objetivos*:* la fortaleza de este principio es que el 100% de colaboradores indicaron que existe y conocen el organigrama organizacional alineado

con los objetivos de CODEA. La debilidad es que el 66% de las personas indicaron que existen oportunidades de mejora en la asignación de roles y responsabilidades, al no existir un manual de puestos actualizado sobre la descripción de los puestos.

4. Principio 1.4: La organización demuestra compromiso para atraer, desarrollar y retener a profesionales competentes, en concordancia con los objetivos de la organización: las fortalezas de este principio son que el 78% de las personas entrevistadas indicó que se definen expectativas de desempeño para cada colaborador de CODEA y un 56% mencionaron que se presentan buenas prácticas en cuanto a la contratación, entrenamiento, evaluación y cuando se deben tomar acciones disciplinarias en el personal.

   Por otra parte, las debilidades asociadas son:

   - El 83% de las personas funcionarias del CODEA indicó que no existen políticas de recursos humanos.
   - El 89% de empleados mencionó que no se proporciona capacitación para mejorar y mantener las habilidades de los colaboradores.
   - El 83% de las personas que se les aplicó el cuestionario mencionó que no existe una cultura de capacitación y transferencia de conocimientos entre funcionarios de CODEA.

5. Principio 1.5: La organización define las responsabilidades de las personas a nivel de control interno para la consecución de los objetivos: este principio sólo presentaba una debilidad, la cual es que el 66% de las personas indicaron que no se documentan las responsabilidades de control interno dentro de las que se incluyen en las descripciones de puestos y responsabilidad de control interno.

Resultados obtenidos para evaluación de riesgos. En el caso de la evaluación de riesgos, con base a COSO 2013, al realizar la ponderación de cada uno de los principios que conforman este componente, se obtiene una nota del 26,73%, según la matriz utilizada para el análisis este resultado es catalogado como Novato y esto se debe a que por medio de los cuestionarios realizados al CODEA se determinó que la evaluación de riesgos es uno de los componentes que presenta mayor cantidad de puntos de mejora. A continuación, el detalle por principio según COSO 2013:

Tabla 10: *Ponderación evaluación de riesgo por principio según COSO 2013*

Evaluación de riesgo			
Principio	**Nota principal**	**Nota secundarios**	**Nota final**
2.1	0,00%*	44,17%	44,17%
2.2	30,00%	0,00%	24,00%
2.3	0,00%*	18,75%	18,75%
2.4	0,00%*	20,00%	20,00%
		Promedio de la nota final:	**26,73%**

*Nota. Para el cálculo de la nota final de los principios 2.1, 2.3, y 2.4, al no tener "principal" asignado, se le procede a asignar un peso del 100% a la nota de "secundarios". Fuente: Elaboración propia.

Alineado con el punto anterior, el análisis hecho para las prácticas de COBIT 5 relacionadas a los principios del componente evaluación de riesgos revela que existen deficiencias en las prácticas de gestión APO02.02, APO12.04, EDM03.0, APO12, DSS04.02, APO02.01y BAI04.02, debido a que se encuentran por debajo del 50% establecido en la matriz, y las cuales se detallan a continuación.

Tabla 11: *Ponderación COBIT 5 homologado con el componente de evaluación de riesgos de COSO 2013*

Sigla	Nombre	Nota
APO02.02	Evaluar el entorno, capacidades y rendimiento actuales	0,00%
APO12.04	Expresar el riesgo	0,00%
EDM03.01	Evaluar la gestión de riesgos	0,00%
N/I	Gestionar el riesgo	0,00%
DSS04.02	Mantener una estrategia de continuidad	12,50%
APO02.01	Comprender la dirección de la empresa	25,00%
BAI04.02	Evaluar el impacto en el negocio	25,00%
BAI04.01	Evaluar la disponibilidad, rendimiento y capacidad actual y crear una línea de referencia	75,00%
APO10.04	Gestionar el riesgo en el suministro	87,50%

Fuente: Elaboración propia.

Las debilidades que se identificaron son:

- Existen debilidades en relación con la práctica de gestión APO02.02: Evaluar el entorno, capacidades y rendimiento actuales, ya que no se logra determinar la existencia de análisis realizados sobre el entorno interno o externo, la capacidad de recursos y rendimientos del CODEA, por ende, no existen evaluaciones de estos rubros.
- Existen deficiencias para el cumplimiento de la práctica de gestión APO12.04: Expresar el riesgo, debido a que no se determina la existencia de un SEVRI o algún análisis enfocado a su identificación.

- Se identifican debilidades en el cumplimiento de la práctica de gestión EDM03.01: Evaluar la gestión del riesgo, debido a que se determina que en primera instancia no se identifican riesgos por lo que no existe la posibilidad de realizar evaluaciones.

- Existen debilidades en relación con la práctica de Gestión DSS04.02: Mantener una estrategia de continuidad, ya que no existe un plan de continuidad del negocio en el CODEA.

- Se identifican debilidades en el cumplimiento de la práctica de gestión APO02.01: Comprender la dirección de la empresa, dado que no se identifican procesos o actividades relacionadas a dicha práctica.

- Existen deficiencias para el cumplimiento de la práctica de gestión BAI04.02: Evaluar el impacto en el negocio, pues no se identifican procesos o actividades relacionadas al impacto del negocio, por lo que no existen evaluaciones.

Asimismo, en los cuestionarios se identificaron fortalezas y debilidades estructuradas por principio según COSO 2013, las cuales se explicarán a continuación:

1. Principio 2.1: La organización define los objetivos con suficiente claridad para permitir la identificación y evaluación de los riesgos relacionados. Dentro de las fortalezas están:

    - El 75% de las personas a las que se les aplicó el formulario indicó que se han identificado y documentado incidentes asociados con la capacidad de recursos (humanos, materiales y presupuestarios) que hayan afectado la operación normal del CODEA.

    - El 100% de las personas a las cuales se les aplicó el cuestionario mencionó que se identifican y se gestionan los riesgos relacionados con la capacidad del

proveedor de entregar el servicio de forma eficiente, eficaz, segura, fiable y continua.

Las debilidades asociadas a este principio son:

- EL 75% de las personas funcionarias encuestadas indica que en el CODEA no realiza un proceso de identificación de riesgos. Con base en lo anterior y a las indagaciones realizadas, se determina que no se utiliza SEVRI para la identificación de riesgos y no existen actividades por medio de las cuales los riesgos identificados se analizan a través de un proceso que incluye estimar la importancia potencial del riesgo y considerar la probabilidad y frecuencia de ocurrencia, y el impacto del riesgo si ocurriera.
- De la mano con el punto anterior, se concluye que no se identifican las fortalezas, oportunidades, debilidades y amenazas en el entorno actual y su impacto en el logro de los objetivos del CODEA. Asimismo, no se ha determinado alguna posible afectación en la continuidad de las actividades del CODEA, no se tiene definido y documentado el apetito al riesgo por la Junta Directiva, y tampoco se tiene un proceso de informar los resultados de los riesgos identificados a la Junta Directiva.

2. Principio 2.2: La organización identifica los riesgos para la consecución de sus objetivos en todos los niveles de la entidad y los analiza como base sobre la cual determina cómo se deben gestionar. La fortaleza en este principio es que el 75% las personas funcionarias encuestadas indican que las actividades, proyectos, iniciativas o cambios se realizan tomando como base la capacidad de presupuesto y recursos.

   Como debilidad se encuentra que el 50% respondió que no se tiene establecido el

tiempo mínimo de recuperación ante una disrupción importante, así como medidas para reducir el impacto.

3. Principio 2.3: La organización considera la probabilidad de fraude al evaluar los riesgos para la consecución de los objetivos. Las fortalezas identificadas para este principio son:

    - La entidad documenta por medio de actas las decisiones y procesos que se realizan dentro del CODEA, por medio de ello se demuestra una revisión activa y reducción de las probabilidades de fraude.

    - El 75% de los encuestados aseguran que, al definir el contrato, se incluye una descripción clara de todos los requisitos de servicio, de acuerdo con la Ley de Contratación Administrativa N.°7494, el restante 25% indica que no tiene conocimiento sobre el proceso.

    Como debilidad se determina que las áreas sujetas a incentivos y presiones se abordan mediante controles de seguimiento adicionales, como auditoría interna de la Municipalidad de Alajuela o revisiones presupuestarias frente a revisiones reales, así como procesos de documentación mediante actas.

4. Principio 2.4: La organización identifica y evalúa los cambios que podrían afectar significativamente al sistema de control interno. Como fortaleza, se identifica que existen entidades reguladoras y de gobierno relevantes, y que al ser un ente adscrito de carácter público debe evaluar nuevas leyes o regulaciones y el impacto en sus actividades.

    La debilidad principal es que el 75% del personal encuestado indica que no se identifican, de forma previa, soluciones a posibles incidentes relacionados con los

recursos (humanos, materiales y presupuestarios).

Resultados obtenidos para actividades de control. En cuanto al componente número 3 de COSO 2013, denominado actividades de control, se obtuvo una nota general del 62,50%, catalogada en el nivel "diestro" de acuerdo con la matriz establecida. Sin embargo, existen riesgos que eventualmente podrían debilitar la consecución de los objetivos institucionales. A continuación, se presenta una tabla resumen de las notas obtenidas por principio, por aplicación primaria, secundaria y nota final:

Tabla 12: *Ponderación de actividades de control por principio según COSO 2013*

Actividades de control			
Principio	**Nota principal**	**Nota secundarios**	**Nota final**
3.1	59,62%	55,88%	58,87%
3.2	62,50%	56,29%	61,26%
3.3	69,38%	59,34%	67,37%
Promedio de nota final:			**62,50%**

Fuente: Elaboración propia.

En cuanto a las 18 prácticas de COBIT 5 asociadas a este componente, se obtuvo que 2 se encuentran en estado nulo, 5 en estado deficiente, 5 en aceptable y 6 en óptima. Aquellas ubicadas en estado nulo y deficiente corresponden a las siguientes:

Tabla 13: *Ponderación COBIT 5 homologado con el componente de actividades de control de COSO 2013*

Sigla	Nombre	Nota
BAI07.04	Establecer un entorno de pruebas	0,00%
MEA02.02	Revisar la efectividad de los controles sobre los procesos de negocio	0,00%
APO01.07	Gestionar la mejora continua de los procesos	37,50%
DSS04.01	Definir la política de continuidad del negocio, objetivos y alcance	37,50%
EDM03.02	Orientar la gestión de riesgos	41,67%
DSS04.07	Gestionar acuerdos de respaldo	50,00%
MEA03.02	Optimizar la respuesta a requisitos externos	50,00%

Fuente: Elaboración propia.

Las debilidades de identificadas son:

- La práctica de gestión BAI07.04: Establecer un entorno de pruebas se encuentra en estado nulo ya que no se logran determinar pruebas representativas para asegurar el rendimiento y calidad.
- La práctica de gestión MEA02.02: Revisar la efectividad de los controles sobre los procesos de negocio se encuentra en estado nulo, ya que no se logran determinar controles para cada proceso.
- Se identifican debilidades en la práctica de gestión APO01.07: Gestionar la mejora continua de los procesos, ya que la evaluación de los procesos críticos no es el adecuado.
- Existen debilidades en relación con la práctica de gestión DSS04.01: definir políticas de continuidad del negocio, objetivos y alcance, esto porque no existe

un plan de continuidad del negocio en el CODEA.

- Se identifican debilidades en el cumplimiento de la práctica de gestión EDM03.02: Orientar la gestión de riesgos, dado que no hay una cultura en las políticas de prevención y detección de riesgos.

- Existen deficiencias para el cumplimiento de la práctica de gestión DSS04.07: Gestionar acuerdos de respaldo, dado que no todos realizan copias de seguridad de sus trabajos.

- Para el cumplimiento de la práctica de gestión MEA03.02: Optimizar la respuesta a requisitos externos, el estado es deficiente, dado que las políticas y procedimientos no se ajustan con regularidad ni se tiene claramente definido el personal.

Los cuestionarios identificaron las siguientes fortalezas y debilidades por principio:

1. Principio 3.1: La organización define y desarrolla actividades de control que contribuyen a la mitigación de los riesgos hasta niveles aceptables para la consecución de los objetivos. Las fortalezas de este principio son:

   - El 100% de las respuestas señaló que sí se cuenta con documentación soporte de los errores detectados en la fase de prueba o posterior a ello en la implementación del nuevo sistema.

   - El 75% indicó que se desarrolla y conserva evidencia que respalde la investigación y la resolución de asuntos (quejas/ temas legales).

   - El 75% indicó que se identifica de manera oportuna incidentes o activos en mal estado.

- El 100% de las respuestas señaló que existen prácticas adecuadas, como un debido proceso para la adquisición de nuevos activos.
- El 100% de los encuestados indicó que se tienen plaqueados todos los activos fijos.
- El 75% indicó que el CODEA comunica a las personas usuarias los posibles riesgos por el uso de los sistemas de información y promueve una cultura de prevención y detección de los mismos.

Las debilidades son las siguientes:

- El 100% de las respuestas señaló que se detectaron errores en la fase de prueba o posterior a ello en la implementación del nuevo sistema.
- El 75% indicó que no se cuenta con políticas de prevención y detección de riesgos.
- El 75% indicó que no se cuenta con una política de prevención y detección de riesgos ante el uso de TI para los colaboradores.
- El 100% de las respuestas señaló que no se mantiene documentada la efectividad o deficiencias de los controles que poseen.
- El 100% de las respuestas señaló que las narrativas o los diagramas de flujo no demuestran una combinación de controles dentro de cada proceso.
- El 50% indicó que no se reacciona inmediatamente al reemplazo, reparación y/o mantenimiento de los activos.

2. Principio 3.2: La organización define y desarrolla actividades de control a nivel de entidad sobre la tecnología para apoyar la consecución de los objetivos. Entre las

fortalezas están:

- 75% de los encuestados señaló que sí identifican y supervisan los cambios legales y regulatorios que le afectan al CODEA.
- El 75% indicó que se tienen definidos a los funcionarios encargados de realizar evaluaciones de los cambios legales y regulatorios.
- El 75% de los encuestados afirmó que sí tienen controles de seguridad sobre los accesos, contraseñas y responsables de información confidencial.
- El 100% confirmó que mantienen los accesos de los usuarios, de acuerdo con los requerimientos de las funciones y procesos de negocio.
- El 75% indicó que en CODEA identifican procesos de soporte de los servicios de TI que eventualmente requieran.
- El 100% confirmó que tienen claramente identificados y registrados en un auxiliar todos los activos del CODEA.
- El 75% de las personas confirmó que se han realizado conteo de activos en el último periodo 2020/2021, ya sea parciales o al 100%.
- Este 75% también señaló que sí se tiene documentación soporte de estos conteos.
- El 75% del personal indicó que en CODEA sí validan la vida útil de los activos; y que estas validaciones se realizan de manera recurrente.
- El 75% de las personas mencionó que cuando se dan violaciones de seguridad referidas a activos, estos se monitorean, se informan y resuelven adecuadamente.

En cuanto a las debilidades asociadas a este principio son:

- El 75% del personal indicó que sí actualizan las políticas, principios procedimientos y estándares para mantener la eficiencia y el cumplimiento de los procesos del CODEA, sin embargo, no lo realizan con una periodicidad definida.
- El 50% de los encuestados señaló que no tienen definidos a los funcionarios encargados de actualizar estás políticas, principios, procedimientos y estándares.
- De igual forma, este 50% indicó que no realizan copias de seguridad de los archivos con los que trabajan.
- El 100% señaló que no tienen definida y documentada alguna política sobre la continuidad de las actividades del CODEA.
- A pesar de tener todos los activos registrados en un auxiliar, el 50% de las personas indicó que esta información no se encuentra registrada en el nuevo ERP.
- El 100% de las personas señaló que no se tienen los procesos de activo identificados mediante diagramas de flujo.
- El 50% de los encuestados mencionó que no se tiene registrado las bajas de activo por desuso, obsolescencia, falla, entre otros.

3. Principio 3.3: La organización despliega las actividades de control a través de políticas que establecen las líneas generales del control interno y procedimientos. Las fortalezas que tiene este principio son las siguientes:

- El 100% de los encuestados indicó que sí tienen establecida alguna política de selección de proveedores que asegure un adecuado y transparente proceso. Mencionan que utilizan el Sistema Integrado de Compras Públicas (SICOP) para mayor control.
- El 75% de las personas mencionó que sí tienen un inventario que incluya un listado de los propietarios y custodios de la información (sistemas y datos).
- El 100% del personal señaló que sí tienen asignado roles y responsabilidades cuando se realizan traslados de datos de un sistema a otro.
- El 75% indicó que sí cuentan con una planeación para la asignación y gestión de los recursos (presupuesto, personas, procesos y tecnologías) de acuerdo con los límites presupuestarios.

En cuanto a las debilidades asociadas a este principio son:

- El 50% del personal mencionó que no se tienen identificados procesos críticos del CODEA, lo cual es una debilidad, ya que hay personal de la misma área que no conocen sobre estos procesos.
- Asimismo, siguiendo la línea del punto anterior, el 75% de las personas mencionó que no se evalúa el rendimiento y capacidad de dichos procesos.
- El 50% indicó que no tienen establecidas políticas y procedimientos que permitan asegurar la confidencialidad, integralidad y seguridad de la información (datos) de CODEA.

Resultados Obtenidos para información y comunicación. En relación con el componente de información y comunicación con base a COSO 2013, al realizar la ponderación de cada uno de los principios que conforman este componente, se obtiene una nota del 70,23%, según la matriz utilizada para el análisis este resultado es catalogado como diestro y esto se debe a que por medio de los cuestionarios realizados al CODEA se determinó que el componente de información y comunicación no presenta debilidades significativas. A continuación, el detalle por principio COSO:

Tabla 14: *Ponderación información y comunicación por principio según COSO 2013*

Información y comunicación			
Principio	**Nota principal**	**Nota secundarios**	**Nota final**
4.1	72,22%	66,25%	71,03%
4.2	63,00%	54,35%	61,27%
4.3	80,00%	72,00%	78,40%
	Promedio de nota final:		**70,23%**

Fuente: Elaboración propia.

Alineado con el punto anterior, el análisis realizado para las prácticas de COBIT 5 relacionados a los principios del componente de entorno de control, se revela que existen debilidades en prácticas de gestión DSS.06.02, EDM03.03, APO08.02, debido que se encuentran por debajo del 50%. Los cuales son las siguientes:

- Existen debilidades en relación con la práctica de gestión DSS06.2: Controlar el procesamiento de la información, debido a que han presentado interrupciones en los sistemas que han limitado que la información sea completa, precisa, oportuna y segura.

- Se identificaron deficiencias para el cumplimiento de la práctica de gestión sobre el EDM03.03: Supervisar la gestión de los riesgos ante la falta de procesos para que los problemas o desviaciones sean comunicados e informados para su resolución.

- Se detectaron deficiencias en relación con las prácticas de gestión relacionadas con el APO08.02: Identificar oportunidades, riesgos y limitaciones de TI para mejorar el negocio dado que no se identifican y comunican a las partes interesadas clave las oportunidades, riesgos y limitaciones relacionadas con las TI.

Tabla 15: *Ponderación COBIT 5 homologado con el componente de información y comunicación de COSO 2013*

Sigla	Nombre	Nota
DSS06.02	Controlar el procesamiento de la información	30,00%
APO08.02	Identificar oportunidades, riesgos y limitaciones de TI para mejorar el negocio	40,00%
EDM03.03	Supervisar la gestión de los riesgos	50,00%

Fuente: Elaboración propia.

Los cuestionarios referentes a este componente identificaron las siguientes fortalezas y debilidades por principio:

1. Principio 4.1: La organización obtiene o genera y utiliza información relevante y de calidad para apoyar el funcionamiento del control interno. Las fortalezas para este principio son:

    - El 80% de personas indicó que se realizan validaciones de que la información cumpla con la normativa y legislación aplicable, así como que sea entregada en tiempo y forma.

- El 100% de personas mencionó que los sistemas de información permiten cumplir con los requerimientos (legales, regulatorios, o normativos) de las partes interesadas (funcionarios de CODEA, Junta Directiva, Contraloría General de la República (CGR), Ministerio de Hacienda y Municipalidad).
- El 80% de colaboradores indicó que se identifica la información que se debe generar (diaria, semanal, mensual, trimestral, semestral y anualmente) a las partes interesadas.
- El 100% de colaboradores mencionó que los sistemas de información permiten generar informes sobre los resultados financieros y no financieros de CODEA para la toma de decisiones.
- El 100% de las personas que se les aplicó el cuestionario indicó que la revisión de la información presentada a la junta directiva queda debidamente documentada en las minutas y/o acta.
- El 80% de las personas funcionarias indicó que se cuentan con políticas para uso adecuado de los sistemas de información (políticas de seguridad de información, políticas de uso de los equipos de TI, políticas de riesgos de seguridad de la información).
- El 100% de personas indicó que se tiene definido procesos de comunicación formal y de revisión de términos contractuales y de servicio con los proveedores de CODEA.

1. El 80% de funcionarios mencionó que se tiene establecido un sistema de gestión de la seguridad de la información (SGSI) y políticas de seguridad documentadas formalmente.

En cuanto a sus debilidades destacan:

- El 60% de funcionarios mencionó que no se comunica a la Junta Directiva los resultados de la gestión integral de riesgos.
- El 80% de personas indicó que han ocurrido interrupciones en los sistemas de información.
- El 60% de colaboradores de CODEA indicó que se realizan estudios del entorno que ayuden a identificar las tendencias tecnológicas y cómo pueden aplicarse al CODEA de modo innovador para mejorar el rendimiento de los procesos de negocio.

2. Principio 4.2 La organización comunica la información internamente, incluidos los objetivos y responsabilidades que son necesarios para apoyar el funcionamiento del sistema de control interno. Las fortalezas destacadas en este principio son:

   - El 60% de empleados indicó que se posee controles sobre software maliciosos.
   - El 70% de personas señaló que los sistemas de información producen información oportuna, actual, precisa, completa, accesible, protegida, verificable.
   - El 60% de las personas mencionó que CODEA comunica a los usuarios los posibles riesgos por el uso de los sistemas de información y promueve una cultura de prevención y detección de los mismos.
   - El 80% de los empleados encuestados mencionó que existe comunicación interna que permita evaluar el cumplimiento de objetivos y para proponer mejoras a las deficiencias detectadas para mejorar el Control Interno.

Así mismo las debilidades asociadas a este principio son:

- El 60% de personas afirmó que se han presentado situaciones en las que no se presentó información a partes interesadas en tiempo y forma.
- El 60% de funcionarios indicó que no existen mecanismos para evitar incumplimientos en la información entregada a terceras partes.

3. Principio 4.3: La organización se comunica con los grupos de interés externos sobre los aspectos clave que afectan al funcionamiento del control interno. Las fortalezas para el principio 4.3 son:

    - El 100% de personas indicó que se da el reconocimiento de proveedores mediante contratos u otras certificaciones.
    - El 100% de personas mencionó que se cuenta con canales que permiten una comunicación eficiente con las partes interesadas.

    Únicamente se identificó una debilidad y esta consiste en que el 100% de las personas consultadas respondió que no existe una línea directa para denunciantes, con un proceso prescrito para abordar todos los asuntos que se denuncian y que la junta no revisa la actividad y resolución de la línea directa de denuncias.

Resultados obtenidos para actividades de supervisión. Por último, actividades de supervisión, se realiza la ponderación de cada uno de los principios que conforman este componente, se obtiene una nota del 59,91%, según la matriz utilizada para el análisis este resultado es catalogado como competente y esto se debe a que por medio de los cuestionarios realizados al CODEA se determinó que se han establecido procedimientos internos por medio de los cuales se da seguimiento a los controles establecidos.

A continuación, se muestra el detalle por principio COSO, y el cálculo de la ponderación:

Tabla 16: *Ponderación actividades de supervisión por principio según COSO 2013*

Actividades de supervisión			
Principio	**Nota principal**	**Nota secundarios**	**Nota final**
5.1	0,00%*	49,81%	49,81%
5.2	80,00%	30,00%	70,00%
Promedio de nota final:			**59,91%**

*Nota. Para el cálculo de la nota final del principio 5.1, al no tener "principal" asignado, se le procede a dar un peso del 100% a la nota de "secundarios". Fuente: Elaboración propia.

Alineado con el punto anterior, el análisis realizado para las prácticas de COBIT 5 relacionadas a los principios del componente actividades de supervisión, deja en evidencia que la entidad realiza actividades asociados con, APO10.01 MEA02.01, DSS05.06, DSS06.04, BAI07.01. En todos los casos encuentran por encima del 50% establecido en la matriz, por lo que se catalogan como aceptables, cada una de ellas se detalla a continuación:

Tabla 17: *Ponderación COBIT 5 homologado con el componente de actividades de supervisión de COSO 2013*

Sigla	Nombre	Nota
APO10.01	Identificar y evaluar las relaciones y contratos con proveedores	60,00%
MEA02.01	Supervisar el control interno	66,67%
DSS05.06	Gestionar documentos sensibles y dispositivos de salida	80,00%
DSS06.04	Gestionar errores y excepciones	80,00%
BAI07.01	Establecer un plan de implementación	90,00%

Fuente: Elaboración propia.

No se identifican debilidades relevantes en el cumplimiento de las prácticas de gestión detalladas en la tabla 17, debido a que según la matriz establecida para el análisis todas se sitúan dentro del rango aceptable, con un porcentaje mayor al 50%, razón por la cual no se establece como punto de enfoque para las mejoras que se propondrán.

Los cuestionarios referentes al último componente de control interno identificaron las siguientes fortalezas y debilidades por principio:

2. Principio 5.1: La organización selecciona, desarrolla y realiza evaluaciones continuas y/o independientes para determinar si los componentes del sistema están presentes y funcionando. Las principales fortalezas son las siguientes:

- Por medio de los cuestionarios aplicados, el 60% de los encuestados determinó que se cuenta con informes, métricas y objetivos que permiten evaluar la gestión de riesgos del CODEA.
- 80% de los funcionarios indicó que poseen medidas para retener información por un periodo adecuado, en caso de que se requieran para futuras investigaciones o revisiones para partes interesadas internas y externas.
- 60% de las personas encuestadas reveló que se tienen establecidos criterios de evaluación del rendimiento de los proveedores.
- El 100% de los funcionarios encuestados indicó que se les realizan auditorías ya sea por empresas contratadas o por entidades públicas (incluida la Municipalidad de Alajuela)
- El 100% de los encuestados indicó que se procede a solicitar aprobación por parte de la Junta Directiva para la implementación de nuevos sistemas de TI.
- En cuanto a su debilidad se identificó que el 60% de las personas encuestadas indicaron que en el CODEA no se realizan autoevaluaciones de control interno para conocer su nivel de madurez.

3. Principio 5.2: La organización evalúa y comunica las deficiencias de control interno de forma oportuna a las partes responsables de aplicar medidas correctivas, incluyendo la alta dirección y el consejo, según corresponda. Las fortalezas en el siguiente principio son:
    - Se logra establecer que el 80% de las personas mencionó que se comunican, priorizan y realizan acciones correctivas cuando se identifican riesgos claves.

- Los resultados de la encuesta arrojan que el 80% de las personas encuestadas indicó que se revisan errores, los documentan y los informan, para mantener seguimiento de ellos.
- El 100% de los funcionarios encuestados indicó que existe un proceso para garantizar que las deficiencias identificadas a través de todas las fuentes (evaluación de la gestión, auditorías, partes externas) se mantengan documentadas y generen un historial.
- Por último, se identificó que no existen debilidades específicas asociadas a este principio.

3.3 Análisis de los procesos de CODEA

A continuación, se detallan los procesos relevantes del CODEA.

3.3.1 Jerarquía de procesos relevantes y sus respectivos flujogramas

Se determinaron inicialmente tres áreas que engloban todos los procesos que se presentan en el CODEA, los procesos estratégicos, sustantivos y de apoyo.

En concordancia con lo anterior, cada uno de estos procesos presenta actividades que permite agruparlos. Sin embargo, en esta sección es importante resaltar que en los procesos estratégicos se desarrollan principalmente actividades de aprobación y toma de decisiones, mientras que en los procesos sustantivos corresponden a la serie de acciones desarrolladas para la ejecución de las actividades deportivas, por lo que se determina que en ambos casos no aportan un valor agregado al diagnóstico por realizar del CODEA. Por otra parte, los procesos de apoyo son aquellos llevados a cabo para mantener la operatividad del CODEA.

Por ello, se consideraron únicamente los procesos de apoyo para la jerarquización y

elaboración de flujograma o pruebas de recorrido.

Criterios para la determinación de procesos relevantes dentro del CODEA. Tomando en consideración los puntos más relevantes para la elaboración de una propuesta de fortalecimiento del control interno del CODEA, se establecieron cuatro criterios. Se considera que un proceso es relevante si, y solo si, cumple en su totalidad los cuatro criterios establecidos.

Criterio 1: naturaleza jurídica y normativa aplicable (¿por qué es tan importante en el CODEA?). Si el proceso es considerado relevante dentro de las actividades del CODEA, tiene injerencia en tema legales, reglamentarios o de cumplimiento.

Criterio 2: alto riesgo y fuertes deficiencias en controles. Si durante las actividades de entrevistas, recaudo de información o durante el análisis se determina que el proceso posee fuertes deficiencias en controles y están ligadas a un alto riesgo.

Criterio 3: alta dependencia a sistemas de información (COBIT 5). Si el proceso posee dentro de sus características alta dependencia por el uso de los sistemas de información utilizados en el CODEA, y si además es un proceso que depende en gran medida de que el sistema sea manejado de manera adecuada por el personal a cargo.

Criterio 4: impacto significativo en el control interno (COSO 2013). Se considera que el proceso es relevante si existe la posibilidad de que alguna deficiencia pueda afectar significativamente el funcionamiento adecuado del control interno del CODEA.

Determinación de procesos relevantes dentro del CODEA. A continuación, se resumen los procesos relevantes identificados. Si el proceso cumplía con alguno de los criterios, se colocó en la casilla correspondiente una equis “X”. Si por el contrario no cumple con el criterio la misma, se dejó en blanco.

Tabla 18: *Resumen determinación de procesos relevantes para CODEA*

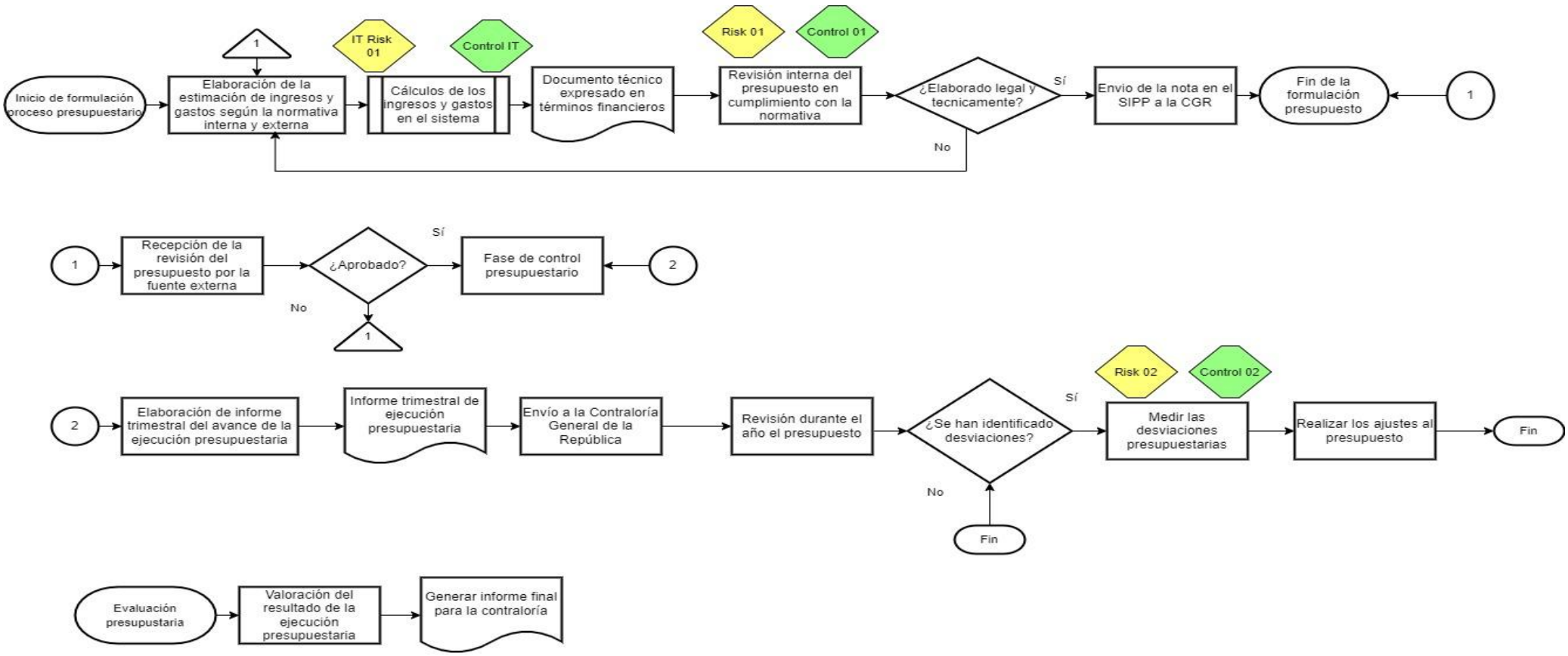
Gestión	Proceso	Criterio 01	Criterio 02	Criterio 03	Criterio 04	Relevancia
Gestión administrativa	Secretaría					0,00%
	Recursos Humanos	X				25,00%
Gestión financiera	Contabilidad			X	X	50,00%
	Presupuesto	X	X	X	X	100,00%
	Tesorería					0,00%
Gestión de compras	Generales compras	X	X	X	X	100,00%
	Específicos de compras	X	X	X	X	100,00%
	Compras por caja chica			X		25,00%
	Devolución de producto (NC).			X		25,00%
Gestión de mantenimiento	Mantenimiento					0,00%
	Misceláneos					0,00%
	Seguridad					0,00%
Gestión de ventas	Ventas locales			X		25,00%
	Ventas tipo servicios			X		25,00%
	Ventas locales en tienda			X		25,00%
	Caja chica			X		25,00%
	Vale de caja			X		25,00%
	Liquidación			X		25,00%
	Reintegros de caja chica			X		25,00%
Gestión de proveeduría	Proceso de inventario		X			25,00%
	Proceso de pago a proveedores	X	X	X	X	100,00%

Fuente: Elaboración propia.

Justificación de los procesos relevantes identificados. A continuación, se detallan los procesos relevantes y no relevantes, con base en los criterios y tablas anteriores, así como su justificación para tal clasificación:

De gestión financiera, el proceso de presupuesto se considera relevante debido a que debe cumplir con aspectos legales y normativos. El proceso de presupuesto depende de los sistemas de información desde su elaboración, ya que requiere la estimación de ingresos y gastos. El proceso presenta deficiencias en cuanto a la comunicación con las partes interesadas y al cumplimiento técnico de algunos requerimientos, por lo tanto, evidencia deficiencias de control. Cualquier deficiencia de control detectada en el proceso de elaboración, control, ejecución y evaluación podría tener implicaciones para CODEA incluso a nivel de sanciones económicas o para sus colaboradores.

Figura 26: *Flujograma del proceso de presupuesto del CODEA*

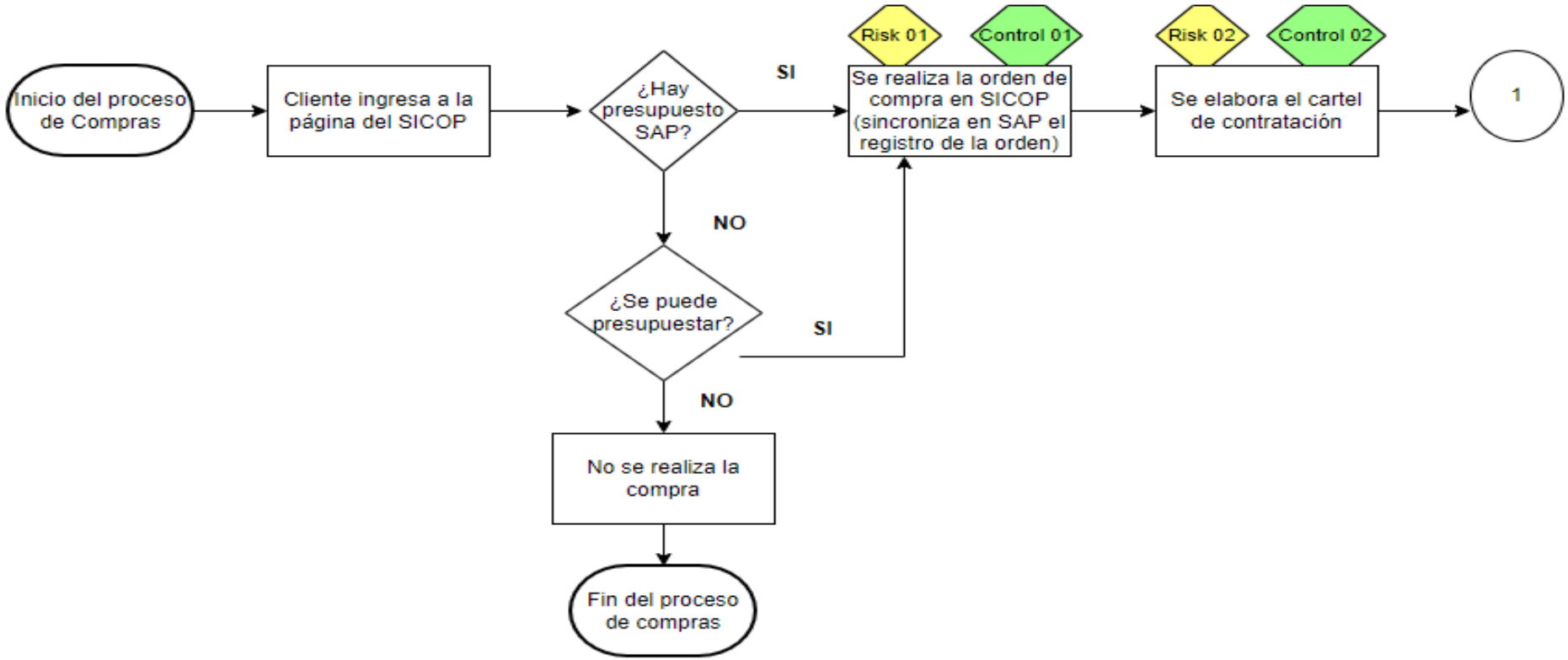


Fuente: Elaboración propia con información suministrada por el personal del CODEA.

Por otra parte, en cuanto a la gestión de compras, se determinó que los procesos generales y específicos de compras son relevantes, puesto que es un proceso de riesgo que tiene injerencia con tema legales, reglamentarios o de cumplimiento. Además, depende en gran medida de los sistemas de información y genera un impacto significativo en el funcionamiento del control interno. Esto sucede porque el proceso de compra debe considerar una necesidad de contratación o compra significativa, ya que esta se debe de verificar con el presupuesto que tiene CODEA y de esta manera establecer si se puede dar o no. Además, se debe adaptar a todos los requerimientos y procedimientos establecidos por Ley.

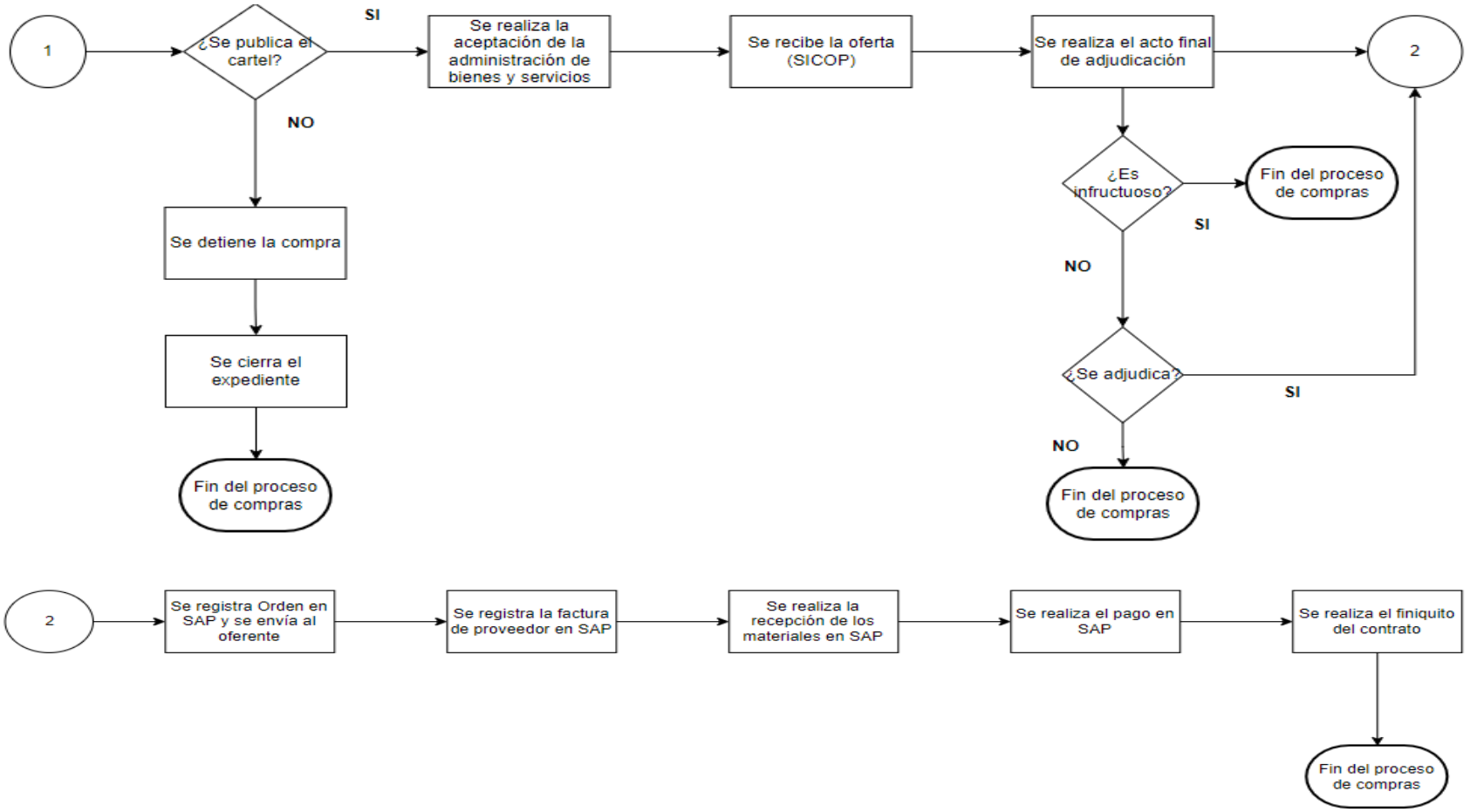
Asimismo, este proceso depende mucho de los sistemas de información, ya que se debe crear un socio de negocio en SAP para poder crear el cartel en SICOP y de esta forma poder sincronizar ambas bases de datos (ver el flujograma de la figura 27).

Figura 27: *Flujograma del proceso de compras del CODEA*



continúa…

…continuación



Fuente: Elaboración propia con información suministrada por el personal del CODEA.

Por último, en relación con la gestión de proveeduría se determinó que el proceso de pago a proveedores es relevante, ya que posee deficiencias en controles y altos riesgos detectados, tiene injerencia con tema legales, reglamentarios o de cumplimiento, depende en gran medida de los sistemas de información y genera un impacto significativo en el funcionamiento del control interno (ver detalle en la tabla 18).

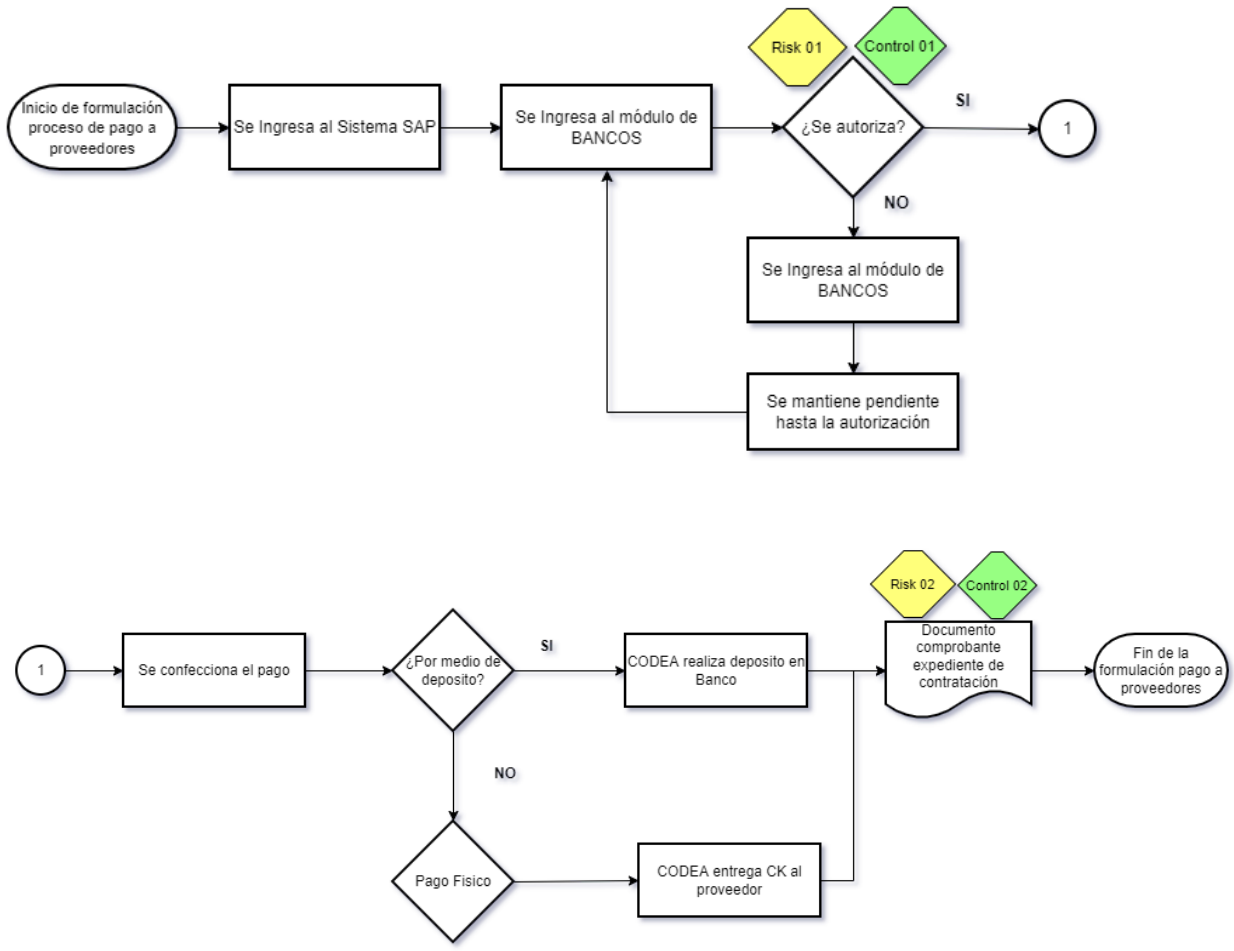
Lo anterior debido a que el proceso de licitación por medio del cual se lleva a cabo la contratación del proveedor, el pago y además las condiciones de las transacciones que se realizarán durante el tiempo del contrato es riguroso y de cumplimiento estricto, lo cual afecta temas legales y de cumplimiento.

Cabe rescatar que los controles determinados corresponden a los de cumplimiento por ley y no a controles internos para la reducción del riesgo de que el pago a proveedores contenga errores, desviaciones o no posea autorizaciones, lo cual puede generar retrasos o ausencia de pago. Esto queda en evidencia en el flujograma de este proceso realizado por la entidad, donde se refleja la no determinación de los riesgos y controles no asociados. En dicho flujograma se indica que no se requieren autorizaciones por parte del director administrativo para realizar pagos y que si el pago es realizado de manera física no se documenta el expediente de contratación.

Adicionalmente, se determina que el pago a proveedores, al significar desprendimiento de recursos monetarios de la entidad, requiere que los controles de revisión y autorización sean adecuados si se considera el riesgo que el efectivo por su naturaleza tiene.

Además, el proceso de pago a proveedores es llevado a cabo por medio del sistema SAP implementado recientemente, por lo que depende de este sistema en gran medida y es realizado por el personal contable del CODEA. Ello requiere de autorizaciones, lo cual podría considerarse como un control del proceso (ver flujograma de la figura 28).

Figura 28: *Flujograma del proceso de proveedores del CODEA*



Fuente: Elaboración propia con información suministrada por el personal del CODEA.

En cuanto a los demás procesos, no se consideran relevantes a efectos de este estudio, debido a que no tienen injerencia con tema legales, reglamentarios o de cumplimiento, no poseen deficiencias en controles y altos riesgos detectados. Además, no dependen en ninguna medida de los sistemas de información y no generan impacto significativo en el funcionamiento del control interno.

3.4 Diagnóstico de la situación actual del control interno de CODEA con base en lo establecido por COSO 2013 y por COBIT 5 para el componente de información y comunicación

En esta sección, se detallan los riesgos identificados en el proceso de análisis, con base en la información recabada en los formularios aplicados a los funcionarios del CODEA y los flujogramas elaborados de los procesos más relevantes identificados en la sección anterior.

3.4.1 Identificación de riesgos generales

De acuerdo con el análisis realizado, los riesgos generales identificados corresponden a los siguientes:

- Continuidad del CODEA/negocio en marcha.
- Disminución de niveles de productividad en las funciones de procesos de apoyo (ante la ausencia de un código de ética y la ausencia de protocolos ante eventuales interrupciones de los sistemas).
- Pérdida de imagen y credibilidad pública (ante la ausencia de un código de ética).
- Desconocimiento de hechos irregulares dentro del CODEA.

- No consecución de uno o más de los objetivos establecidos en el plan operativo anual.
- Cuestionamiento de la suficiencia y confiabilidad de la información generada por el CODEA.
- Pérdida de información (copias de seguridad, interrupciones, flujograma de pago proveedores).
- Toma de decisiones estratégicas debilitadas por la falta de conocimiento de las fortalezas, oportunidades, debilidades y amenazas del CODEA.
- Toma de decisiones estratégicas debilitadas por el desconocimiento del nivel de madurez del control interno.
- Sanciones externas que limiten la operatividad del CODEA.
- Errores, desviaciones, retrasos, fallo en el pago a proveedores.

3.4.2 Identificación de riesgos específicos

De acuerdo con el análisis realizado, los riesgos específicos identificados corresponden a los siguientes:

- Preparación insuficiente del CODEA ante posibles cambios internos y externos en aspectos económicos, legales regulatorios, ambientales, sociales, tecnológicos y otros.

- Riesgos de capacidad y rendimiento enfocados al negocio en marcha afectado por desastres naturales, pérdida de personal, cambios abruptos.
- Asignación de recursos y capacidades erróneas.
- Desconocimiento del impacto en el negocio de disponibilidad, rendimiento y capacidad de recursos.
- Desconocimiento de los procesos ante falta de manuales.
- Riesgo en duplicidad de documentos.

3.4.3 Evaluación de riesgos por matrices de calor

A continuación, se explicará el procedimiento para evaluar los riesgos por medio de matrices de calor.

3.4.3.1 Determinación de parámetros. Se establecieron inicialmente los parámetros por medio de los cuales se realiza el análisis de los riesgos identificados en las etapas previas. Estos se determinaron tomando en cuenta los procesos, tipos de riesgos, así como la importancia de prevenir, detectar y mitigar los riesgos más relevantes identificados. A continuación, se detallan los parámetros utilizados:

Categoría del riesgo. Se establece la naturaleza del riesgo este parámetro se utiliza en la etapa de identificación y corresponden a los siguientes: cambios en el entorno, disponibilidad de recursos, factor humano, infraestructura, personas usuarias, seguridad, ética, tecnología de información, eventos antrópicos, desastres naturales, operativo.

Procesos. Se establece si el riesgo tiene relación con los procesos analizados, en este caso, estratégico o de apoyo. Dicho parámetro es utilizado en la etapa de identificación.

Impacto. Para la etapa de análisis se establece el parámetro de impacto, el cual hace referencia a nivel general que se causa como efecto del riesgo y se determina según la escala de la tabla 19.

Tabla 19: *Determinación de impacto de riesgo*

Impacto	Valor
No aplica	0%
Muy bajo	1%
Bajo	10%
Moderado	20%
Alto	40%
Muy alto	80%

Fuente: Elaboración propia.

Probabilidad. Este parámetro es determinado para la etapa de análisis y hace referencia a cuál es la probabilidad que se espera un riesgo ocurra y se evalúa con base en la tabla 20.

Tabla 20: *Determinación de probabilidad de riesgo*

Probabilidad	Descripción	Desde		Hasta
Remoto	Evento improbable	0	<=	10%
Bajo	Poco probable que suceda	> 10%	<=	30%
Moderado	Evento ocasional	> 30%	<=	50%
Alto	Gran posibilidad que suceda	> 50%	<=	70%
Muy alto	Evento prácticamente inevitable	> 70%	<=	90%

Fuente: Elaboración propia.

Estrategia. Este parámetro es determinado para la etapa final de respuesta a los riesgos que pasaron por el análisis y hace referencia a la recomendación de cómo la entidad debe administrar los riesgos. Se pueden observar las diferentes estrategias en la siguiente tabla:

Tabla 21*: Determinación de estrategia de riesgo*

Estrategia
Amenaza - Prevenir
Amenaza - Transferir
Amenaza - Mitigar
Amenaza - Aceptar
Oportunidad - Explorar
Oportunidad - Mejorar
Oportunidad - Compartir
Oportunidad - Aceptar

Fuente: Elaboración propia.

Estatus. Este parámetro hace referencia a un aspecto de seguimiento por parte de la entidad una vez realizado el análisis sobre el estatus actual del riesgo, el cual se evalúa de acuerdo a las categorías: activo, pasado y cancelado.

3.4.3.2 Identificación de los riesgos (causas y consecuencias). De acuerdo con los parámetros establecidos y los riesgos identificados en las etapas previas, se procedió a categorizar los riesgos de acuerdo con su descripción, causas y consecuencias, esto para tener más facilidad a la hora de iniciar la etapa de análisis.

Para ello, se analizó el riesgo que se tenía identificado y se determinó la causa del por qué era un riesgo para el CODEA. Las causas más relevantes fueron la ausencia de un SEVRI o manuales estipulados para la gestión de riesgos, la falta de copias de seguridad de la información, la carencia de análisis FODA, la inexistencia de un código de ética documentado y el hecho de que se ha trabajado con el mismo presupuesto por dos períodos seguidos (2020-2021) debido a desaprobaciones por parte de la Contraloría General de la República. Todo ello puede repercutir negativamente en la gestión integral del CODEA.

3.4.3.3 Análisis de los riesgos. En el análisis de riesgos se determina la probabilidad de que el riesgo se materialice, y el nivel de impacto en la gestión del CODEA. Al multiplicar la probabilidad de ocurrencia del riesgo y su impacto, se obtiene el riesgo inherente.

3.4.3.4 Matriz de calor. La matriz de calor se utiliza para clasificar los diferentes riesgos generales de acuerdo con su probabilidad de ocurrencia e impacto. Con ello, se catalogan como riesgo alto, medio o bajo de riesgo inherente. El riesgo alto, medio y bajo se presentan en color rojo, amarillo y verde respectivamente. Dicha matriz categoriza la exposición al riesgo (riesgo inherente) sin considerar los posibles controles. A continuación, en la tabla 22 se muestra la matriz y la cantidad de riesgos por color:

Tabla 22: *Matriz de riesgos de calor*

Riesgo	Probabilidad	Probabilidad	Impacto	Impacto	Nivel riesgo
Continuidad del CODEA/negocio en marcha.	**Rara**	**1**	**Catastrófico**	**5**	**Riesgo inherente bajo**
Desconocimiento de hechos irregulares dentro del CODEA.	**Inusual**	**2**	**Grave**	**4**	**Riesgo inherente moderado**
Errores, desviaciones, retrasos, falta de pago a proveedores.	**Poco probable**	**3**	**Grave**	**4**	**Riesgo inherente alto**
Cuestionamiento de la suficiencia y confiabilidad de la información generada por el CODEA.	**Poco probable**	**3**	**Grave**	**4**	**Riesgo inherente alto**
Sanciones externas que limiten la operatividad del CODEA.	**Poco probable**	**3**	**Grave**	**4**	**Riesgo inherente alto**
Disminución de niveles de productividad en las funciones de procesos de apoyo.	**Muy probable**	**4**	**Catastrófico**	**5**	**Riesgo inherente extremo**
No consecución de uno o más de los objetivos establecidos en el plan anual operativo.	**Muy probable**	**4**	**Catastrófico**	**5**	**Riesgo inherente extremo**

Pérdida de información.	**Muy probable**	**4**	**Catastrófico**	**5**	**Riesgo inherente extremo**
Toma de decisiones estratégicas debilitadas por el desconocimiento del nivel de madurez del control interno.	**Recurrente**	**5**	**Grave**	**4**	**Riesgo inherente extremo**
Toma de decisiones estratégicas debilitadas por la falta de conocimiento de las fortalezas, oportunidades, debilidades y amenazas del CODEA.	**Recurrente**	**5**	**Grave**	**4**	**Riesgo inherente extremo**

Fuente: Elaboración propia.

3.4.4 Resultados obtenidos

Para el componente de entorno de control se determinó que sus deficiencias más significativas se relacionan con la falta de un código de ética documentado que sea divulgado por todos los niveles organizacionales. Sin embargo, se ha desarrollado una cultura que resalta la importancia del comportamiento íntegro y ético por medio la comunicación verbal y mediante el ejemplo, las actuaciones, compromisos y actuaciones de los miembros de la junta directiva y de la administración.

Se identificó que no existen canales de comunicación anónimos que permitan a los colaboradores informar sobre conductas ilegales, no ética o indebida, o comunicar de manera confidencial sobre temas relacionados a la imagen de CODEA, calidad de los trabajos, soborno y corrupción. Además, se concluyó que no existen estrategias que permitan a las personas funcionarias contar con transferencia de conocimientos y capacitaciones para mejorar sus

funciones y que existe una falta de políticas de recursos humanos documentadas e informadas a todos los niveles de la entidad. Por último, la falta de un manual de puestos debidamente actualizado genera un desconocimiento generalizado que no permite comprender y conocer las funciones aplicables a cada uno de los puestos.

Una vez realizado el análisis para evaluación de riesgos, se determina que es el componente más afectado por los resultados obtenidos, esto debido principalmente a que carecen de un Sistema Específico de Valoración de Riesgos Institucional (SEVRI) u otro mecanismo para la administración y supervisión de los riesgos. Asimismo, el CODEA actualmente no posee actividades, herramientas o procesos que estén ligados a la mejora de este componente.

Un aspecto relevante de la evaluación de riesgos es que tiene injerencia directa en los resultados de los demás componentes, ya que en cada uno de ellos se manifiestan riesgos que no están siendo identificados, analizados y monitoreados, lo que significa que es un área de mejora potencial determinada.

En cuanto al componente de actividades de control, se identificó que se encuentra debilitado, esto a raíz de que no existen actividades debidamente definidas y formalizadas que contribuyan a identificar, analizar y evaluar los procesos del CODEA, así como la mejora continua de los mismos. Además, no se cuenta con políticas de prevención y detección de riesgos que permitan generar estrategias de respuesta a los mismos.

Por otra parte, a nivel de TI, no se realizan copias de seguridad de los archivos con los que se trabaja y no se tiene políticas ni procedimientos que permitan asegurar la confidencialidad, integridad y seguridad de la información y datos del CODEA.

Por otro lado, se determina que, para el componente de información y comunicación, hay deficiencias en la comunicación interna del personal y las áreas internas del CODEA, ya que hay ocasiones en donde no se presenta la información en la forma correcta. Además, otro punto a considerar es que no se cuenta con un plan de capacitación que permita a sus funcionarios mantener sus conocimientos actualizados.

Con respecto al componente actividades de supervisión, se determina que en el CODEA no se realizan actividades de autoevaluación de control interno. Además, no se realizan procesos de identificación de riesgos, por lo que no existe un monitoreo adecuado de los mismos. Sin embargo, se determinó que se realizan auditorías internas y externas de TI, operativas y financieras que de manera directa ayudan a solventar los procesos de supervisión y a disminuir los riesgos que pueden afectar a este componente

Capítulo 4

Diseño de la propuesta de fortalecimiento de control interno para CODEA

4.1 Objetivos de la propuesta

Los objetivos que se plantearon para realizar la propuesta de fortalecimiento para el CODEA son los siguientes:

Objetivo general de la propuesta

Definir un sistema de valoración de riesgos que le permita al CODEA identificar, analizar y definir acciones de administración de los riesgos que podrían afectar negativamente en el logro de los objetivos y metas institucionales.

Objetivos específicos de la propuesta

1. Contar con una herramienta que permita ejecutar y documentar el proceso de identificación, análisis y respuesta a los riesgos.
2. Mitigar los efectos negativos generados ante la ausencia de un Sistema Específico de Valoración de Riesgos Institucional (SEVRI).
3. Establecer una base de valoración de riesgos que agilice una futura implementación del Sistema Específico de Valoración de Riesgos Institucional (SEVRI).
4. Incentivar buenas prácticas asociadas a la valoración de riesgos derivados del uso de las Tecnologías de Información (TI).

4.2 Aplicación de los criterios técnicos base para el diseño de la propuesta de control interno

A continuación, se expondrán los criterios técnicos que se utilizaron para el adecuado diseño de la propuesta de control interno.

4.2.1 COSO 2013

La propuesta pretende incorporar elementos fundamentales de COSO 2013, los cuales corresponden a los siguientes:

- Orientado a la consecución de los objetivos del CODEA: Tales objetivos pueden ser operacionales, de presentación de informes y de cumplimiento. Se espera que la herramienta proporcione a la organización una mayor probabilidad en el cumplimiento de objetivos relacionados con la presentación de informes, el cumplimiento de la regulación vigente, y los operativos del funcionamiento de la entidad (COSO, 2013).

- Capaz de proporcionar una seguridad razonable, no una seguridad absoluta para la Administración y la Junta Directiva: Ya que la herramienta reconoce que pueden existir incertidumbres y riesgos, que no se puede predecir con seguridad. Por lo que, se pretende aumentar la probabilidad del cumplimiento de objetivos mejorando la identificación, análisis, y monitoreo de los riesgos (COSO, 2013).

- Adaptable a la estructura del CODEA: La herramienta tiene una aplicación flexible para toda la entidad de acuerdo con su naturaleza, así como las leyes y demás normativa que le aplican (COSO, 2013).

- Involucramiento de las personas: Considera la necesidad de no solamente considerar políticas y procedimientos documentados, sino también el involucramiento de las personas a todos los niveles de la entidad y con las acciones para efectuar el control interno. Con la herramienta se pretende asignar responsabilidades y concientizar sobre la importancia del proceso de gestión de riesgos. (COSO, 2013).

- Proceso continuo: Ya que es un medio para un fin, no un fin en sí mismo. Por lo que la herramienta pretende que el proceso de identificación, análisis y monitoreo de riesgos sea dinámico e iterativo, que se adapte a las necesidades de la entidad, y con ello lograr que sus operaciones sean efectivas (COSO, 2013).

- Congruente con la misión y visión, estrategias, y objetivos del CODEA: La herramienta pretende estar alineada con todos los principios de gestión del CODEA.

- Apoyar a la organización con sus esfuerzos en la mejora del control interno, principalmente con el componente de evaluación de riesgos, y así como; mejorar los demás cuatro componentes de control (COSO, 2013).

4.2.2 COBIT 5

Mediante la sugerencia de diferentes controles, la herramienta pretende generar un mayor acercamiento del CODEA hacia COBIT 5 en los siguientes aspectos:

- DSS06.02 Controlar el procesamiento de la información: Que el procesamiento de la información en el CODEA sea válido, completo, preciso, oportuno y seguro (ISACA, 2012).

- APO08.02 Identificar oportunidades, riesgos y limitaciones de TI para mejorar el negocio: Identificar oportunidades potenciales en el CODEA para que la TI sea catalizadora de la mejora del rendimiento institucional (ISACA, 2012).

- EDM03.03 Supervisar la gestión de riesgos: Establecer cómo las desviaciones o los problemas serán identificados, seguidos e informados para su resolución dentro del CODEA (ISACA, 2012).

- APO13.03 Supervisar y revisar el Sistema de Gestión de Seguridad de la Información (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 (ISACA, 2012).

- DSS05.01 Proteger contra software malicioso (malware): Implementar y mantener efectivas medidas, preventivas, de detección y correctivas a lo largo de la institución para proteger los sistemas de información y tecnología del software malicioso (por ejemplo, virus, gusanos, software espía –spyware- y correo basura) (ISACA, 2012).

- EDM02.01 Evaluar la optimización de valor: Evaluar continuamente las inversiones en activos de TI para determinar la probabilidad de alcanzar los objetivos del CODEA y aportar valor a un coste razonable (ISACA, 2012).

- 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 institución y solución

propuesta.

- EDM02.02 Orientar la optimización del valor: Orientar los principios y las prácticas de gestión de valor para posibilitar la realización del valor óptimo de las inversiones en los sistemas del CODEA (ISACA, 2012).

- APO08.04 Coordinar y comunicar: Trabajar con las partes interesadas y coordinar de extremo a extremo la entrega de los servicios TI (ISACA, 2012).

- BAI02.01 Definir y mantener los requerimientos técnicos y funcionales de negocio: Identificar, priorizar, especificar y acordar los requerimientos de información del CODEA, funcionales, técnicos y de control que cubra el alcance/entendimiento de todas las iniciativas necesarias para alcanzar los resultados esperados (ISACA, 2012).

- 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 estén alineados con los objetivos institucionales (ISACA, 2012).

- DSS05.02 Gestionar la seguridad de la red y las conexiones: Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión (ISACA, 2012).

- 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 (ISACA, 2012).

- APO10.03 Gestionar contratos y relaciones con proveedores: La herramienta fomentará, el mejoramiento del proceso de comunicación formal y de revisión de términos contractuales y de servicio con los proveedores del CODEA (ISACA, 2012).

- BAI04.04 Supervisar y revisar la disponibilidad y la capacidad: La herramienta fomentará, la adecuada preparación y presentación de informes referentes al desempeño y disponibilidad de los recursos (humanos, materiales y presupuestarios) (ISACA, 2012).

- EDM02.03 Supervisar la optimización de valor: Supervisar los indicadores clave y sus métricas para determinar el grado en que el negocio está generando valor público y generar informes (ISACA, 2012).

- EDM05.01 Evaluar los requisitos de elaboración de informes de las partes interesadas: 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 (ISACA, 2012).

- EDM05.02 Orientar la comunicación con las partes interesadas y la elaboración de informes: 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 (ISACA, 2012).

4.3 Diseño de la propuesta

Para contextualizar la propuesta de fortalecimiento para el CODEA, se procede a describir la propuesta, así como su proceso, costo-tiempo y beneficios que esta generará con su implementación.

4.3.1 Descripción general de la propuesta

La presente propuesta se denomina “Sistema de Gestión de Valoración de Riesgos Transitoria” (Ver anexo N), la misma consiste en generar una metodología de valoración de riesgos para que el CODEA pueda implementar temporalmente mientras se define las líneas estratégicas de la institución y por ende un Sistema Específico de Valoración de Riesgos Institucional (SEVRI).

Se toma la decisión de realizar este modelo como propuesta final debido a que, con los análisis realizados en los capítulos previos, el componente de valoración de riesgos es el que requiere de mayor atención debido a su poco nivel de desarrollo y aplicación. Además, se determina que al realizar este modelo se le otorga al CODEA una herramienta que les sistematiza el proceso de identificación de riesgos y la definición de medidas ante riesgos que permitan su tratamiento, esto impacta positivamente en el proceso de planificación que la institución desee desarrollar y a su vez, brinda una seguridad razonable sobre la consecución de sus objetivos.

Este modelo contempla cinco fases que el CODEA deberá llevar a cabo para su aplicación, a continuación, el detalle de cada una:

a) Fase 1 identificación de riesgos: Esta fase consiste en realizar un proceso de identificación de riesgos, para esto se brinda la opción de utilizar como base

un Inventario de Riesgos[8] predefinido el cual se encuentra basado en el Modelo de Riesgo Proviti y en el Modelo de Estructura de Riesgos de la Contraloría General de la República. En este inventario se puede observar un listado de riesgos clasificados de acuerdo con los modelos citados anteriormente, así mismo cada riesgo posee una pregunta de sí o no que permite a los usuarios identificar la existencia del riesgo en la institución y, además, también tiene asociado una posible acción a implementar para dar respuesta a dicho riesgo.

Es importante indicar que el Modelo de Riesgo Protiviti realiza una clasificación de los riesgos en tres bloques: 1) Riesgos del entorno, 2) Riesgos de información para la toma de decisiones y 3) Riesgos de procesos. A esta primera clasificación le llamaremos "Clasificación 1".

Tabla 23: *Cantidad de riesgos por clasificación 1*

Clasificación 1	Cantidad de riesgos
Riesgos del entorno	5
Riesgos de información para la toma de decisiones	13
Riesgos de procesos	40
Suma total	**58**

Fuente: Elaboración propia.

[8] Ver anexo M Inventario de Riesgos suministrado al CODEA con la Herramienta de Evaluación de Riesgos Transitoria.

En cuanto al Modelo de Estructura de Riesgos de la Contraloría General de la República, este utiliza como referencia el Modelo de Riesgo Protiviti, sin embargo, realiza una segunda clasificación que permite un mayor entendimiento sobre la naturaleza del riesgo. A esta segunda clasificación le llamaremos Clasificación 2.

Tabla 24: *Cantidad de riesgos por clasificación 2*

Clasificación 2	Cantidad de riesgos
Ambiental	1
Información pública	1
Reputación	1
Humanos	2
Información operativa	2
Social	2
Estratégicos	3
Financieros	3
Dirección	4
Gobierno	4
Integridad	4
General	5
Información de gestión	5
Información estratégica	5
Tecnologías de la información	6
Operacionales	10
Suma total	**58**

Fuente: Elaboración propia

Cabe agregar, que ambos modelos fueron utilizados únicamente como referencia, ya que se realizaron las adaptaciones y ajustes necesarios para la naturaleza y realidad institucional del CODEA.

b) Fase 2 evaluación y análisis de riesgos: la segunda fase consiste en evaluar y analizar los riesgos identificados. En este proceso deberá documentar y justificar el análisis realizado a cada riesgo.

Primeramente, se debe determinar el valor del impacto tomando en consideración tres factores, los cuales son: impacto operativo, impacto legal y regulatorio, e impacto de imagen y credibilidad pública. Ver Tabla 25.

Tabla 25: *Factores que influyen en el impacto*

Operativo	Legal y regulatorio	Imagen y credibilidad pública
Se refiere a la operación normal de los procesos del CODEA, considerando los términos de productividad, eficiencia, eficacia y economía.	Se refiere al cumplimiento de la normativa legal y regulatoria vigente y sus consecuencias en caso de incumplimiento.	Se refiere al nivel de impacto que la situación puede generar sobre la percepción de la imagen institucional del CODEA en el público.

Fuente: Elaboración propia.

Luego de considerar estos tres factores, el nivel de impacto se realiza asignando un valor al riesgo en una escala del 1 al 5, siendo el nivel 1 el más bajo, como categoría menor, y el 5 como el nivel más alto, como categoría catastrófica.

Tabla 26: *Escala para determinar el nivel de impacto de cada riesgo*

Valor	Categoría	Descripción
5	Catastrófico	Riesgo cuya materialización influye directamente en el cumplimiento de la misión, visión y objetivos de la institución; asimismo puede implicar pérdida patrimonial o daño de la imagen, dejando además sin funciones total o parcialmente por un periodo importante de tiempo, afectando los programas o servicios que entrega la institución.
4	Grave	Riesgo cuya materialización podría dañar de manera significativa el patrimonio institucional, daño a la imagen y limitaciones al logro de los objetivos estratégicos. Asimismo, se necesita un periodo de tiempo considerable para restablecer la operación o corregir los daños.
3	Moderado	Riesgo cuya materialización causaría una pérdida importante en el patrimonio o un daño en la imagen institucional.
2	Bajo	Riesgo que no afecta el cumplimiento de los objetivos estratégicos y que en caso de materializarse podría causar daños al patrimonio o imagen, que se puede corregir en poco tiempo
1	Menor	Riesgo que en caso de materializarse podría tener efectos muy pequeños en la institución.

Fuente: Elaboración propia con base en la *Guía de Autoevaluación de Riesgos en el Sector Público* (Auditoría Superior de la Federación, 2014, p.22).

Seguidamente, se debe determinar la probabilidad de que el evento suceda, por lo que nuevamente se asigna otro valor al riesgo en una escala del 1 al 5, donde el 1 representa riesgo de ocurrencia raro, y el 5 una ocurrencia recurrente.

Tabla 27: *Escala para determinar la probabilidad de ocurrencia de cada riesgo*

Valor	Probabilidad	Descripción
5	Recurrente	Riesgo cuya probabilidad de ocurrencia es muy alta, es decir, se tiene plena seguridad que éste se materialice, tiende a estar entre 90% y 100%.
4	Muy probable	Riesgo cuya probabilidad de ocurrencia es alta, es decir, se tiene entre 75% a 95% de seguridad que éste se materialice.
3	Poco probable	Riesgo cuya probabilidad de ocurrencia es media, es decir, se tiene entre 51% a 74% de seguridad que éste se materialice
2	Inusual	Riesgo cuya probabilidad de ocurrencia es baja, es decir, se tiene entre 25% a 50% de seguridad que éste se materialice.
1	Rara	Riesgo cuya probabilidad de ocurrencia es muy baja, es decir, se tiene entre 1% a 25% de seguridad que éste se materialice.

Fuente: Elaboración propia con base en la *Guía de Autoevaluación de Riesgos en el Sector Público* (Auditoría Superior de la Federación, 2014, p.22).

Finalmente, cuando se asignen los valores para determinar el nivel de impacto y probabilidad del riesgo, estos deberán de multiplicarse. El resultado final será valorado en escalas que irán aumentando en 5 puntos hasta alcanzar 25 puntos.

Tabla 28: *Escala para determinar el riesgo inherente*

Escala	Nivel de riesgo	Descripción
16-25	Extremo	Riesgo cuya materialización influye directamente en el cumplimiento de logros objetivos, metas, imagen, continuidad y negocio en marcha del CODEA.
11-15	Alto	Su materialización podría dañar de manera significativa a la institución.
6-10	Moderado	Los efectos no afectan en gran medida a la institución si el riesgo llega a materializarse.
1-5	Bajo	Efectos menores a la institución si el riesgo llega a materializarse.

Fuente: Elaboración propia.

c) Fase 3 riesgo residual: "Es el nivel de riesgo después de aplicar las actividades de control para su administración" (Contraloría General de la República [CGR] , 2011, p.23).

En línea con el concepto de riesgo residual establecido por la CGR, la entidad deberá valorar nuevamente los riesgos, tomando en consideración los controles existentes. Este nuevo análisis determinará una nueva probabilidad de ocurrencia e impacto, de manera que se establecerá un nuevo nivel de riesgo conocido como riesgo residual.

El cálculo del riesgo residual se realizará de la siguiente manera:

Valor de la probabilidad considerando controles existentes * Valor del impacto considerando controles existentes = Riesgo residual

De acuerdo con el nivel de riesgo residual arrojado por la herramienta, la entidad deberá decidir cuál será la respuesta al riesgo a implementar.

d) Fase 4 respuesta al riesgo: en esta fase se realiza el proceso de dar respuestas a los riesgos. La respuesta a los riesgos consiste en la decisión que toma la entidad sobre qué hacer con el riesgo, en este sentido existen las siguientes cuatro posibilidades a considerar:

    1. Aceptar el riesgo: La entidad decide no ejecutar acciones ya sean preventivas o correctivas de los riesgos y decide aceptar las consecuencias. En este sentido, la Antología Curso PC-0425 Control Interno Y Auditorias Especiales V3.1 2018 pg. 59 indica que generalmente las entidades toman esta acción cuando las "... consecuencias son pequeñas y el esfuerzo para mitigarlo o transferirlo es mucho. No es posible dar otro tipo de respuesta"

    2. Transferir el riesgo: Se da en los casos en los que existe la posibilidad de "trasladar el impacto total o parcial de un riesgo a un tercero, junto con la responsabilidad por la respuesta" (Antología Curso PC-0425 Control Interno Y Auditorias Especiales V3.1 2018 pg. 59) ya que este genera un costo asociado y generalmente hace referencia a seguros, contratos, garantías.

    3. Mitigar el riesgo: El impacto del riesgo se puede disminuir mitigando sus consecuencias, si se hace realidad, a través de la creación y aplicación de controles que permitan tal fin. (Antología

Curso PC-0425 Control Interno Y Auditorias Especiales V3.1 2018 pg. 60)

4. Prevenir el riesgo: Se considera una de las mejores acciones ya que hace referencia a un enfoque proactivo, es decir es más sencillo y económico prevenir que posteriormente reparar daños causados.

Es por esto que, junto con el inventario de riesgos predeterminado, se generaron posibles controles que el CODEA podría aplicar para la prevención y/o mitigación del riesgo de acuerdo con su naturaleza y realidad institucional.

Así mismo, estos controles serán sugeridos únicamente a aquellos riesgos que superen la tolerancia al riesgo predefinida por la entidad.

e) Fase 5 comunicación de resultados: esta fase consiste en documentar y comunicar los resultados obtenidos del proceso de valoración de riesgos al jerarca, esto con el fin de que la información generada sea de insumo para la toma de decisiones institucionales.

Para la comunicación de resultados el encargado deberá:

1. Comentar los resultados obtenidos al Jerarca de la entidad, en este caso al Director Administrativo y a la Junta Directiva del CODEA.
2. Presentar un expediente del proceso de valoración de riesgos realizado con el objetivo de determinar las acciones correspondientes para la administración de riesgos.
3. Girar las instrucciones necesarias a los responsables designados en la implementación de los controles de tratamiento a los riesgos.

4.3.2 Proceso de la aplicación de la propuesta

Se recomienda que la implementación de esta propuesta se realice de acuerdo con las siguientes tres fases:

- Fase 1 capacitación sobre la propuesta: Se debe realizar una reunión con el personal del CODEA para que conozcan su uso, así como el beneficio que generará. En esta reunión se explicarán las cinco fases del modelo y el diseño de este.
- Fase 2 aplicación piloto de la propuesta: Una vez realizada la capacitación y abarcando todas las consultas que la herramienta puede generar en el personal, se recomienda realizar la aplicación de esta, ya que es en esta fase se evaluará su funcionamiento, así como su manejo.
- Fase 3 implementación formal de la propuesta: Se le recomienda a la administración el implementar de manera formal el uso de la propuesta. Asimismo, se debe considerar que para este punto se le debe de recordar a los altos mandos del CODEA que la periodicidad de la valoración de riesgos es de al menos una vez al año.

4.3.2.1 Diseño I de la propuesta basada en COBIT 5. Para el diseño de la propuesta basada en COBIT 5, se tomó como referencia la identificación y análisis de sus procesos realizada en el capítulo anterior, esto para la construcción del inventario de riesgos.

Como bien se ha mencionado en puntos anteriores, mediante el inventario de riesgos predeterminado, se procede a sugerir controles para que el CODEA pueda tratar los riesgos identificados, algunos de estos controles toman como base las mejores prácticas de COBIT 5 que son aplicables al CODEA. (Ver anexo L)

4.3.2.2 Diseño II de la propuesta basada en COSO 2013. COSO 2013 también fue utilizado con el fin de generar el inventario de riesgos, esto mediante la identificación de posibles riesgos que se generarían a raíz de desviaciones según con lo establecido por este marco, así como las posibles medidas que se deberían implementar para su tratamiento.

4.3.3 Costos y tiempo en la aplicación de la propuesta en CODEA

En este apartado se procede a realizar el cálculo en costo y tiempo de la realización de la propuesta para su aplicación en el CODEA.

4.3.3.1 Costo en tiempo. El costo en tiempo resulta del estimado en horas de trabajo en las que se espera cumplir con la propuesta tomando en cuenta las etapas y los detalles que cada una de ellas conlleva, adicional se toma en cuenta que la propuesta es realizada por 4 personas por ende se estima dicha cantidad de profesionales. A continuación, se presenta el detalle de las etapas, así como las horas estimadas de cada una de ellas:

Tabla 29: *Cálculo de costo en tiempo de la propuesta*

Etapas	Profesional 1	Profesional 2	Profesiona l 3	Profesional 4	TOTAL Individuales	Horas Conjuntas (x4)
1. Proceso de planeación	**4**				**4**	
2. Elaboración del inventario de Riesgos	**7**	**7**	**7**	**7**	**28**	**12**
Identificación	2	2	2	2	8	2
Evaluación y Análisis	1	1	1	1	4	4
Respuesta al Riesgo	3	3	3	3	12	4
Riesgo Residual	1	1	1	1	4	2
Comunicación de Resultados				1	1	2
3. Elaboración de la Herramienta						**15**
4. Elaboración de la Guía	**4**	**4**	**4**	**4**	**16**	**2**
5. Comunicación de Propuesta	**1**	**1**	**1**	**2**	**5**	**2**
6. Capacitación personal						**4**
	16	**12**	**12**	**14**	**54**	**148**
				Total Horas		**202**

Fuente: Elaboración propia

4.3.3.2 Costos monetarios. Se establece un estimado de cuánto sería el costo de realizar esta propuesta por cuatro profesionales en contaduría pública, siendo estos terceros independientes del CODEA. Para ello se toma en cuenta el costo en tiempo detallado anteriormente y las tarifas de honorarios profesionales mínimos de los Contadores Públicos Autorizados (CPA) vigentes y establecidas por el Colegio de Contadores Públicos de Costa Rica (CCPA)[9].

Según el apartado II del Artículo 5 del documento Tarifas de Honorarios Profesionales Mínimos de los Contadores Públicos Autorizados del CCPA "*Se aplicará una tarifa mínima de ¢22.695,71 (veintidós mil seiscientos noventa y cinco colones con setenta y un céntimos) por hora profesional*".

Tabla 30: *Cálculo de costo monetario de la propuesta*

Total Horas		202
Valor hora profesional	₡	22.695,71
Total Costo monetario	**₡**	**4.584.533,42**

Nota: El cálculo consiste en la multiplicación del total de horas utilizadas en realizar la propuesta para el CODEA, por el valor de la hora profesional establecida por el CCPA. Fuente: Elaboración propia.

[9] Documento emitido por el Colegio de Contadores Públicos de Costa Rica (CCPA), por medio del cual se detallan las Tarifas de Honorarios Profesionales para los Contadores Públicos Autorizados establecidas por el Poder Ejecutivo mediante el artículo 10 de la Ley No 1038. Dicha información se mantiene actualizada en la Página Oficial del CCPA https://www.ccpa.or.cr/tarifas-de-honorarios-profesionales-minimos-de-los-cpa/

4.3.4 Beneficios de la aplicación de la propuesta en CODEA

Parte de los beneficios que la aplicación de esta Propuesta generaría en el CODEA, es que se lograría establecer una metodología en el CODEA para la gestión de riesgos tomando en cuenta que en los últimos años en dicha entidad este proceso no se ha realizado. Es importante mencionar que al aplicarse esta metodología se identificarían riesgos que podrían afectar la consecución de los objetivos institucionales, por lo que a su vez se establecerían acciones de mitigación, prevención, detección u otras que permitan su adecuado tratamiento.

Al tomar como base tanto COSO 2013 como COBIT 5 se establece una gestión de riesgos que pretende cubrir de extremo a extremo la entidad. Además, cabe rescatar que, mediante el Inventario de Riesgos el CODEA contemplaría una gran gama de riesgos posibles que se encuentran debidamente clasificados y que a su vez facilitará su análisis.

Por medio de la propuesta se logrará generar conciencia de la importancia de la gestión de los riesgos, además de ser de apoyo a la Dirección y Gobierno del CODEA para agilizar y fortalecer la toma de decisiones.

Aunado a ello al contemplar a todos los niveles y áreas, genera responsabilidades de comunicación, resolución de inconvenientes y conocimiento de contratiempos, por ende, se da también involucramiento por parte de todo el personal requerido en la gestión de los riesgos.

Capítulo 5

Conclusiones y recomendaciones

5.1 Conclusiones

Este proyecto surge ante la necesidad del CODEA de fortalecer su control interno, esto debido a que el buen funcionamiento del control interno se considera un factor clave para la consecución de los objetivos institucionales, específicamente en lo que refiere a eficiencia y eficacia de sus procesos, la confiabilidad de la información y al cumplimiento regulatorio.

Así mismo, tomando en cuenta la creciente transformación digital del modus operandi institucional que el país ha venido enfrentando, obliga a que las instituciones incluyan dentro de su control interno, actividades relacionadas al buen manejo de las tecnologías y seguridad de la información. Por lo cual, el uso de estos dos marcos internacionales de buenas prácticas (COSO 2013 y COBIT 5) en el CODEA, constituye una estrategia que tiene como objetivo fortalecer a la entidad de extremo a extremo mediante la aplicación del “Sistema de Gestión de Valoración de Riesgos Transitorio”.

Sin embargo, mediante el análisis realizado al CODEA, se determinó que existen algunas otras condiciones específicas que requieren mejorarse según la teoría COSO 2013 y COBIT 5, estas se describen a continuación:

1. Para el componente de entorno de control, se identifica que la entidad no cuenta con un código de ética definido, no posee un plan de capacitación con el cual se fortalezca el intercambio de conocimientos, el trabajo en equipo y se promueva una cultura de cumplimiento y mejora continua de los procesos que contribuya al cumplimiento de los objetivos. Por otro lado, existe un manual de puestos sin embargo no se encuentra debidamente actualizado lo cual limita a la institución en la designación de responsabilidades y la posterior evaluación del rendimiento de sus funcionarios. Y finalmente, no existe una línea de comunicación directa y anónima que permita denunciar acciones inapropiadas.

2. El componente de evaluación de riesgos fue determinado mediante los análisis realizados como el más afectado por la no inexistencia de acciones de valoración de riesgos institucional, específicamente en lo que refiere al establecimiento de un Sistema Específico de Valoración de Riesgo Institucional (SEVRI), de acuerdo con la Ley General de Control Interno N.°8292 que permita identificar, analizar, responder y monitorear los diversos riesgos a los que está expuesto el CODEA y de esta forma ubicarse al menos en un nivel de riesgo institucional aceptable.

3. Se determinó la existencia de debilidades ligadas a los principios COBIT 5 como lo son la no realización de análisis del entorno externo, no se identifican procesos o actividades relacionadas al impacto del negocio lo cual requiere de evaluaciones que actualmente no son ejecutadas.

4. No se realizan evaluaciones de la capacidad de recursos y rendimientos, además se determinaron fallas en el principio de expresar el riesgo ya que al no existir los debidos análisis, no hay información de ellos por comunicar, finalmente no existe un plan de continuidad del negocio en el CODEA.

5. En cuanto al componente de actividades de control, no existe un Plan de Continuidad de Negocios, hay deficiencias en políticas y prácticas de seguridad de la información. En cuanto a la documentación de los procesos, está no identifica controles y riesgos como se pudo observar en los flujogramas suministrados. Y el registro de la información en el sistema SAP es insuficiente debido a que aún está pendiente incluir otra información en el mismo.

6. En relación con el componente de información y comunicación, la Junta Directiva no recibe información, acerca de los riesgos a los que está expuesto el CODEA, que permita una adecuada toma de decisiones, esto ante la ausencia de un proceso de valoración de riesgos.

   Asimismo, con respecto a las debilidades halladas asociadas a los principios de COBIT 5, se resalta la falta de procesos que permitan la comunicación de problemas y desviaciones, interrupciones en el procesamiento de la información que han limitado que la información sea completa, precisa, oportuna y segura.

7. Finalmente, en cuanto a las actividades de seguimiento, no se realizan actividades de seguimiento y autoevaluación de control interno.

5.2 Recomendaciones

Siguiendo como base las conclusiones descritas en el apartado anterior, se recomienda al CODEA establecer mecanismos que permitan mejorar su control interno. A continuación se detallan las recomendaciones:

1. Se recomienda en primera instancia fortalecer el componente de entorno de control, ya que de él se desprenden las políticas y procedimientos, las conductas de los colaboradores para el cumplimiento de los objetivos además los niveles de supervisión, por todas estas razones se deben establecer canales anónimos de comunicación, fomentar la filosofía de la entidad, desarrollar un código de ética y un manual de puestos los cuales deben mantenerse debidamente actualizados.

2 Se recomienda al CODEA aplicar la herramienta transitoria desarrollada en este proyecto con una periodicidad mínima de un año, esto con el fin de reducir los efectos de la ausencia de un SEVRI ya que la herramienta representa una base para el reconocimiento de riesgos y su administración, así como el establecimiento de controles. Es importante señalar que, mediante este proceso, la entidad documente y mantenga una revisión constante de los riesgos identificados y de la ejecución de los controles definidos.

2. Con base en COBIT 5, se recomienda utilizar herramientas como FODA u otras, que permitan evaluar tanto el entorno interno como externo, de esta manera, la entidad podrá realizar análisis que generen resultados de los efectos e impactos en sus procesos y negocios. Con base en estos resultados la entidad podrá realizar evaluaciones y comunicarlas a las partes interesadas de manera oportuna.

3. Para el componente de actividades de control, se considera relevante el instituir prácticas y políticas de control claramente identificadas y comunicadas a los colaboradores, así como la determinación de responsables. Esto le permitirá al CODEA la identificación de riesgos y el fomento de la responsabilidad del personal en su compromiso con el Control Interno. Se recomienda además, la documentación adecuada de los procesos de la institución, con el fin de tener claro donde se encuentran los controles de cada uno de esos procesos y a cuáles riesgos se enfrentan para de esta manera contar con planes de acción.

4. El componente de información y comunicación es primordial para el funcionamiento adecuado del control interno, ya que por medio de éste interactúan los demás componentes. Es por esta razón y de acuerdo a COBIT 5, que se le recomienda al CODEA establecer canales de divulgación ágiles y directos hacia los diferentes grupos de interés tanto internos como externos, así como informar a la Junta Directiva de los resultados que se generen de la aplicación de la herramienta transitoria de valoración de riesgos ya que servirá de base para la toma de decisiones y consecución de objetivos.

5. Por último para el componente de seguimiento de controles se recomienda al CODEA, establecer un adecuado sistema de evaluación, monitoreo y seguimiento de su control interno, si bien se realizan distintas de auditorías externas a la entidad que fomentan una cultura de autoevaluación y seguimiento, estas no resultan suficientes para dar un seguimiento y una autoevaluación continua a su gestión, puesto que no se realizan con una periodicidad definida, por lo que se recomienda establecer prácticas internas continuas y concretas para valorar la calidad y el funcionamiento del Control Interno, como lo son diagnósticos, atención de

resultados de riesgos identificados, capacitaciones continuas, revisión y actualización de las políticas y prácticas, todo esto con el fin de asegurar que los hallazgos y los resultados de otras revisiones se atiendan con prontitud.

Referencias

Abella, R. (2006). Coso II y la gestión integral de riesgos del negocio. Recuperado de: http://pdfs.wke.es/6/6/7/3/pd0000016673.pdf

Auditoría Superior de la Federación (ASF). (2014). Guía de Autoevaluación de Riesgos en el Sector Público. Recuperado de: http://www.oas.org/juridico/pdfs/mesicic5_mex_ane_64.pdf

Bayas, M. (2014). Desarrollo de un modelo de madurez tecnológico para categorizar a las instituciones financieras de los segmentos 3 y 4 de la superintendencia de economía popular y solidaria. *Universidad de Las Fuerzas Armadas*. Recuperado de: https://repositorio.espe.edu.ec/bitstream/21000/9007/1/AC-MEAST-%20ESPE-048258.pdf

Castañeda, J. (2018). *Gestión, administración de riesgos y modelos de control interno*. Bogotá: Fundación Universitaria del Área Andina. Recuperado de: https://digitk.areandina.edu.co/flip/index.jsp?pdf=/bitstream/handle/areandina/3542/78%20GESTI%c3%93N%2c%20ADMINISTRACI%c3%93N%20DE%20RIESGOS%20Y%20MODELOS%20DE%20CONTROL%20INTERNO.pdf?sequence=1&isAllowed=y

Código Municipal. Ley 7794 de 1998. 18 de mayo de 1998. (Costa Rica). Recuperado de: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_norma.aspx?param1=NRM&nValor1=1&nValor2=40197&nValor3=0&strTipM=FN

Colegio de Contadores Públicos de Costa Rica. (2021). *Tarifas De Honorarios Profesionales Mínimos De Los Contadores Públicos Autorizados.* Recuperado de:

https://docs.google.com/viewerng/viewer?url=http://ccpa.or.cr/wp-content/themes/maximus/pdf/fiscalia/Tarifas+de+Honorarios+Profesionales+M%C3%ADnimos+de+los+CPA.pdf

Comité Cantonal de Deportes y Recreación de Alajuela. (2019). Horizonte estratégico del Comité Cantonal de Deportes y Recreación. Documento no publicado.

Committee of Sponsoring Organization of the Treadway Commission (COSO) (2013). Control Interno - Marco Integrado. Resumen ejecutivo. (Instituto de Auditores Internos de España y PwC España, Trad.). (Trabajo original publicado en 2012). Recuperado de :https://auditoresinternos.es/uploads/media_items/coso-resumen-ejecutivo.original.pdf

Committee of Sponsoring Organization of the Treadway Commission (COSO).(2017). Gestión del Riesgo Empresarial Integrando Estrategia y Desempeño. Resumen ejecutivo. (Instituto de Auditores Internos de España y PwC, Trad.). (Trabajo original publicado en 2018). Recuperado de :https://auditoresinternos.es/uploads/media_items/coso-2018-esp.original.pdf

Contraloría General de la República. (2017). Informe de auditoría de carácter especial acerca de la actividad del Comité Cantonal de Deportes y Recreación de Paraíso (INFORME N. DFOE-DL-IF-00010-2017). Recuperado de: https://cgrfiles.cgr.go.cr/publico/docs_cgr/2017/SIGYD_D_2017018988.pdf

Contraloría General de la República. (2020). Sistema de Información sobre Planes y Presupuestos (SIPP). Recuperado de: https://cgrweb.cgr.go.cr/apex/f?p=150220:2:::NO:::

Contraloría General de la República. (s.f.). *Modelo de madurez del sistema de control interno.* Recuperado de: https://www.cgr.go.cr/03-documentos/normativa/control-interno.html

Contraloría General de la República. (2011). *Curso Virtual "Control Interno" – Componente 2: Valoración del Riesgo*. Recuperado de: https://www.pgr.go.cr/wp-content/uploads/2017/04/Valoracion_del_Riesgo_teoria.pdf

Dictamen C-062 de 2018. [Procuraduría General de la República]. Criterio en torno a las atribuciones que le otorga el artículo 164 del Código Municipal al Comité Cantonal de Deportes y Recreación. 04 de abril de 2018. Recuperado de http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Pronunciamiento/pro_ficha.aspx?param1=PRD&param6=1&nDictamen=20459&strTipM=T

Directrices Generales para el Establecimiento y Funcionamiento del Sistema Específico de Valoración del Riesgo Institucional (SEVRI) (D-3-2005-CO-DFOE). Recuperado de: https://www.cgr.go.cr/03-documentos/normativa/control-interno.html

González, L. (2005). Control interno y cuadro de mando integral una poderosa combinación intangible. *Cuba Siglo XXI*. Recuperado de https://www.nodo50.org/cubasigloXXI/economia/gmendez_310705.pdf

Hernández, J. (2018). COBIT, una metodología que genera valor en las empresas. *Universidad Piloto de Colombia*. Recuperado desde: http://repository.unipiloto.edu.co/handle/20.500.12277/4677

IT Governance Institute. (2007). *Cobit 4.1*. Recuperado de: https://biblioteca.info.unlp.edu.ar/uploads/docs/cobit.pdf

INTOSAI. (2004). Guía para las normas de control interno del sector público (INTOSAI GOV 9100). INTOSAI Professional Standards Committee. Recuperado de: https://controlinterno.poder-judicial.go.cr/index.php/leyes-y-normativa-relacionada-informacion?download=52:guia-para-las-normas-de-control-interno-del-sector-publico-intosai-gov-9100

ISACA. (2012a). COBIT 5. *Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa*.

ISACA. (2012b). COBIT 5. *Implementación.*

ISACA. (2012c). COBIT 5. *Procesos Catalizadores.*

Ley 6890 de 1983. Reformas al Código Municipal y otras Leyes. 23 de setiembre de 1983. D.O. No. 180. Recuperado de: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=8963&nValor3=9614&strTipM=TC

Ley Orgánica de la Contraloría General de la República. (Versión de la norma diciembre de 2018). 04 de noviembre de 1994. D.O. No. 210. Recuperado de: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_norma.aspx?param1=NRM&nValor1=1&nValor2=21629&nValor3=0&strTipM=FN

Normas de control interno para el Sector Público (N-2-2009-CO-DFOE), La Gaceta nº 26 (Contraloría General de la República). Recuperado de: https://www.cuc.ac.cr/app/cms/www/files/NCI.pdf

Oficio DFOE-DL-0162 de 2021. [Contraloría General de la República]. Emisión de criterio relacionado con la aprobación de los reglamentos internos para un Comité Cantonal de

Deportes y Recreación. 12 de febrero de 2021.Recuperado de: https://cgrfiles.cgr.go.cr/publico/docs_cgr/2021/SIGYD_D/SIGYD_D_2021002312.pdf

Reglamento No.34 de 2011 [Municipalidad de Alajuela]. Reglamento para la Organización y Funcionamiento del Comité Cantonal de Deportes y Recreación de Alajuela. 22 de diciembre de 2011. D.O 246. Recuperado de: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=71689&nValor3=88985&strTipM=TC

Rivas, G. (2011). Modelos contemporáneos de control interno. *Fundamentos teóricos Observatorio Laboral Revista Venezolana*, 4 (8), julio-diciembre, pp. 115-136. Recuperado de: https://www.redalyc.org/pdf/2190/219022148007.pdf

Sampieri, R., Fernandez C., Baptista, M. (2014). *Metodología de la investigación* (Sexta edición). México D.F.: McGraw-Hill/Interamericana. Recuperado de: https://www.uca.ac.cr/wp-content/uploads/2017/10/Investigacion.pdf

Sánchez, M. (2014). Auditoría Informatica COBIT 5 Vs. COBIT 4.1. *Manizales*. Recuperado de: https://chaui201411700921759.wordpress.com/2014/06/19/cobit-5-comparativo-con-cobit-4-1/

Sistema costarricense de información jurídica. Reformas al Código Municipal y Otras Leyes. 14 de setiembre de 1983. D.O. No. 180. Recuperado de: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=8963&nValor3=9614&strTipM=TC

Tamayo & Tamayo. (2003). *El proceso de la investigación científica*. México D.F. :LIMUSA.http://www.enfermeriaaps.com/portal/?wpfb_dl=4387

Unión Nacional de Gobiernos Locales. (2013). Código Municipal Comentado. Ley No. 7794. Recuperado de: https://www.muni-carta.go.cr/wp-content/uploads/2018/04/CodigoMunicipalcomentado.pdf

Anexos

CAPÍTULO II

Anexo A.

Montos presupuestados y ejecutados por el CODEA, periodo 2020

Institución	Suma Presupuestado	Suma Ejecutado
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE ABANGARES	160.510.100,13	88.906.295,58
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE ACOSTA	159.537.614,64	64.257.501,45
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE AGUIRRE	668.963.367,48	166.105.011,95
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE ALAJUELA	4.423.420.155	0
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE ALAJUELITA	393.994.278,05	0
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE ALFARO RUIZ	120.821.530,74	0
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE ALVARADO	76.267.538,19	0
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE ASERRI	217.694.200	125.816.265
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE ATENAS	204.557.260	32.827.436,76
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE BAGACES	323.039.526,33	102.627.136,62
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE BARVA	888.451.260,03	184.781.697,47
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE BELÉN	2.450.834.643,86	2.140.876.712,92
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE BUENOS AIRES	257.173.591,33	114.059.169,92
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE CARRILLO GUANACASTE	719.673.312	332.179.259,91
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE CARTAGO	3.531.493.750	1.722.290.687,84
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE CORREDORES	346.219.540,45	77.731.585,18
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE COTO BRUS	190.011.255,21	91.882.037,27
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE CURRIDABAT	1.436.423.524,01	0
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE DESAMPARADOS	1.776.693.408,91	1.005.986.756,49
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE DOTA	54.723.666,21	0
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE EL GUARCO	233.951.604	148.434.341,49
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE ESCAZU	6.116.278.333	3.361.519.505,95
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE ESPARZA	1.702.024.233,08	1.430.793.789,89
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE FLORES	241.316.620,21	0

COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE GARABITO	618.064.372,47	361.084.044,67
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE GOICOECHEA	1.917.212.236,92	1.267.857.404,50
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE GOLFITO	246.998.542,24	0
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE GRECIA	938.084.584,80	735.020.503
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE GUÁCIMO	221.892.617,82	(
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE GUATUSO	62.079.475,47	16.429.243,41
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE HEREDIA	2.071.031.503,34	1.607.693.472,97
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE HOJANCHA	113.518.124,90	86.543.131,46
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE JIMÉNEZ	126.035.735,13	76.727.827,88
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE LA CRUZ GUANACASTE	292.732.000	73.535.911,74
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE LA UNIÓN	1.110.302.051,60	739.392.080,61
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE LEON CORTES	67.581.661,63	9.060.822,36
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE LIBERIA	1.862.698.515,36	748.239.480,79
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE LIMÓN	875.495.976	0
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE LOS CHILES	89.137.508,70	0
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE MATINA	249.178.616,99	150.215.108,03
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE MONTES DE OCA	1.073.572.545,13	764.932.049,88
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE MONTES DE ORO	229.115.753,36	86.844.117,93
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE MORA	400.216.257,45	259.592.492,50
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE MORAVIA	4.188.876.413,27	141.786.822,49
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE NANDAYURE	157.893.021,90	0
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE NARANJO	263.140.882,91	0
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE NICOYA	398.232.650	212.576.035,11
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE OREAMUNO	250.605.193,86	198.556.125,81
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE OROTINA	241.111.199,37	0
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE OSA	292.668.664,74	255.463.565,55
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE PALMARES	329.659.735,32	180.321.694,24
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE PARAÍSO	788.510.008,65	734.903.558,61
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE PARRITA	174.734.136,55	131.415.979,27
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE PÉREZ ZELEDÓN	660.026.060,70	277.061.036,95
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE POÁS	203.193.227,26	130.680.126,69
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE POCOCÍ	1.053.535.749,96	234.093.833,80
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE PUNTARENAS	913.282.632,84	0

COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE PURISCAL	246.395.699,83	0
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE SAN CARLOS	1.549.885.601,92	1.096.021.650,70
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE SAN ISIDRO DE HEREDIA	325.728.876,40	91.720.611,27
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE SAN JOSÉ	13.983.581.547,62	9.817.534.804,47
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE SAN MATEO	58.397.157	0
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE SAN RAFAEL DE HEREDIA	444.575.996,37	297.688.294,80
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE SAN RAMÓN	866.575.293,13	397.317.236,81
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE SANTA ANA	1.678.756.833	677.039.665
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE SANTA BÁRBARA HEREDIA	540.909.047,92	350.169.972,34
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE SANTA CRUZ	1.209.730.640,09	0
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE SARAPIQUI	453.955.391,31	250.062.913,01
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE SARCHI	253.493.786,67	165.934.287,92
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE SIQUIRRES	299.425.019,42	0
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE TALAMANCA	148.849.111,44	36.734.141,76
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE TARRAZU	131.553.561,07	123.475.208,89
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE TIBÁS	1.361.662.847,94	371.705.613,81
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE TILARAN	166.720.464	106.069.596
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE TURRIALBA	573.410.286,06	477.648.518,99
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE TURRUBARES	15.000.000	0
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE UPALA	219.618.190,49	98.452.464,20
COMITÉ CANTONAL DE DEPORTE Y RECREACIÓN DE VASQUEZ DE CORONADO	358.522.911,37	0
COMITÉ CANTONAL DE DEPORTES Y RECREACIÓN DEL CANTON DE CAÑAS	316.841.592,28	216.461.073,80
Suma total	**74.378.081.824,83**	**35.245.137.715,71**

Anexo B.

Montos presupuestados por estrato, en millones de colones, periodo 2020

Número de Estrato	Límites	Cantidad de CCDR	* Monto Total Presupuestado por Estrato
1	0- 1.000	60	₡19.880
2	1.001-2.000	12	₡17.732
3	2.001-3.000	2	₡4.522
4	3.001-4.000	1	₡3.531
5	4.001-5.000	2	₡8.612
6	5.001-6.000	0	₡0
7	6.001-7.000	1	₡6.116
8	7.001-8.000	0	₡0
9	8.001-9.000	0	₡0
10	9.001-10.000	0	₡0
11	10.001-11.000	0	₡0
12	11.001-12.000	0	₡0
13	12.001-13.000	0	₡0
14	13.001-14.000	1	₡13.984
Totales:		**79**	**₡74.378**

Nota. En millones de colones

Anexo C.

Ingresos del CODEA, periodo 2021

Cuenta	Descripción	Inicial	Extraordinario	Total	%
1.0.0.0.00.00.0.0.000	**INGRESOS CORRIENTES**	**88.609.415**	**195.513.065**	**284.122.480**	**19,84%**
1.3.0.0.00.00.0.0.000	**INGRESOS NO TRIBUTARIOS**	**88.609.415**	**0**	**88.609.415**	**31,19%**
1.3.1.0.00.00.0.0.000	VENTA DE BIENES Y SERVICIOS	80.260.615	0	80.260.615	90,58%
1.3.1.2.00.00.0.0.000	VENTA DE SERVICIOS	80.260.615	0	80.260.615	
1.3.1.2.09.00.0.0.000	OTROS SERVICIOS	80.260.615	0	80.260.615	
1.3.1.2.09.09.0.0.000	Venta de otros servicios	80.260.615	0	80.260.615	
1.3.2.0.00.00.0.0.000	INGRESOS DE LA PROPIEDAD	2.087.200	0	2.087.200	2,36%
1.3.2.3.00.00.0.0.000	RENTA DE ACTIVOS FINANCIEROS	2.087.200	0	2.087.200	
1.3.2.3.01.00.0.0.000	INTERESES SOBRE TÍTULOS VALORES	2.087.200	0	2.087.200	
1.3.2.3.01.06.0.0.000	Intereses sobre títulos valores de Instituciones Públicas Financieras	521.800	0	521.800	
1.3.2.3.01.07.0.0.000	Intereses sobre títulos valores del Sector Privado	1.565.400	0	1.565.400	
1.3.9.0.00.00.0.0.000	OTROS INGRESOS NO TRIBUTARIOS	6.261.600	0	6.261.600	7,07%
1.3.9.9.00.00.0.0.000	Ingresos varios no especificados	6.261.600	0	6.261.600	
1.4.0.0.00.00.0.0.000	**TRANSFERENCIAS CORRIENTES**	**0**	**195.513.065**	**195.513.065**	**220,65%**
1.4.1.0.00.00.0.0.000	TRANSFERENCIAS CORRIENTES DEL SECTOR PUBLICO	0	195.513.065	195.513.065	100,00%
1.4.1.4.00.00.0.0.000	Transferencias corrientes de Gobiernos Locales	0	195.513.065	195.513.065	
2.0.0.0.00.00.0.0.000	**INGRESOS DE CAPITAL**	**798.300.000**	**0**	**798.300.000**	**55,73%**
2.4.0.0.00.00.0.0.000	**TRANSFERENCIAS DE CAPITAL**	**798.300.000**	**0**	**798.300.000**	**100,00%**
2.4.1.0.00.00.0.0.000	TRANSFERENCIAS DE CAPITAL DEL SECTOR PUBLICO	798.300.000	0	798.300.000	
2.4.1.4.00.00.0.0.000	Transferencias de capital de Gobiernos Locales	798.300.000	0	798.300.000	
3.0.0.0.00.00.0.0.000	**FINANCIAMIENTO**	**350.000.000**	**0**	**350.000.000**	**24,43%**
3.1.0.0.00.00.0.0.000	**FINANCIAMIENTO INTERNO**	**350.000.000**	**0**	**350.000.000**	**100,00%**
3.1.1.0.00.00.0.0.000	PRÉSTAMOS DIRECTOS	350.000.000	0	350.000.000	
3.1.1.6.00.00.0.0.000	Préstamos directos de Instituciones Públicas Financieras	350.000.000	0	350.000.000	
Total presupuestado		**1.236.909.415**	**195.513.065**	**1.432.422.480**	

Anexo D.

Egresos del CODEA, periodo 2021

Cuenta	Descripción	Inicial	Extraordinario	Total	%
0.00.00	**REMUNERACIONES**	**466.347.044,00**	**0,00**	**466.347.044,00**	**30,79%**
0.01.00	**REMUNERACIONES BÁSICAS**	**214.431.560,00**	**0,00**	**214.431.560,00**	**45,98%**
2000.01.01	Sueldos para cargos fijos	209.281.560,00	0,00	209.281.560,00	
2000.01.05	Suplencias	5.150.000,00	650.000,00	5.800.000,00	
0.02.00	**REMUNERACIONES EVENTUALES**	**15.979.560,00**	**0,00**	**15.979.560,00**	**3,43%**
2000.02.01	Tiempo extraordinario	12.079.560,00	0,00	12.079.560,00	
2000.02.03	Disponibilidad laboral	3.900.000,00	0,00	3.900.000,00	
0.03.00	**INCENTIVOS SALARIALES**	**136.505.900,00**	**0,00**	**136.505.900,00**	**29,27%**
2000.03.01	Retribución por años servidos	62.160.500,00	0,00	62.160.500,00	
2000.03.02	Restricción al ejercicio liberal de la profesión	19.570.000,00	0,00	19.570.000,00	
2000.03.03	Decimotercer mes	24.926.000,00	0,00	24.926.000,00	
2000.03.04	Salario escolar	23.669.400,00	0,00	23.669.400,00	
0.03.99	Otros incentivos salariales	6.180.000,00	0,00	6.180.000,00	
0.04.00	**CONTRIBUCIONES PATRONALES AL DESARROLLO Y LA SEGURIDAD SOCIAL**	**56.154.469,84**	**0,00**	**56.154.469,84**	**12,04%**
2000.04.01	Contribución Patronal al Seguro de Salud de la Caja Costarricense del Seguro Social	37.344.963,74	47.945.000,00	85.289.963,74	
2000.04.04	Contribución Patronal al Fondo de Desarrollo Social y Asignaciones Familiares	17.099.551,00	0,00	17.099.551,00	
2000.04.05	Contribución Patronal al Banco Popular y de Desarrollo Comunal	1.709.955,10	0,00	1.709.955,10	
0.05.00	**CONTRIBUCIONES PATRONALES A FONDOS DE PENSIONES**	**43.275.554,16**	**0,00**	**43.275.554,16**	**9,28%**

	Y OTROS FONDOS DE CAPITALIZACIÓN				
2000.05.01	Contribución Patronal al Seguro de Pensiones de la Caja Costarricense de Seguro Social	16.825.958,18	0,00	16.825.958,18	
2000.05.02	Aporte Patronal al Régimen Obligatorio de Pensiones Complementarias	5.129.865,30	0,00	5.129.865,30	
2000.05.03	Aporte Patronal al Fondo de Capitalización Laboral	10.259.730,60	0,00	10.259.730,60	
2000.05.05	Contribución Patronal a fondos administrados por entes privados	11.060.000,08	0,00	11.060.000,08	
1.00.00	**SERVICIOS**	**417.962.504,40**	**52.945.000,00**	**470.907.504,40**	**31,09%**
01.01.00	**ALQUILERES**	**6.000.000,00**	**0,00**	**6.000.000,00**	**1,27%**
01.01.01	Alquiler de edificios, locales y terrenos	4.000.000,00	0,00	4.000.000,00	
01.01.02	Alquiler de maquinaria, equipo y mobiliario	2.000.000,00	0,00	2.000.000,00	
01.02.00	**SERVICIOS BÁSICOS**	**50.300.000,00**	**0,00**	**50.300.000,00**	**10,68%**
01.02.01	Servicio de agua y alcantarillado	2.000.000,00	0,00	2.000.000,00	
01.02.02	Servicio de energía eléctrica	44.075.000,00	0,00	44.075.000,00	
01.02.04	Servicio de telecomunicaciones	4.225.000,00	0,00	4.225.000,00	
01.03.00	**SERVICIOS COMERCIALES Y FINANCIEROS**	**3.905.000,00**	**0,00**	**3.905.000,00**	**0,83%**
01.03.02	Publicidad y propaganda	605.000,00	0,00	605.000,00	
01.03.03	Impresión, encuadernación y otros	1.800.000,00	0,00	1.800.000,00	
01.03.04	Transporte de bienes	500.000,00	0,00	500.000,00	
01.03.06	Comisiones y gastos por servicios financieros y comerciales	1.000.000,00	0,00	1.000.000,00	
01.04.00	**SERVICIOS DE GESTIÓN Y APOYO**	**202.600.000,00**	**47.945.000,00**	**250.545.000,00**	**53,20%**
01.04.01	Servicios médicos y de laboratorio //(2019)	3.100.000,00	0,00	3.100.000,00	

	Servicios en ciencias de la salud				
01.04.02	Servicios jurídicos	6.000.000,00	0,00	6.000.000,00	
01.04.04	Servicios en ciencias económicas y sociales	500.000,00	25.000.000,00	25.500.000,00	
01.04.99	Otros servicios de gestión y apoyo	193.000.000,00	22.945.000,00	215.945.000,00	
01.05.00	**GASTOS DE VIAJE Y DE TRANSPORTE**	**43.650.000,00**	**0,00**	**43.650.000,00**	**9,27%**
01.05.01	Transporte dentro del país	40.000.000,00	0,00	40.000.000,00	
01.05.02	Viáticos dentro del país	3.650.000,00	0,00	3.650.000,00	
01.06.00	**SEGUROS, REASEGUROS Y OTRAS OBLIGACIONES**	**10.600.000,00**	**0,00**	**10.600.000,00**	**2,25%**
01.06.01	Seguros	10.600.000,00	0,00	10.600.000,00	
01.07.00	**CAPACITACIÓN Y PROTOCOLO**	**32.122.500,00**	**0,00**	**32.122.500,00**	**6,82%**
01.07.01	Actividades de capacitación	3.122.500,00	0,00	3.122.500,00	
01.07.02	Actividades protocolarias y sociales	13.000.000,00	0,00	13.000.000,00	
01.07.03	Gastos de representación institucional	16.000.000,00	0,00	16.000.000,00	
01.08.00	**MANTENIMIENTO Y REPARACIÓN**	**33.785.004,40**	**5.000.000,00**	**38.785.004,40**	**8,24%**
01.08.01	Mantenimiento de edificios, locales y terrenos	15.000.000,00	5.000.000,00	20.000.000,00	
01.08.04	Mantenimiento y reparación de maquinaria y equipo de producción	3.500.000,00	0,00	3.500.000,00	
01.08.05	Mantenimiento y reparación de equipo de transporte	1.600.000,00	0,00	1.600.000,00	
01.08.07	Mantenimiento y reparación de equipo y mobiliario de oficina	500.000,00	0,00	500.000,00	
01.08.08	Mantenimiento y reparación de equipo de cómputo y sistemas de información	13.185.004,40	0,00	13.185.004,40	
1.99.00	**SERVICIOS DIVERSOS**	**35.000.000,00**	**0,00**	**35.000.000,00**	**7,43%**
1.99.99	Otros servicios no especificados	35.000.000,00	0,00	35.000.000,00	

2.00.00	**MATERIALES Y SUMINISTROS**	**137.025.000,08**	**2.000.000,00**	**139.025.000,08**	**9,18%**
02.01.00	**PRODUCTOS QUÍMICOS Y CONEXOS**	**23.275.000,08**	**0,00**	**23.275.000,08**	**16,74%**
02.01.01	Combustibles y lubricantes	3.225.000,00	0,00	3.225.000,00	
02.01.02	Productos farmacéuticos y medicinales	5.000.000,00	0,00	5.000.000,00	
02.01.99	Otros productos químicos y conexos	15.050.000,08	0,00	15.050.000,08	
02.03.00	**MATERIALES Y PRODUCTOS DE USO EN LA CONSTRUCCIÓN Y MANTENIMIENTO**	**3.600.000,00**	**0,00**	**3.600.000,00**	**2,59%**
02.03.01	Materiales y productos metálicos	1.000.000,00	0,00	1.000.000,00	
02.03.04	Materiales y productos eléctricos, telefónicos y de cómputo	1.600.000,00	0,00	1.600.000,00	
02.03.06	Materiales y productos de plástico	1.000.000,00	0,00	1.000.000,00	
02.04.00	**HERRAMIENTAS, REPUESTOS Y ACCESORIOS**	**500.000,00**	**0,00**	**500.000,00**	**0,36%**
02.04.01	Herramientas e instrumentos	500.000,00	0,00	500.000,00	
2.99.00	**ÚTILES, MATERIALES Y SUMINISTROS DIVERSOS**	**109.650.000,00**	**2.000.000,00**	**111.650.000,00**	**80,31%**
2.99.01	Útiles y materiales de oficina y cómputo	3.000.000,00	0,00	3.000.000,00	
2.99.04	Textiles y vestuario	63.300.000,00	0,00	63.300.000,00	
2.99.05	Útiles y materiales de limpieza	5.400.000,00	0,00	5.400.000,00	
2.99.99	Otros útiles, materiales y suministros diversos	37.950.000,00	2.000.000,00	39.950.000,00	
3.00.00	**INTERESES Y COMISIONES**	**20.000.000,00**	**0,00**	**20.000.000,00**	**1,32%**
03.02.00	**INTERESES SOBRE PRÉSTAMOS**	**20.000.000,00**	**0,00**	**20.000.000,00**	**100,00%**
03.02.06	Intereses sobre préstamos de Instituciones Públicas Financieras	20.000.000,00	0,00	20.000.000,00	

5.00.00	**BIENES DURADEROS**	**266.614.820,90**	**140.568.065,00**	**407.182.885,90**	**26,88%**
05.01.00	**MAQUINARIA, EQUIPO Y MOBILIARIO**	**30.750.001,67**	**650.000,00**	**31.400.001,67**	**7,71%**
05.01.01	Maquinaria y equipo para la producción	4.650.001,67	0,00	4.650.001,67	
05.01.02	Equipo de transporte	1.100.000,00	650.000,00	1.750.000,00	
05.01.05	Equipo y programas de cómputo //(2019) Equipo de cómputo	25.000.000,00	0,00	25.000.000,00	
05.02.00	**CONSTRUCCIONES, ADICIONES Y MEJORAS**	**235.864.819,23**	**139.918.065,00**	**375.782.884,23**	**92,29%**
05.02.07	Instalaciones	235.864.819,23	139.918.065,00	375.782.884,23	
6.00.00	**TRANSFERENCIAS CORRIENTES**	**3.075.000,00**	**0,00**	**3.075.000,00**	**0,20%**
06.03.00	**PRESTACIONES**	**3.075.000,00**	**0,00**	**3.075.000,00**	**100,00%**
06.03.01	Prestaciones legales	3.075.000,00	0,00	3.075.000,00	
8.00.00	**AMORTIZACION**	**8.000.000,00**	**0,00**	**8.000.000,00**	**0,53%**
08.02.00	**AMORTIZACIÓN DE PRÉSTAMOS**	**8.000.000,00**	**0,00**	**8.000.000,00**	**100,00%**
08.02.06	Amortización de préstamos de Instituciones Públicas Financieras	8.000.000,00	0,00	8.000.000,00	
Total presupuestado		**1.319.024.369**	**195.513.065**	**1.514.537.434**	**100,00%**

Anexo E.

Presupuesto del CODEA, periodo 2021

Programa	Presupuesto	Valor %
Operativo	606.532.879,81	49,04%
Deportivo	493.313.621,62	39,88%
Administrativo	121.582.913,39	9,83%
Comités comunales	15.480.000,00	1,25%
	1.236.909.414,82	**100,00%**

CAPÍTULO III

Anexo F.

Correo Masivo al personal del CODEA, Formularios de Google

Estimado (a) Nombre del funcionario

Se adjunta el siguiente enlace https://forms.gle/n3yT72o7QCEFCNxo7 que corresponde a un formulario que contiene una serie de preguntas, las cuales son aplicadas con el fin de complementar el proceso de Trabajo Final de Graduación (tesis) llevado a cabo para optar por el grado de Licenciatura en Contaduría Pública de la Universidad de Costa Rica. Así mismo, le indicamos que la aplicación de estos formularios ya fue avalada por el director del Comité, MBA. Jordan Vargas.

La idea es conocer a grandes rasgos algunas generalidades del CODEA en relación con los componentes de COSO 2013 y los conceptos expuestos por COBIT 5, para así poder generar un producto que sea de gran valor para el CODEA, de forma que se ajuste a sus necesidades actuales y futuras, y a su vez, que permita fortalecer el control interno de la entidad.

Se estima un tiempo de llenado de 6 minutos, le solicitamos amablemente que nos ayude a completarlo antes del lunes 15 de noviembre.

Cualquier consulta o duda que se presente, puede comunicarse con:

Daniela Arrieta al correo danarrietaa@gmail.com; Marilyn Castro, al correo marilyn.castroque96@gmail.com; Jesús Murillo al correo jemuva2014@gmail.com y/o Yerlin Navarro al correo yerlinnb19@gmail.com.

De antemano le agradecemos enormemente el tiempo dedicado.

Anexo G.

Matriz de principios de COBIT 5 base para la Homologación con COSO 2013.

Dominio de COBIT	Nombre Dominio	Sigla Objetivo	Objetivo de Gobierno o Gestión de TI	¿Métrica de proceso o de TI?	Métricas actividades aplicables a CODEA	Entradas	Salidas
EDM01	Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno	EDM 01.02	Orientar el sistema de gobierno.	Proceso	Comunicar principios del gobierno TI, establecer o delegar el establecimiento de las estructuras, procesos, asignar responsabilidades, autoridad y responsabilidad, garantizar mecanismos de notificación	N/A	Comunicaciones del gobierno de la empresa
EDM01	Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno	EDM 01.03	Supervisar el sistema de gobierno.	Proceso	Evaluar efectividad y rendimiento partes interesadas, proporcionar supervisión de la efectividad del cumplimiento con el sistema de control de la empresa. Supervisar los mecanismos rutinarios y regulares para garantizar que el uso de TI cumple con las obligaciones relevantes	Informes, resultados de estudios, monitorización, confirmaciones de cumplimiento, obligaciones, informes de auditoría	Retroalimentación sore rendimiento y efectividad del gobierno
EDM02	Asegurar la Entrega de Beneficios	EDM 02.01	Evaluar la Optimización de valor	Proceso/01	Comprender los requerimientos de las partes interesadas; temas estratégicos de TI, tales como la dependencia de las TI; y comprender la tecnología y sus capacidades considerando la importancia actual y potencial de TI para la estrategia de la empresa.	Hoja de ruta estratégica	Evaluación de alineación estratégica
EDM02	Asegurar la Entrega de Beneficios	EDM 02.01	Evaluar la Optimización de valor	Proceso/06	Comprender y considerar cómo de efectivos son los roles, responsabilidades, asignaciones y organismos de toma de decisiones actuales asegurando la creación de valor de las inversiones, servicios y activos de TI.	Hoja de ruta estratégica	Evaluación de alineación estratégica
EDM02	Asegurar la Entrega de Beneficios	EDM 02.01	Evaluar la Optimización de valor	Proceso/07	Considerar cómo de bien alineada está la gestión de las inversiones, servicios y activos de TI con la gestión de valor y las prácticas de gestión financiera.	Hoja de ruta estratégica	Evaluación de alineación estratégica
EDM02	Asegurar la Entrega de Beneficios	EDM 02.02	Orientar la Optimización de valor	Proceso/05	Definir y comunicar a nivel de empresa los objetivos de entrega de valor y las medidas de resultados para permitir un control eficaz.	No posee entradas	Requerimientos para las revisiones de cambio de fase (stage-gate)
EDM02	Asegurar la Entrega de Beneficios	EDM 02.03	Supervisar la Optimización de valor	Proceso/01	1. Definir un conjunto equilibrado de objetivos de desempeño, métricas, metas y puntos de referencia. Las métricas deberían cubrir la actividad y la medida de resultados, incluyendo los indicadores de retardo y de avance de los resultados, así como un equilibrio adecuado de las medidas financieras y no financieras. Revisarlos y acordarlos con las funciones de TI y de negocio, y otras partes interesadas relevantes.	Informes de rendimiento de la cartera de inversiones	Comentarios sobre el rendimiento de la cartera y del programa Acciones para mejorar la entrega de valor
EDM02	Asegurar la Entrega de Beneficios	EDM 02.03	Supervisar la Optimización de valor	Proceso	2. Recoger los datos pertinentes, oportunos, completos, fiables y precisos para informar sobre los avances en la entrega de valor respecto a los objetivos. Obtener una sucinta, de alto nivel, completa vista de la cartera, programa y desempeño TI (capacidades técnicas y operativas) que soporten la toma de decisiones y aseguren que los resultados esperados se están logrando.	Informes de rendimiento de la cartera de inversiones	Comentarios sobre el rendimiento de la cartera y del programa Acciones para mejorar la entrega de valor

EDM02	Asegurar la Entrega de Beneficios	Genérico	Alineamiento de TI y estrategia de negocio	TI/01	• Nivel de satisfacción de las partes interesadas con el alcance del portafolio de programas y servicios planeados	N/A	N/A
EDM02	Asegurar la Entrega de Beneficios	Genérico	Transparencia de los costes, beneficios y riesgos de las TI	TI/06	• Porcentaje de servicios TI con costes operativos y beneficios esperados claramente definidos y aprobados.	N/A	N/A
EDM03	Asegurar la Optimización del Riesgo	Genérico	N/A	TI/04	Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos	N/A	N/A
EDM03	Asegurar la Optimización del Riesgo	Genérico	N/A	TI/04	Frecuencia de actualización del perfil de riesgo	N/A	N/A
EDM03	Asegurar la Optimización del Riesgo	EDM 03.01	Evaluar la gestión de riesgos.	N/A	Determinar el nivel de riesgos relacionados con las TI que la empresa está dispuesta a asumir para cumplir con sus objetivos (apetito de riesgo).	APO12.01 Factores y problemas de riesgos emergentes Fuera del Ámbito de COBIT_ Principios de la gestión de riesgos de la empresa	Guías de apetito de riesgo APO12.03 Niveles de tolerancia de riesgo aprobados APO12.03 Evaluación de las actividades de gestión de riesgo APO12.01
EDM03	Asegurar la Optimización del Riesgo	EDM 03.01	Evaluar la gestión de riesgos.	N/A	2. 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.	APO12.01 Factores y problemas de riesgos emergentes Fuera del Ámbito de COBIT Principios de la gestión de riesgos de la empresa	Guías de apetito de riesgo APO12.03 Niveles de tolerancia de riesgo aprobados APO12.03 Evaluación de las actividades de gestión de riesgo APO12.01
EDM03	Asegurar la Optimización del Riesgo	EDM 03.02	Orientar la gestión de riesgos.	N/A	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.	APO12.03 Perfil de riesgo agregado incluyendo el estado de las acciones de gestión del riesgo Fuera del Ámbito de COBIT_ Perfiles y planes de mitigación de la Gestión del Riesgo de la Empresa (ERM)	Políticas de gestión de riesgos APO12.01 Objetivos claves a ser monitorizados por la gestión de riesgos APO12.01 Proceso aprobado para la medición de la gestión de riesgos APO12.01
EDM03	Asegurar la Optimización del Riesgo	EDM 03.02	Orientar la gestión de riesgos.	N/A	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.	APO12.03 Perfil de riesgo agregado incluyendo el estado de las acciones de gestión del riesgo Fuera del Ámbito de COBIT_ Perfiles y planes de mitigación de la Gestión del Riesgo de la Empresa (ERM)	Políticas de gestión de riesgos APO12.01 Objetivos claves a ser monitorizados por la gestión de riesgos APO12.01 Proceso aprobado para la medición de la gestión de riesgos APO12.01

EDM03	Asegurar la Optimización del Riesgo	EDM 03.03	Supervisar la gestión de riesgos.	N/A	Supervisar hasta qué punto se gestiona el perfil de riesgo dentro de los umbrales de apetito de riesgo.	APO12.02 Resultados del análisis de riesgos 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	Acciones correctivas para tratar las desviaciones en la gestión del riesgo_APO12.06 Problemas de la gestión de riesgos para la Dirección_EDM05.01
EDM03	Asegurar la Optimización del Riesgo	EDM 03.03	Supervisar la gestión de riesgos.	N/A	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.	APO12.02 Resultados del análisis de riesgos 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	Acciones correctivas para tratar las desviaciones en la gestión del riesgo_APO12.06 Problemas de la gestión de riesgos para la Dirección_EDM05.01
EDM03	Asegurar la Optimización del Riesgo	EDM 03.03	Supervisar la gestión de riesgos.	N/A	4. Informar cualquier problema de gestión de riesgos al Consejo o al Comité de Dirección.	APO12.02 Resultados del análisis de riesgos 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	Acciones correctivas para tratar las desviaciones en la gestión del riesgo_APO12.06 Problemas de la gestión de riesgos para la Dirección_EDM05.01
EDM04	Asegurar la optimización de los Recursos	EDM 04.01	Evaluar la gestión de recursos.	N/A	a. 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. b. Definir los principios para la gestión y el control de la arquitectura de la empresa.	a. Planes de desarrollo de competencias b. Decisiones sobre los resultados de evaluación de proveedores	a. Principios rectores de la arquitectura de la empresa b. Plan de recursos aprobado
EDM04	Asegurar la optimización de los Recursos	EDM 04.02	Orientar la gestión de recursos.	N/A	a. 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. b. Asignar responsabilidades para la ejecución de la gestión de recursos. c. Alinear la gestión de recursos con la planificación de RRHH y financiera de la empresa.	N/A	a. Comunicación de las estrategias de reasignación de recursos b. Responsabilidades asignadas para la gestión de los recursos c. Principios para la protección de recursos

EDM04	Asegurar la optimización de los Recursos	EDM 04.03	Supervisar la gestión de recursos.	N/A	a. 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.	N/A	a. Comentarios sobre la asignación y la eficacia de los recursos y capacidades b. Acciones correctivas para hacer frente a las desviaciones de gestión de recursos
EDM05	Asegurar la Transparencia de las partes interesadas	EDM 05.01	Evaluar los requisitos de elaboración de informes de las partes interesadas.	Proceso	Examinar y juzgar requisitos actuales y futuros de elaboración de informes respecto al uso de TI y para otros interesados dentro de la empresa. Mantener los principios de comunicación con interesados externos e internos	Mejorar entrega de valor, cuestiones de gestión del riesgo a tratar por el Consejo de Administración y retroalimentación sobre la asignación y eficacia de los recursos	Evaluar requisitos corporativos en la elaboración de informes Principios de elaboración de informes y de comunicación
EDM05	Asegurar la Transparencia de las partes interesadas	EDM 05.02	Orientar la comunicación con las partes interesadas y la elaboración de informes.	Proceso	Estrategia de comunicación para interesados internos y externos. Mecanismos para garantizar que la información cumple todos los criterios Mecanismos de validación y aprobación de la elaboración de informes	Informe de análisis de riesgos y perfil de riesgo de las partes interesadas	Reglas de validación y aprobaciones. Directrices de escalado
EDM05	Asegurar la Transparencia de las partes interesadas	EDM 05.03	Supervisar la comunicación con las partes interesadas.	Proceso	Evaluar periódicamente la eficacia de los mecanismos para asegurar precisión y fiabilidad. Así como las salidas de la comunicación con interesados externos e internos	Informe de la revisión de aseguramiento. Resultados de la revisión	Evaluación de la eficacia de la elaboración de informes
APO01	Gestionar el Marco de gestión de TI	APO0 1.03	Mantener los elementos catalizadores del sistema de gestión.	Proceso	a. 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. b. 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. c. 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. d. 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. e. Evaluar y actualizar las políticas, como mínimo una vez al año, para ajustarlas a los cambiantes entornos operativo o de negocio.	Principios rectores del gobierno corporativo Problemas y factores de riesgo emergentes Resultados del análisis de riesgos	Políticas relativas a TI

APO01	Gestionar el Marco de gestión de TI	APO01.04	Comunicar los objetivos y la dirección de gestión	Proceso	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. 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. Proporcionar recursos suficientes y cualificados para dar soporte al proceso comunicativo	Comunicación de gobierno corporativo Principios de protección de recursos Comunicación de impactos de riesgo Política y objetivos de continuidad empresarial Políticas de seguridad sobre terminales	Comunicación de objetivos de TI
APO01	Gestionar el Marco de Gestion de TI	APO01.06	Definir la propiedad de la información (datos) y del sistema.	Proceso	1. Proveer políticas y directrices para asegurar la adecuación y consistencia de la clasificación de la información (datos) en toda la empresa. 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. 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	N/A	Directrices para la clasificación de datos Directrices para el control y seguridad de datos Procedimientos de integridad de datos
APO01	Gestionar el Marco de Gestion de TI	APO01.07	Gestionar la mejora continua de los procesos	Proceso	3. Considerar las maneras de mejorar la eficiencia y eficacia (p. ej., mediante formación, documentación, estandarización y automatización de procesos). 4. Aplicar prácticas de gestión de calidad para la actualización de procesos. 5. Retirar procesos, componentes o catalizadores desactualizados.	Realimentación de la efectividad y funcionamiento del gobierno Actualización de políticas, principios, procedimientos y estándares	Evaluaciones de la capacidad de los procesos Oportunidades de mejoras de proceso Objetivos y métricas de rendimiento para el seguimiento de la mejora de procesos
APO01	Gestionar el Marco de Gestion de TI	APO01.08	Mantener el cumplimiento con las políticas y procedimientos.	Proceso	a. Hacer un seguimiento del cumplimiento con políticas y procedimientos. b. Analizar los incumplimientos y adoptar las acciones apropiadas (puede incluir el cambio de requerimientos). c. Integrar rendimiento y cumplimiento dentro de los objetivos individuales del personal.	Políticas del entorno Actualización de políticas, principios, procedimientos y estándares	Acciones de remediación por no cumplimiento
APO02	Gestionar la Estrategia	APO02.01	Comprender la dirección de la empresa.	N/A	1. Desarrollar y mantener un entendimiento de las estrategias y objetivos del negocio, así como del entorno y los retos operativos actuales.	APO04.02 Oportunidades de innovación vinculadas con los motivadores de la industria Estrategia y análisis de las fortalezas, debilidades, oportunidades, amenazas de la empresa (DAFO)	Fuentes y prioridades para cambios
APO02	Gestionar la Estrategia	APO02.01	Comprender la dirección de la empresa.	N/A	5. Determinar prioridades para el cambio estratégico.	APO04.02 Oportunidades de innovación vinculadas con los motivadores de la industria Estrategia y análisis de las fortalezas, debilidades, oportunidades, amenazas de la empresa (DAFO)	Fuentes y prioridades para cambios

APO02	Gestionar la Estrategia	APO02.02	Evaluar el entorno, capacidades y rendimiento actuales.	N/A	2. Identificar los actuales y potenciales riesgos y tecnologías en declive.		
APO02	Gestionar la Estrategia	APO02.02	Evaluar el entorno, capacidades y rendimiento actuales.	N/A	3. Identificar diferencias entre el negocio actual y las capacidades de TI, entre servicios y estándares y mejores prácticas de referencia, entre empresas competidoras y sus capacidades de TI y entre un análisis comparativo de las mejoras prácticas y la provisión de servicios emergentes de TI.		
APO02	Gestionar la Estrategia	APO02.02	Evaluar el entorno, capacidades y rendimiento actuales.	N/A	4. Identificar los problemas, fortalezas, oportunidades y amenazas en el entorno actual, las capacidades y servicios para entender el desempeño actual. Identificar las áreas a mejorar en términos de la contribución de TI a los objetivos del negocio.		
APO03	Gestionar la Arquitectura empresarial	APO03.01	Desarrollo de la visión de la arquitectura empresarial	N/A	a. Identificar a las partes interesadas clave de la empresa y sus objetivos/preocupaciones y definir los requisitos clave de la empresa a ser considerados. b. Crear la visión de la arquitectura atendiendo a las preocupaciones de las partes interesadas, en los requisitos de capacidad del negocio. c. Identificar los riesgos empresariales asociados con el cambio de la nueva visión de la arquitectura, evaluar el nivel de riesgo inicial (por ejemplo, crítico, marginal o despreciable) y desarrollar una estrategia de mitigación para cada riesgo importante.	a. Hoja de ruta estratégica	a. Principios de arquitectura b. Alcance de la arquitectura definido
APO03	Gestionar la Arquitectura empresarial	APO03.03	Seleccionar las oportunidades y las oportunidades	N/A	a. Confirmar el grado de preparación de la empresa y el riesgo asociado a la transformación empresarial b. Evaluar las necesidades, las carencias, las soluciones y los factores para identificar un conjunto mínimo de requisitos funcionales cuya integración en el plan de trabajo daría lugar a una implementación más eficiente y eficaz de la arquitectura objetivo.	N/A	a. Estrategia de implementación de alto nivel
APO03	Gestionar la Arquitectura empresarial	APO03.04	Definir la implementación de la arquitectura	N/A	a. Confirmar las fases y los progresos de la arquitectura de transición. b. Definir los requisitos de gobierno de implementación de la arquitectura.	N/A	a. Necesidades de recursos b. Fases de implementación
APO03	Gestionar la Arquitectura empresarial	APO03.05	Proveedor los servicios de arquitectura	N/A	a. Gestionar los requisitos de la arquitectura empresarial y dar soporte con los principios de dicha arquitectura, modelos y componentes básicos.	N/A	a. Orientación para el desarrollo de soluciones
APO08	Gestionar las relaciones	APO08.02	Identificar oportunidades, riesgos y limitaciones de TI para mejorar el negocio	Proceso	Tomar un papel proactivo en identificar y comunicar a las partes interesadas clave oportunidades, riesgo y limitaciones	Identificar lagunas en servicios de TI, planes de acciones de mejora, informes de rendimiento, causas raíz	Acuerdo en pasos y planes de acción

APO08	Gestionar las relaciones	APO08.04	Coordinar y comunicar	Proceso	Coordinar y comunicar cambios y actividades de transición, roles responsabilidades, tomar en consideración la reacción del negocio	Acuerdos nivel servicio, comunicación impacto riesgo, plan de uso operación, soporte, comunicación de los tiempos mantenimiento	Plan de comunicación, paquetes y respuestas de los clientes
APO10	Gestionar los Proveedores	APO10.01	Identificar y evaluar las relaciones y contratos con proveedores.	N/A	2. Establecer y mantener un criterio de evaluación de contratos y proveedores que permita una revisión general del rendimiento de los proveedores de manera consistente.	Fuera del Ámbito de COBIT Contratos con los proveedores	Relevancia del contratista y criterios de evaluación Interno Catálogo de proveedores BAI02.02 Revisiones potenciales de los contratos con los proveedores Interno
APO10	Gestionar los Proveedores	APO10.02	Seleccionar proveedores.	N/A	En el caso específico de la adquisición de software, incluir y hacer cumplir los derechos y obligaciones de todas las partes en los términos contractuales. Estos derechos y obligaciones pueden incluir la propiedad y el licenciamiento de la propiedad intelectual, el mantenimiento, las garantías, los procesos de arbitraje, las condiciones de actualización y la aptitud para el propósito definido, incluyendo seguridad, depósito de garantía y derechos de acceso.	BAI02.02 Plan de adquisiciones/ desarrollos de alto nivel	Solicitudes de Información (RFIs) y peticiones de propuestas (RFPs) a proveedores_ BAI02.01_ BAI02.02 Evaluaciones de RFIs y RFPs_BAI02.02 Resultados decididos tras las evaluaciones de proveedores_EDM04.01_BAI02.02
APO10	Gestionar los Proveedores	APO10.02	Seleccionar proveedores.	N/A	En el caso específico de la adquisición de desarrollos, incluir y hacer cumplir los derechos y obligaciones de todas las partes en lops términos contractuales. Estos derechos y obligaciones pueden incluir la propiedad y el licenciamiento de la propiedad intelectual; aptitud para el propósito definido, incluyendo metodologías, pruebas, procesos de gestión de la calidad, incluyendo los criterios de evaluación del rendimiento, formas de pago, garantías, los procesos de arbitraje, gestión de recursos humanos y cumplimiento con las políticas corporativas.	BAI02.02 Plan de adquisiciones/ desarrollos de alto nivel	Solicitudes de Información (RFIs) y peticiones de propuestas (RFPs) a proveedores_ BAI02.01_ BAI02.02 Evaluaciones de RFIs y RFPs_BAI02.02 Resultados decididos tras las evaluaciones de proveedores_EDM04.01_BAI02.02
APO10	Gestionar los Proveedores	APO10.03	Gestionar contratos y relaciones con proveedores.	N/A	Especificar un proceso de comunicación formal y de revisión, que incluyan las interacciones con el proveedor y la planificación.	BAI03.04 Planes de adquisiciones aprobados	Roles y responsabilidades de los proveedores Interno Procesos de revisión y comunicación Interno Resultados y sugerencias de mejora Interno

APO10	Gestionar los Proveedores	APO10.03	Gestionar contratos y relaciones con proveedores.	N/A	Acordar, gestionar, mantener y renovar los contratos con los proveedores. Asegurar que los contratos son conformes con las normas corporativas y con los requisitos legales y regulatorios.	BAI03.04 Planes de adquisiciones aprobados	Roles y responsabilidades de los proveedores Interno Procesos de revisión y comunicación Interno Resultados y sugerencias de mejora Interno
APO10	Gestionar los Proveedores	APO10.04.	Gestionar el riesgo en el suministro.	N/A	1. Identificar, supervisar y, cuando sea apropiado, gestionar los riesgos relacionados con la capacidad del proveedor de entregar el servicio de forma eficiente, eficaz, segura, fiable y continua.	APO12.04 • Resultados de la evaluación de riesgos de terceros. • Análisis de Riesgos e informes de perfil de riesgo para las partes interesadas.	Identificar el riesgo de entrega del proveedor APO12.01_ APO12.03_ BAI01.01 Identificar requisitos contractuales para minimizar riesgo Interno
APO10	Gestionar los Proveedores	APO10.04.	Gestionar el riesgo en el suministro.	N/A	A la hora de definir el contrato, para los riesgos potenciales, incluir una descripción clara de todos los requisitos de servicio, incluyendo depósitos de garantía, proveedores alternativos o acuerdos en suspenso para mitigar el riesgo de un posible fallo del proveedor; los aspectos de seguridad, la propiedad intelectual y los requisitos legales y regulatorios.	APO12.04 • Resultados de la evaluación de riesgos de terceros. • Análisis de Riesgos e informes de perfil de riesgo para las partes interesadas.	Identificar el riesgo de entrega del proveedor APO12.01_ APO12.03_ BAI01.01 Identificar requisitos contractuales para minimizar riesgo Interno
APO12	Gestionar el riesgo	APO12.01	Recopilar datos	Proceso	Registrar datos relevantes sobre el entorno de operación interno y externo de la empresa que pudieran jugar un papel significativo en la gestión. Registrar datos sobre eventos de riesgo que han causado o pueden causar impactos al beneficio/valor facilitado por TI, del riesgo de TI. Determinar las condiciones específicas que existían o faltaban cuando ocurrieron los eventos de riesgo	Evaluación de actividades de gestión de riesgos, procesos aprobados para medir la gestión, objetivos claves por la gestión riesgo, brechas y riesgos, evaluación riesgo	Datos en el entorno de operación, eventos de riesgo y en factores contribuyentes. Elementos factores riesgo emergentes
APO12	Gestionar el riesgo	APO12.02	Analizar el riesgo	Proceso	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.	Analisis de impacto negocio, evaluaciones de amenazas, avisos	Alcance de los esfuerzos de analisis de riesgos, escenarios de riesgos, resultados
APO12	Gestionar el riesgo	APO12.03	Mantener un perfil de riesgo	Proceso	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. Agregar escenarios de riesgo actuales, por categoría, línea de negocio y área funcional.	Niveles aprobados de tolerancia, guía apetito riesgo, riesgo entrega de proveedores identificados, amenazas potenciales	Escenarios de riesgo documentados, perfil de riesgo
APO12	Gestionar el riesgo	APO12.04	Expresar el riesgo	Proceso	Informar de los resultados del análisis de riesgos a todas las partes interesadas afectadas en términos y formatos útiles para soportar las decisiones. Proporcionar a los responsables de toma de decisiones un entendimiento de los escenarios peor y más probable, de empresa.	N/A	Analisis de riesgo e informes, revisión de resultados de evaluaciones

APO12	Gestionar el riesgo	APO12.05	Definir un portafolio de acciones para la gestión de riesgos	Proceso	Determinar si cada entidad organizativa supervisa el riesgo y acepta la responsabilidad para operar dentro de sus niveles de tolerancia individuales y de portafolio. 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.	N/A	Propuestas de proyecto para reducir el riesgo
APO12	Gestionar el riesgo	APO12.06	Responder al riesgo	Proceso	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. Aplicar el plan de respuesta apropiado para minimizar el impacto cuando ocurren incidentes de riesgo.	Acciones correctoras para tratar las desviaciones de gestión de riesgos	Planes de respuesta para incidentes, comunicación del impacto del riesgo, causas raíz
APO013	Gestionar la Seguridad	APO13.01	Establecer y mantener un SGSI.	Proceso	6. Definir y comunicar los roles y las responsabilidades de la gestión de la seguridad de la información	Enfoque de seguridad de la empresa	Política de SGSI Declaración de alcance del SGSI
APO013	Gestionar la Seguridad	APO13.02	Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.	Proceso	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. 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. 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. 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. 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.	Diferencias y cambios necesarios para alcanzar la capacidad objetivo Propuestas de proyectos para reducir el riesgo	Plan de tratamiento de riesgos de seguridad de la información Casos de negocio de seguridad de información
APO013	Gestionar la Seguridad	APO13.03	Supervisar y revisar el SGSI	Proceso	Proporcionar información para el mantenimiento de los planes de seguridad para que consideren las incidencias de las actividades de supervisión y revisión periódica.	Incidentes clasificados y priorizados y requerimientos de servicios	Informes de auditoría del SGSI Recomendaciones para mejorar el SGSI

BAI02	Gestionar la definición de requisitos	BAI02.01	Definir y mantener los requerimientos técnicos y funcionales de negocio.	N/A	a. 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.	a. Modelo de arquitectura de la información b. Descripciones de los dominios de referencia y definición de arquitectura c. Procedimientos de integridad de datos d. Guías de control y seguridad de los datos e. Guías de clasificación de datos	a. Repositorio de definición de requerimientos
BAI02	Gestionar la definición de requisitos	BAI02.03	Gestionar los riesgos de los requerimientos.	N/A	a. 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). b. Analizar y priorizar los riesgos de los requerimientos conforme probabilidad e impacto. Si aplica, determinar los impactos en coste y tiempo. c. Identificar modos de controlar, evitar o mitigar los riesgos de los requerimientos en orden de prioridad.	N/A	a. Registro de riesgo de los requerimientos b. Acciones de mitigación de riesgo
BAI04	Gestionar la Disponibilidad y la Capacidad	BAI04.01	Evaluar la disponibilidad, rendimiento y capacidad actual y crear una línea de referencia	Proceso	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. 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. Identificar y dar seguimiento a todos los incidentes causados por un rendimiento o una capacidad inadecuados.	Registro de requisitos de riesgo	Evaluaciones respecto a ANSs
BAI04	Gestionar la Disponibilidad y la Capacidad	BAI04.02	Evaluar el impacto en el negocio.	Proceso	1. Identificar solamente aquellas soluciones o servicios que son críticas para los procesos de gestión de la disponibilidad y la capacidad. 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.	ANSs internos y externos	Escenarios de disponibilidad, rendimiento y capacidad
BAI04	Gestionar la Disponibilidad y la Capacidad	BAI04.04	Supervisar y revisar la disponibilidad y la capacidad.	Proceso	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. 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. Integrar las actividades de supervisión e información en las actividades iterativas de gestión de la capacidad (supervisión, análisis, ajuste e	N/A	Informes de disponibilidad y rendimiento

					implementaciones). 4. Proveer informes de capacidad para los procesos de presupuesto.		
BAI04	Gestionar la Disponibilidad y la Capacidad	BAI04.05	Investigar y abordar cuestiones de disponibilidad, rendimiento y capacidad.	Proceso	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. 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. 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).	N/A	Brechas de rendimiento y capacidad
BAI05	Gestionar la Facilitación del Cambio Organizativo	BAI05.04	Facultar a los que juegan algún papel e identificar ganancias en el corto plazo.	N/A	2. Planificar las necesidades de formación del personal para desarrollar las habilidades y actitudes adecuadas para que se sientan facultados.	N/A	Metas de desempeño de RRHH alineadas APO07.04 Beneficios en el corto plazo (quick-wins) identificados BAI01.04 Comunicación de los beneficios BAI01.06
BAI05	Gestionar la Facilitación del Cambio Organizativo	BAI05.04	Facultar a los que juegan algún papel e identificar ganancias en el corto plazo.	N/A	3. Alinear los procesos de RRHH y sistemas de medición (p. ej., evaluación del desempeño, decisiones de compensación, decisiones de promoción, reclutamiento y contratación) para dar soporte a la visión.	N/A	Metas de desempeño de RRHH alineadas APO07.04 Beneficios en el corto plazo (quick-wins) identificados BAI01.04 Comunicación de los beneficios BAI01.06
BAI07	Gestionar la Aceptación del Cambio y la Transición	BAI07.01	Establecer un plan de implementación.	Proceso	Confirmar que todos los planes de implantación son aprobados por las partes interesadas tanto de ámbito técnico como de negocio, y revisados por auditoría interna, si es apropiado.	Plan de gestión de la calidad Plan y cronograma de cambio Peticiones de cambio aprobadas	Plan de implantación aprobado. Proceso de marcha atrás de la implantación o de recuperación
BAI07	Gestionar la Aceptación del Cambio y la Transición	BAI07.04	Establecer un entorno de pruebas.	Proceso	Crear una base de datos de pruebas que sea representativa del entorno de producción. Sanear los datos reales usados en el entorno de pruebas de acuerdo a las necesidades de negocio y estándares de la organización (ej. considere si los requisitos de cumplimiento normativo o legal obligan al uso de datos saneados).	N/A	Datos de prueba
BAI07	Gestionar la Aceptación del Cambio y la Transición	BAI07.05	Ejecutar pruebas de aceptación.	Proceso	Revisar el registro categorizado de errores encontrados en el proceso de pruebas por el equipo de desarrollo, verificando que todos los errores han sido corregidos o aceptados formalmente.	N/A	Registro de resultados de las pruebas Evaluación de los resultados de las pruebas de aceptación

BAI08	Gestionar el Conocimiento	BAI04.01	Cultivar y facilitar una cultura de intercambio de conocimientos	Proceso	1. Comunicar proactivamente el valor del conocimiento para impulsar la creación, uso, reutilización y compartición de conocimiento. 2. Impulsar la compartición y transferencia de conocimiento mediante la identificación de factores que influyan en la motivación. 3. Crear un entorno, herramientas y elementos que den soporte a la compartición y transferencia de conocimientos. 4. Integrar prácticas de gestión del conocimiento en otros procesos de TI.		Comunicaciones sobre el valor del conocimiento
BAI08	Gestionar el Conocimiento	BAI04.03	Organizar y contextualizar la información, transformándola en conocimiento.	Proceso	1. Identificar atributos compartidos y casar fuentes de información, creando relaciones entre conjuntos de información (etiquetado de información). 2. Crear vistas para conjuntos de datos relacionados, considerando requisitos organizativos y de las partes interesadas. 3. Concebir e implantar un esquema para gestionar la información no estructurada que no esté disponible a partir de fuentes formales (ej. conocimiento experto). 4. Publicar y hacer accesible el conocimiento a las partes interesadas relevantes basándose en roles y mecanismos de acceso	Planes de transferencia de conocimiento	Repositorios de información publicada
BAI09	Gestionar los Activos	BAI09.01	Identificar y registrar los activos actuales.	N/A	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.	BAI03.04 Actualizaciones al inventario de activos BAI10.02 Repositorio de configuración	Registro de activos APO06.01 BAI10.03 Resultados de comprobaciones físicas de inventario BAI10.03_ BAI10.04_ DSS05.03 Resultados de revisiones de adecuación al objetivo APO02.02
BAI09	Gestionar los Activos	BAI09.01	Identificar y registrar los activos actuales.	N/A	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.	BAI03.04 Actualizaciones al inventario de activos BAI10.02 Repositorio de configuración	Registro de activos APO06.01 BAI10.03 Resultados de comprobaciones físicas de inventario BAI10.03_ BAI10.04_ DSS05.03 Resultados de revisiones de adecuación al objetivo APO02.02
BAI09	Gestionar los Activos	BAI09.01	Identificar y registrar los activos actuales.	N/A	5. Determinar de forma regular si cada activo continúa proporcionando valor y, si es así, estimar la vida útil prevista de dicha validez.	BAI03.04 Actualizaciones al inventario de activos BAI10.02 Repositorio de configuración	Registro de activos APO06.01 BAI10.03 Resultados de comprobaciones físicas de inventario BAI10.03_ BAI10.04_ DSS05.03 Resultados de revisiones de adecuación al objetivo APO02.02

BAI09	Gestionar los Activos	BAI09.02	Gestionar Activos Críticos.	N/A	2. Supervisar el rendimiento de los activos críticos examinando las tendencias de incidentes y, en caso necesario, tomar medidas para reparar o reemplazar.	N/A	Comunicación de tiempo de inactividad planificado para mantenimiento PO08.04 Contratos de mantenimiento Interno
BAI09	Gestionar los Activos	BAI09.02	Gestionar Activos Críticos.	N/A	3. De forma regular, considerar el riesgo de fallo o necesidad del reemplazo de cada activo crítico.	N/A	Comunicación de tiempo de inactividad planificado para mantenimiento PO08.04 Contratos de mantenimiento Interno
BAI09	Gestionar los Activos	BAI09.02	Gestionar Activos Críticos.	N/A	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.	N/A	Comunicación de tiempo de inactividad planificado para mantenimiento PO08.04 Contratos de mantenimiento Interno
BAI09	Gestionar los Activos	BAI09.02	Gestionar Activos Críticos.	N/A	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.	N/A	Comunicación de tiempo de inactividad planificado para mantenimiento PO08.04 Contratos de mantenimiento Interno
BAI09	Gestionar los Activos	BAI09.02	Gestionar Activos Críticos.	N/A	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.	N/A	Comunicación de tiempo de inactividad planificado para mantenimiento PO08.04 Contratos de mantenimiento Interno
BAI09	Gestionar los Activos	BAI09.02	Gestionar Activos Críticos.	N/A	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.	N/A	Comunicación de tiempo de inactividad planificado para mantenimiento PO08.04 Contratos de mantenimiento Interno
BAI09	Gestionar los Activos	BAI09.03	Gestionar el ciclo de vida de los activos.	N/A	1. Adquirir todos los activos basándose en solicitudes aprobadas y de acuerdo con las políticas y las prácticas de adquisición de la empresa.	N/A	Solicitudes de adquisición de activos aprobadas. Interno Registro de activos actualizado. BAI10.03 Retirada autorizada de activos. BAI10.03
BAI09	Gestionar los Activos	BAI09.03	Gestionar el ciclo de vida de los activos.	N/A	2. Identificar el origen, recibir, verificar, probar y registrar todos los activos de una manera controlada, incluyendo el etiquetado físico, si fuera necesario.	N/A	Solicitudes de adquisición de activos aprobadas. Interno Registro de activos actualizado. BAI10.03 Retirada autorizada de activos. BAI10.03

BAI09	Gestionar los Activos	BAI09.03	Gestionar el ciclo de vida de los activos.	N/A	3. Aprobar los pagos y completar el proceso con proveedores según las condiciones acordadas por contrato.	N/A	Solicitudes de adquisición de activos aprobadas. Interno Registro de activos actualizado. BAI10.03 Retirada autorizada de activos. BAI10.03
BAI09	Gestionar los Activos	BAI09.03	Gestionar el ciclo de vida de los activos.	N/A	5. Asignar activos a los usuarios, con aceptación y firma de responsabilidades, según corresponda.	N/A	Solicitudes de adquisición de activos aprobadas. Interno Registro de activos actualizado. BAI10.03 Retirada autorizada de activos. BAI10.03
BAI09	Gestionar los Activos	BAI09.03	Gestionar el ciclo de vida de los activos.	N/A	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.	N/A	Solicitudes de adquisición de activos aprobadas. Interno Registro de activos actualizado. BAI10.03 Retirada autorizada de activos. BAI10.03
DSS01	Gestionar Operaciones	DSS01.02	Gestionar servicios externalizados de TI	Proceso	Asegurar que los procesos y requerimientos 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.	Plan de operación y uso	Planes de aseguramiento independientes
DSS02	Gestionar Peticiones e Incidentes de Servicio	DSS02.01	Definir esquemas de clasificación de incidentes y peticiones de servicio.	Proceso	3. Definir modelos de peticiones de servicio según el tipo de petición de servicio correspondiente para facilitar la autoayuda y el servicio eficiente para las peticiones estándar.	Reglas de monitorización de activos y condiciones de eventos	Criterios para registro de problemas
DSS02	Gestionar Peticiones e Incidentes de Servicio	DSS02.06	Cerrar peticiones de servicio e incidentes	Proceso	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. 2. Cerrar peticiones de servicio e incidentes.	Registros de problemas cerrados	Confirmación del usuario de resolución o cumplimiento satisfactorios
DSS04	Gestionar la continuidad	DSS04.01	Definir la política de continuidad del negocio, objetivos y alcance.	N/A	a. Identificar procesos de negocio internos y subcontratados y actividades de servicio que son críticas para las operaciones de la empresa o necesarias para cumplir con las obligaciones legales y/o contractuales. b. Identificar las partes interesadas clave y los roles y responsabilidades para definir y acordar la política de continuidad y su alcance. c. Definir y documentar los objetivos y el alcance mínimos acordados de la política de continuidad del negocio e imbricar la planificación de continuidad en la cultura empresarial. d. Identificar procesos de soporte al negocio esenciales y servicios TI relacionados.	N/A	a. Política y objetivos de continuidad de negocio b. Escenarios de incidentes que causan una interrupción

DSS04	Gestionar la continuidad	DSS04.02	Mantener una estrategia de continuidad.	N/A	a. Identificar escenarios potenciales probables que puedan dar pie a eventos que puedan causar incidentes disruptivos importantes. b. Realizar un análisis de impacto en el negocio para evaluar el impacto en tiempo de una disrupción en funciones críticas del negocio y el efecto que tendría en ellas. c. Establecer el tiempo mínimo necesario para recuperar un proceso de negocio y su soporte de TI, basándose en una duración aceptable de interrupción del negocio y la interrupción máxima tolerable. d. Analizar la probabilidad de amenazas que puedan causar pérdidas de continuidad de negocio e identificar medidas que puedan reducir la probabilidad y el impacto, mejorando la prevención e incrementando la resiliencia. e. Analizar los requerimientos de continuidad para identificar las posibles estrategias de negocio y opciones técnicas.	a. Causas raíz relacionadas con riesgos b. Comunicaciones del impacto de los riesgos	a. Análisis de impacto en el negocio b. Requerimientos de continuidad
DSS04	Gestionar la continuidad	DSS04.03	Desarrollar e implementar una respuesta a la continuidad del negocio.	N/A	a. Definir las acciones y comunicaciones de respuesta a incidentes que deben ser realizadas en un evento de disrupción. Definir los roles y responsabilidades relacionadas, incluyendo la responsabilidad para la política y la implementación. b. Desarrollar y mantener planes de continuidad de negocio operativos que contengan los procedimientos que deben ser seguidos para permitir continuar operando los procesos críticos de negocio. c. Asegurar que los proveedores y socios externos clave tengan implantados planes de continuidad efectivos. Obtener evidencias auditadas si es necesario. d. Definir y documentar los recursos necesarios para soportar los procedimientos de continuidad y recuperación, considerando personas, instalaciones e infraestructura de TI. e. Definir y documentar los requerimientos de información de respaldo para soportar los planes, incluyendo planes y documentos en papel, así como ficheros de datos y considerar las necesidades de seguridad y almacenamiento en otra ubicación.	N/A	a. Acciones y comunicaciones de respuesta a incidentes b. Plan de Continuidad de Negocio (BCP)
DSS04	Gestionar la continuidad	DSS04.04	Ejercitar, probar y revisar el plan de continuidad.	N/A	a. Definir los objetivos para ejercitar y probar los sistemas del plan (de negocio, técnicos, logísticos, administrativos, procedimentales y operacionales) para verificar la completitud del plan de continuidad de negocio (BCP) para enfrentarse a los riesgos de negocio.	N/A	N/A
DSS04	Gestionar la continuidad	DSS04.05	Revisar, mantener y mejorar el plan de continuidad.	N/A	a. Revisar el plan de continuidad regularmente para considerar el impacto de cambios nuevos o mayores en: organización de la empresa, procesos de negocio, acuerdos de externalización, tecnologías, infraestructura, sistemas operativos y sistemas de aplicaciones.	N/A	N/A
DSS04	Gestionar la continuidad	DSS04.07	Gestionar acuerdos de respaldo.	N/A	a. Hacer copias de seguridad de sistemas, aplicaciones, datos y documentación de acuerdo a una planificación definida. b. Asegurar que los sistemas, aplicaciones, datos y documentación mantenidos o procesados por terceras partes están adecuadamente respaldados o asegurados de otra forma. Considerar el hecho de requerir el retorno de las copias de seguridad de terceras partes. Considerar acuerdos de depósito (escrow). c. Extender la concienciación y la formación en Planes de Continuidad de Negocio (BCP). d. Probar y mantener legibles las copias de seguridad y las archivadas periódicamente.	N/A	a. Probar los resultados de las copias de seguridad de los datos

DSS05	Asegurar la Transparencia de las partes interesadas	DSS05.01	Proteger contra software malicioso (malware).	Proceso	Divulgar concienciación sobre el software malicioso y forzar procedimientos y responsabilidades de prevención. 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 semiautomáticamente).	N/A	Política de prevención de software malicioso. Evaluaciones
DSS05	Asegurar la Transparencia de las partes interesadas	DSS05.02	Gestionar la seguridad de la red y las conexiones.	Proceso	Basándose en el análisis de riesgos y en los requerimientos del negocio, establecer y mantener una política de seguridad para las conexiones. 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.	Guías de clasificación de la información	Política de seguridad en la conectividad. Resultados de las pruebas de intrusión
DSS05	Asegurar la Transparencia de las partes interesadas	DSS05.03	Gestionar la seguridad de los puestos de usuario final.	Proceso	Configurar los sistemas operativos de forma segura. Implementar mecanismos de bloqueo.	Modelo de arquitectura de la información. Resultados de pruebas de inventarios físicos. Informe de violaciones	Políticas de seguridad para dispositivos de usuario final
DSS05	Asegurar la Transparencia de las partes interesadas	DSS05.04	Gestionar la identidad del usuario y el acceso lógico.	Proceso	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.	Definición de roles y responsabilidades relacionadas con TI	Derechos de acceso de los usuarios aprobados. Resultado revisiones
DSS05	Asegurar la Transparencia de las partes interesadas	DSS05.05	Gestionar el acceso físico a los activos de TI.	Proceso	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. 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.	N/A	Peticiones de acceso aprobadas. Y registros de acceso
DSS05	Asegurar la Transparencia de las partes interesadas	DSS05.06	Gestionar documentos sensibles y dispositivos de salida.	Proceso	Establecer procedimientos para gobernar la recepción, uso, eliminación y destrucción de formularios especiales y dispositivos de salida, dentro, en y fuera de la empresa. Asignar privilegios de acceso a documentos sensibles y dispositivos de salida basados en el principio del menor privilegio, equilibrando riesgo y requerimientos de negocio.	Modelo de arquitectura de la información	Inventario de documentos y dispositivos sensibles. Privilegio de acceso
DSS05	Asegurar la Transparencia de las partes interesadas	DSS05.07	Supervisar la infraestructura para detectar eventos relacionados con la seguridad.	Proceso	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. 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.	N/A	Registros de incidentes de seguridad. Características e incidentes

DSS06	Gestionar Controles de Proceso de Negocio	DSS06.01	Alinear las actividades de control embebidas en los procesos de negocio con los objetivos corporativos.	Proceso	Priorizar las actividades de control basadas en el riesgo inherente del negocio e identificar controles clave. 3. Asegurar la propiedad de las actividades de control claves. 4. Supervisar continuamente las actividades de control de extremo a extremo para identificar oportunidades de mejora	Procedimientos de integridad de datos	Resultados de las revisiones de efectividad de procesamiento
DSS06	Gestionar Controles de Proceso de Negocio	DSS06.02	Controlar el procesamiento de la información	Proceso	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. 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.	Plan de operación y uso	Informes de control de procesamiento
DSS06	Gestionar Controles de Proceso de Negocio	DSS06.03	Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.	Proceso	Asignar roles y responsabilidades sobre la base de la descripción aprobada de puestos y actividades de procesos de negocio asignadas. 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.	Responsabilidades asignadas para la gestión de recursos Roles, responsabilidades y derechos de decisión del SGC	Responsabilidades y roles asignados Niveles de autoridad asignados
DSS06	Gestionar Controles de Proceso de Negocio	DSS06.04	Gestionar errores y excepciones.	Proceso	Revisar errores, excepciones y desviaciones. 3. Hacer seguimiento, corregir, aprobar y reenviar documentos fuente y transacciones. 4. Mantener evidencia de las medidas correctivas. 5. Informar acerca de errores de proceso de información relevantes de manera oportuna para realizar el análisis de tendencias y causas raíz.	N/A	Evidencia de corrección y remediación de errores Informes de errores y análisis de las causas raíz
DSS06	Gestionar Controles de Proceso de Negocio	DSS06.05	Asegurar la trazabilidad de los eventos y responsabilidades de información.	Proceso	Capturar la fuente de información, evidencia que la soporta y el registro de las transacciones. 3. Eliminar la fuente de información, la evidencia que la soporta y el registro de transacciones de acuerdo con la política de retención.	N/A	Registro de transacciones
DSS06	Gestionar Controles de Proceso de Negocio	DSS06.06	Asegurar los activos de información.	Proceso	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	N/A	Informes de violación
MEA01	Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad	MEA01.04	Analizar e informar sobre el rendimiento.	N/A	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.	N/A	Informes de desempeño. EDM01.03_Todo APO_Todo BAI_Todo DSS_ Todo MEA

MEA01	Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad	MEA 01.04	Analizar e informar sobre el rendimiento.	N/A	5. Analizar la causa de las desviaciones respecto a las metas, iniciar acciones correctivas, asignar responsabilidades para la remediación y realizar su seguimiento. En el momento oportuno, revisar todas las desviaciones y buscar causas raíz cuando sea necesario. Documentar las incidencias para contar con guía adicional si el problema vuelve a aparecer. Documentar los resultados.	N/A	Informes de desempeño. EDM01.03_Todo APO_Todo BAI_Todo DSS_ Todo MEA
MEA02	Supervisar, evaluar y valorar el sistema de control interno	MEA 02.01	Supervisar el control interno.	N/A	a. 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. b. Considerar las evaluaciones independientes del sistema de control interno (p. ej. por auditoría interna o iguales - peers). c. 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). e. 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. f. 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. g. 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.	a. Resultados de la evaluación de riegos realizados por terceros b. Informes de auditoría del SGSI estándares y buenas prácticas de la industria	a. Resultados de las revisiones y supervisión del control interno
MEA02	Supervisar, evaluar y valorar el sistema de control interno	MEA 02.02	Revisar la efectividad de los controles sobre los procesos de negocio.	N/A	a. Entender y priorizar el riesgo de acuerdo con los objetivos organizativos. b. Identificar los controles clave y desarrollar una estrategia adecuada para la validación de controles. c. Identificar la información que indica de forma convincente si el entorno de control interno está operando de forma efectiva. d. Desarrollar e implementar procedimientos eficientes para determinar si la información convincente está basada en los criterios de información. e. Mantener evidencia de la efectividad del control.	N/A	a. Evidencia de la efectividad del control
MEA03	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos	MEA 03.01	Identificar requisitos externos de cumplimiento.	Proceso	Asignar la responsabilidad de identificar y supervisar los cambios legales y regulatorios y otros requisitos contractuales externos aplicables a la utilización de recursos de TI y al procesamiento de la información dentro de las operaciones de negocio y de TI. Identificar y valorar la totalidad de los posibles requisitos de cumplimiento y su impacto sobre las actividades de TI en ámbitos como los flujos de datos, la privacidad, los controles internos, los informes financieros, la regulación sectorial, la propiedad intelectual y la seguridad e higiene en el trabajo.	Requisitos de cumplimiento legal y regulatorio	Registro de requisitos de cumplimiento

MEA03	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos	MEA 03.02	Optimizar la respuesta a requisitos externos.	Proceso	Revisar y ajustar con regularidad las políticas, los principios, los estándares, los procedimientos y las metodologías para que mantengan su eficacia en asegurar el cumplimiento requerido y la gestión del riesgo empresarial. Contar para ello con expertos internos y externos, según proceda. Comunicar nuevos requisitos y modificaciones	N/A	Políticas, principios, procedimientos y estándares actualizados. Comunicaciones de las modificaciones
EDM02	Asegurar la Entrega de Beneficios	EDM 02.01	Evaluar la Optimización de valor	Proceso/02	Comprender los elementos clave de gobierno necesarios para la entrega fiable, segura y coste efectivo de un valor óptimo por el uso de los servicios, activos y recursos de TI existentes y potenciales.	Hoja de ruta estratégica	Evaluación de alineación estratégica
EDM03	Asegurar la Optimización del Riesgo	Genér ico	N/A	TI/04	Porcentaje de procesos de negocio críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos	N/A	N/A
EDM03	Asegurar la Optimización del Riesgo	Genér ico	N/A	TI/06	Porcentaje de servicios TI con costes operativos y beneficios esperados claramente definidos y aprobados.	N/A	N/A
APO01	Gestionar el Marco de Gestion de TI	APO0 1.02	Establecer roles y responsabilidade s	Proceso	a. 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. b. Asegurar que la rendición de cuentas queda definida a través de los roles y responsabilidades.	Niveles de autoridad Responsabilidades asignadas para la gestión de recursos Roles, responsabilidades y derechos de decisión dentro del sistema de gestión de la calidad (SGC) • Niveles de autoridad asignados • Roles y responsabilidades asignados	Definición de roles y responsabilidades relativos a TI Definición de prácticas de supervisión
APO02	Gestionar la Estrategia	APO0 2.03	Definir el objetivo de las capacidades de TI	N/A	2. Identificar las amenazas por el rechazo a las actuales y nuevas tecnologías adquiridas.	APO04.05 • Análisis de las iniciativas rechazadas • Resultados y recomendaciones de las iniciativas de pruebas de concepto.	Objetivos de TI a alto nivel Interno Requerimientos del negocio y capacidades de TI Interno Propuesta de cambio en la arquitectura del negocio APO03.03
APO02	Gestionar la Estrategia	APO0 2.03	Definir el objetivo de las capacidades de TI	N/A	3. Definir los objetivos/metas de TI a alto nivel y cómo contribuirán a los objetivos de negocio empresariales.	APO04.05 • Análisis de las iniciativas rechazadas • Resultados y recomendaciones de las iniciativas de pruebas de concepto.	Objetivos de TI a alto nivel Interno Requerimientos del negocio y capacidades de TI Interno Propuesta de cambio en la arquitectura del negocio APO03.03

APO02	Gestionar la Estrategia	APO02.04	Realizar un análisis de diferencias.	N/A	3. Evaluar el impacto de posibles cambios en el negocio y en los modelos operativos de TI, la capacidad de investigación y desarrollo de tecnología y los programas de inversión de TI.	EDM02.01 Evaluación de la alineación estratégica APO04.06 Evaluaciones sobre el uso de enfoques innovadores APO05.02 Expectativas sobre el retorno de inversión BAI01.05 Resultados del programa de supervisión de consecución de objetivos BAI01.06 Revisión de los resultados de cambios de fase (stage- gate) BAI01.13 Resultados de la revisión post-implementación	Diferencias y cambios requeridos para alcanzar la meta de capacidad_EDM04.01_APO13.02_BAI03.11 Declaración del valor beneficio para el entorno deseado_BAI03.11
APO02	Gestionar la Estrategia	APO02.06	Comunicar la estrategia y la dirección de TI.	N/A	1. Desarrollar y mantener una red de aprobación, apoyo e impulso de la estrategia de TI.	EDM04.02 Comunicación de las estrategias de los recursos	Plan de comunicación Interno Paquete de comunicación Todo APO_Todo BAI_Todo DSS_Todo MEA
APO02	Gestionar la Estrategia	APO02.06	Comunicar la estrategia y la dirección de TI.	N/A	4. Obtener realimentación y actualizar el plan de comunicaciones y de entrega según sea necesario.	EDM04.02 Comunicación de las estrategias de los recursos	Plan de comunicación Interno Paquete de comunicación Todo APO_Todo BAI_Todo DSS_Todo MEA
APO04	Gestionar la Innovación	APO04.04	Evaluar el potencial de las tecnologías emergentes y las ideas innovadoras	Proceso	Evaluar las tecnologías identificadas, considerando aspectos tales como tiempo para alcanzar la madurez, riesgo inherente de la nueva tecnología (incluyendo posibles implicaciones legales), ajuste con la arquitectura empresarial y potencial para proporcionar valor añadido.	N/A	Evaluar ideas de innovación, alcance de la prueba de concepto y descripción de los casos de negocio
APO06	Gestionar el Presupuesto y los Costes	APO06.04	Modelar y asignar costes.	N/A	1. Clasificar todos los costes de TI adecuadamente, incluidos los relativos a los proveedores de servicio, de acuerdo con el marco de contabilidad de la gestión de la empresa.		Costes de TI categorizados Interno Modelo de asignación de costes Interno Comunicaciones de asignación de costes. Interno Procedimientos operativos Interno
APO06	Gestionar el Presupuesto y los Costes	APO06.04	Modelar y asignar costes.	N/A	4. Diseñar el modelo de costes para ser lo suficientemente transparente como para permitir a los usuarios identificar su uso real y sus cargos, y para mejor catalizar la previsibilidad de los costes de TI y la utilización eficiente y eficaz de los recursos de TI.		Costes de TI categorizados Interno Modelo de asignación de costes Interno Comunicaciones de asignación de costes. Interno Procedimientos operativos Interno

APO07	Gestionar los recursos humanos	APO07.01	Mantener la dotación de personal suficiente y adecuada.	N/A	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. 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. 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.	a. Principios rectores para la asignación de recursos y capacidades b. Plan y presupuesto de TI.	a. Evaluaciones de requisitos de personal b. Planes de desarrollo de carrera y de competencias
APO07	Gestionar los recursos humanos	APO07.02	Identificar personal clave de TI.	N/A	a. Minimizar la dependencia en una sola persona	N/A	N/A
APO07	Gestionar los recursos humanos	APO07.03	Mantener las habilidades y competencias del personal.	N/A	a. 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.	N/A	a. Planes de desarrollo de habilidades
APO07	Gestionar los recursos humanos	APO07.04	Evaluar el desempeño laboral de los empleados.	N/A	a. 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). b. Implementar y comunicar un proceso disciplinario. c. Recopilar los resultados de la evaluación de desempeño de 360 grados.	N/A	a. Evaluaciones de desempeño
APO07	Gestionar los recursos humanos	APO07.05	Planificar y realizar un seguimiento del uso de recursos humanos de TI y del negocio.	N/A	a. 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. b. Mantener información adecuada sobre el tiempo dedicado a diferentes tareas, trabajos, servicios o proyectos.	N/A	a. Análisis de deficiencias en la obtención de recursos
APO07	Gestionar los recursos humanos	APO07.06	Gestionar el personal contratado.	N/A	a. 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.	N/A	a. Políticas de contratación de personal b. Revisión de acuerdos contractuales

APO08	Gestionar las relaciones	APO08.01	Entender las expectativas del negocio	Proceso	Identificar las partes interesadas, revisar la orientación de la empresa, mantener una atención sobre los procesos, esclarecer expectativas, acuerdos de expectativas, gestionarlas	Hoja de ruta estratégica	Expectativa de negocio aclarada y acordada
APO08	Gestionar las relaciones	APO08.03	Gestionar las relaciones con el negocio	Proceso	Asignar un responsable de la relación como punto único de contacto por cada unidad de negocio significativa. Gestionar la relación de un modo formal y transparente que asegure el enfoque. Definir y comunicar un proceso de reclamaciones. Planificar interacciones específicas. Asegurar que las decisiones claves son acordadas	Incidentes, confirmación de expectativas cumplidas, estado de las peticiones	Decisiones clave, estado de las quejas
APO08	Gestionar las relaciones	APO08.05	Proveer datos de entrada para la mejora continua de los servicios	Proceso	Análisis de satisfacción de clientes y proveedores, trabajar conjuntamente para identificar, comunicar e implementar iniciativas de mejora	Catalogo servicio, resultados de calidad, requisitos clientes, resultados revisiones, monitorización, plan mantenimiento	Análisis de satisfacción, definición de proyectos de mejora potencial
APO09	Gestionar los acuerdos de servicio	APO09.01	Identificar servicios TI.	Proceso	Identificar áreas de mejora de los servicios existentes y de las opciones de nivel del servicio. Analizar las actividades de los procesos de negocio para identificar la necesidad de servicios TI nuevos o rediseñados	N/A	Carencias identificadas de los servicios TI de cara al negocio
APO09	Gestionar los acuerdos de servicio	APO09.03	Definir y preparar acuerdos de servicio	Proceso	4. Mantener una relación estrecha con la gestión de proveedores para asegurar que los contratos comerciales apropiados con proveedores de servicio externos cimentan los acuerdos de servicio con los clientes, siempre que sea aplicable.	Requisitos del cliente para la gestión de la calidad.	Acuerdos de nivel de servicio (ANSs) Acuerdos de nivel operativos (OLAs).
APO09	Gestionar los acuerdos de servicio	APO09.04	Supervisar e informar de los niveles de servicio	Proceso	Hacer revisiones regulares para anticipar e identificar tendencias en el rendimiento del nivel de servicio. Proporcionar información de gestión apropiada para ayudar en la gestión del rendimiento. Acordar planes de acción y remedio para los incidentes del rendimiento o tendencias negativas del mismo	Causas raíz de fallos de calidad en la entrega Resultados de la monitorización de la calidad de la entrega del servicio o solución Incidentes y peticiones de servicio priorizados y clasificados Incidentes y peticiones de servicio cerrados	Planes de acción de mejora y remedio
APO09	Gestionar los acuerdos de servicio	APO09.05	Revisar acuerdos de servicio y contratos.	Proceso	Revisar los términos de los acuerdos de servicio regularmente para asegurar que son efectivos y actuales y que los cambios en los requisitos, servicios TI, paquetes de servicios u opciones de nivel de servicio se tienen en cuenta cuando sea apropiado.	Resultados de revisiones y auditorías de calidad	ANS actualizados
APO10	Gestionar los Proveedores	APO10.05	Supervisar el cumplimiento y el rendimiento del proveedor.	N/A	Definir y documentar los criterios para supervisar el rendimiento de los proveedores alineado con los acuerdos de nivel de servicio y asegurando que el proveedor informa según estos criterios de forma regular y transparente.	N/A	Criterios de supervisión del cumplimiento de los proveedores Interno Resultados de las revisiones de la supervisión del cumplimiento de los proveedores_MEA01.03

APO10	Gestionar los Proveedores	APO10.05	Supervisar el cumplimiento y el rendimiento del proveedor.	N/A	Supervisar y revisar la entrega de servicios para asegurar que el proveedor está proporcionando una calidad del servicio adecuada, cumpliendo los requisitos y las condiciones de los contratos.	N/A	Criterios de supervisión del cumplimiento de los proveedores Interno Resultados de las revisiones de la supervisión del cumplimiento de los proveedores_MEA01.03
APO10	Gestionar los Proveedores	APO10.05	Supervisar el cumplimiento y el rendimiento del proveedor.	N/A	Revisar el rendimiento y el coste de los proveedores para asegurar que son competitivos y fiables, en comparación con proveedores alternativos y condiciones de mercado.	N/A	Criterios de supervisión del cumplimiento de los proveedores Interno Resultados de las revisiones de la supervisión del cumplimiento de los proveedores_MEA01.03
APO10	Gestionar los Proveedores	APO10.05	Supervisar el cumplimiento y el rendimiento del proveedor.	N/A	Registrar y evaluar los resultados de la revisión periódica y discutirlos con el proveedor para identificar las necesidades y oportunidades de mejora.	N/A	Criterios de supervisión del cumplimiento de los proveedores Interno Resultados de las revisiones de la supervisión del cumplimiento de los proveedores_MEA01.03
APO11	Gestionar la calidad	APO11.01	Establecer un sistema de gestión de la calidad (SGC).	N/A	a. Definir roles, tareas, capacidades de decisión y responsabilidades para la gestión de la calidad, dentro de la estructura organizativa.	a. Sistema empresarial de gestión de la calidad	a. Roles, responsabilidades y capacidades de decisión del SGC. B. Planes de gestión de calidad
APO11	Gestionar la calidad	APO11.02	Definir y gestionar los estándares, procesos y prácticas de calidad.	N/A	a. Definir las normas, procedimientos y prácticas de gestión de la calidad en consonancia con los requisitos del marco de control TI. Hacer uso de las mejores prácticas de la industria como referencia para la mejora y adaptación de los procesos de gestión de la calidad de la empresa.	a. Buenas prácticas de la industria	a. Estándares de calidad
APO11	Gestionar la calidad	APO11.03	Enfocar la gestión de la calidad en los clientes.	N/A	a. Gestionar las necesidades y las expectativas del negocio para cada proceso de negocio, servicio operativo y nuevas soluciones de TI y mantener sus criterios de aceptación de la calidad. Capturar los criterios de aceptación de la calidad para su inclusión en los ANS.	N/A	a. Criterios de aceptación
APO11	Gestionar la calidad	APO11.04	Supervisar y hacer controles y revisiones de calidad.	N/A	a. Supervisar las métricas de calidad basadas en objetivos alineadas con los objetivos generales de calidad y cubriendo la calidad de todos los servicios y los proyectos individuales.	a. Resultados de las revisiones de calidad, excepciones y, correcciones	a. Metas y métricas del proceso de calidad de los servicios
APO11	Gestionar la calidad	APO11.05	Integrar la gestión de la calidad en la implementación de soluciones y la entrega de servicios.	N/A	a. Supervisar de manera continua los niveles de servicio e incorporar prácticas de gestión de la calidad en todos los procesos y prácticas de prestación de servicios. b. Identificar y documentar las causas raíz de las no conformidades y comunicar los resultados a la dirección de TI	N/A	a. Causa raíz en las fallas de la calidad

APO11	Gestionar la calidad	APO11.06	Mantener mejora continua	N/A	a. Identificar ejemplos recurrentes de los defectos de calidad, determinar su causa raíz, evaluar su impacto y resultado y acordar acciones de mejora con todos los miembros de los proyectos y los servicios. b. Promover una cultura de calidad y mejora continua.		a. Comunicaciones sobre las mejores prácticas y la mejora continua
BAI04	Gestionar la Disponibilidad y la Capacidad	BAI04.03	Planificar requisitos de servicio nuevos o modificados	Proceso	técnicas de modelado para validar los planes de disponibilidad, rendimiento y capacidad. 3. Priorizar las necesidades de mejora y crear planes de disponibilidad y capacidad justificables en costes. 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	Componentes de la solución documentados	Planes de capacidad y rendimiento
BAI05	Gestionar la Facilitación del Cambio Organizativo	BAI05.01	Establecer el deseo de cambiar.	N/A	1. Evaluar el alcance y el impacto del cambio divisado, las diferentes partes interesadas que se verán afectadas, la naturaleza del impacto y la involucración necesaria por cada grupo de partes interesadas y la disposición y habilidad actual para adoptar el cambio.	Criterios de aceptación confirmados por las partes interesadas (BAI02.01) Acciones de mitigación de riesgos (BAI02.03)	Comunicaciones de los motivadores del cambio
BAI05	Gestionar la Facilitación del Cambio Organizativo	BAI05.01	Establecer el deseo de cambiar.	N/A	2. Identificar, impulsar y comunicar puntos de conflicto, eventos negativos, riesgos, insatisfacción de clientes y problemas del negocio, así como beneficios iniciales, oportunidades y recompensas futuras y ventajas competitivas, como fundamento para el establecimiento del deseo de cambiar.	Criterios de aceptación confirmados por las partes interesadas (BAI02.01) Acciones de mitigación de riesgos (BAI02.03)	Comunicaciones de los motivadores del cambio
BAI05	Gestionar la Facilitación del Cambio Organizativo	BAI05.03	Comunicar la visión deseada.	N/A	2. Realizar la comunicación a niveles adecuados de la empresa de acuerdo con el plan.	N/A	Plan de comunicación de la visión BAI01.04 Comunicaciones de la visión BAI01.05
BAI05	Gestionar la Facilitación del Cambio Organizativo	BAI05.03	Comunicar la visión deseada.	N/A	4. Verificar la comprensión de la visión deseada y dar respuesta a cualquier cuestión destacada por el personal.	N/A	Plan de comunicación de la visión BAI01.04 Comunicaciones de la visión BAI01.05
BAI05	Gestionar la Facilitación del Cambio Organizativo	BAI05.06	Integrar nuevos enfoques.	N/A	2. Usar sistemas de medida del desempeño para identificar las causas raíz de una baja adopción de los cambios y aplicar medidas correctoras.	N/A	Resultados de auditorías de cumplimiento MEA02.02_MEA03.03 Comunicaciones de concienciación Interno Resultados de la revisión de rendimiento de RRHH APO07.04

BAI05	Gestionar la Facilitación del Cambio Organizativo	BAI05.07	Mantener los cambios.	N/A	1. Proporcionar tutoría, formación, entrenamiento y transferencia de conocimiento al personal nuevo para mantener los cambios.	N/A	Planes de transferencia del conocimiento BAI08.03 BAI08.04 Comunicación del compromiso de la Dirección Interno Revisión del uso operativo MEA02.02
BAI05	Gestionar la Facilitación del Cambio Organizativo	BAI05.07	Mantener los cambios.	N/A	2. Mantener y reforzar los cambios mediante comunicaciones regulares demostrando el compromiso de la alta dirección.	N/A	Planes de transferencia del conocimiento BAI08.03 BAI08.04 Comunicación del compromiso de la Dirección Interno Revisión del uso operativo MEA02.02
BAI05	Gestionar la Facilitación del Cambio Organizativo	BAI05.07	Mantener los cambios.	N/A	3. Realizar revisiones periódicas de la operación y uso de los cambios e identificar mejoras.	N/A	Planes de transferencia del conocimiento BAI08.03 BAI08.04 Comunicación del compromiso de la Dirección Interno Revisión del uso operativo MEA02.02
BAI05	Gestionar la Facilitación del Cambio Organizativo	BAI05.07	Mantener los cambios.	N/A	4. Captar lecciones aprendidas sobre la implementación de los cambios y divulgar este conocimiento en toda la empresa.	N/A	Planes de transferencia del conocimiento BAI08.03 BAI08.04 Comunicación del compromiso de la Dirección Interno Revisión del uso operativo MEA02.02
BAI06	Gestionar los cambios	BAI06.02	Gestionar cambios de emergencia.	N/A	a. Definir qué constituye un cambio de emergencia. b. Asegurar que hay un procedimiento documentado para declarar, evaluar, aprobar de formar preliminar, autorizar una vez hecho el cambio y registrar el cambio de emergencia.	N/A	a. Revisión de cambios de emergencia tras su implementación
BAI06	Gestionar los cambios	BAI06.04	Cerrar y documentar los cambios	N/A	a. Incluir los cambios en la documentación (ej. procedimientos de negocio y operativos de TI, documentación de continuidad de negocio y recuperación frente a desastres, información de configuración, documentación de la aplicación, pantallas de ayuda y material de formación) en el procedimiento de gestión del cambio como parte integral del cambio.	N/A	a. Documentación del cambio
BAI07	Gestionar la Aceptación del Cambio y la Transición	BAI07.02	Planificar la conversión de procesos de negocio, sistemas y datos.	Proceso	Definir un plan de migración de procesos de negocio, datos, servicios e infraestructura de TI. Considerar, por ejemplo, hardware, redes, sistemas operativos, software, datos transaccionales, ficheros maestros, copias de seguridad y archivadas, interfaces con otros sistemas (tanto internos como externos), posibles requisitos de cumplimiento y documentación del sistema en el desarrollo del plan.	N/A	Plan de mitigación

BAI07	Gestionar la Aceptación del Cambio y la Transición	BAI07.06	Pasar a producción y gestionar los lanzamientos.	Proceso	Prepararse para el traspaso del entorno de pruebas al de producción de procedimientos de negocio y servicios que los soportan, aplicaciones e infraestructura, de acuerdo con los estándares de la organización sobre gestión del cambio.	N/A	Plan y registro de lanzamientos
BAI07	Gestionar la Aceptación del Cambio y la Transición	BAI07.08	Ejecutar una revisión post-implantación.	Proceso	Establecer procedimientos para asegurar que las revisiones post-implantación identifican, evalúan e informan	Resultados y auditorías de revisión de la calidad	Informe de revisión. Plan de acciones correctivas
BAI08	Gestionar el Conocimiento	BAI04.02	Identificar y clasificar las fuentes de información.	Proceso	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. 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).	Requisitos y fuentes de conocimiento	Clasificación de fuentes de información
BAI08	Gestionar el Conocimiento	BAI04.04	Utilizar y compartir el conocimiento.	Proceso	2. Transferir el conocimiento a los usuarios de conocimientos basándose en un análisis de necesidades, técnicas de aprendizaje efectivas y herramientas de acceso. 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.	Planes de transferencia de conocimiento	Esquemas de concienciación y formación de conocimiento
BAI09	Gestionar los Activos	BAI09.04	Optimizar el coste de los activos.	N/A	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.	N/A	Resultados de las revisiones de optimización de costes APO02.02 Oportunidades para reducir el coste de activos o aumentar su valor APO02.02
BAI09	Gestionar los Activos	BAI09.04	Optimizar el coste de los activos.	N/A	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.	N/A	Resultados de las revisiones de optimización de costes APO02.02 Oportunidades para reducir el coste de activos o aumentar su valor APO02.02

BAI09	Gestionar los Activos	BAI09.05	Administrar Licencias.	N/A	1. Mantener un registro de todas las licencias de software adquiridas y sus acuerdos de licencia asociados.	N/A	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
BAI09	Gestionar los Activos	BAI09.05	Administrar Licencias.	N/A	2. De forma regular, llevar a cabo una auditoría para identificar a todos las copias de software instalado con licencia.	N/A	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
BAI09	Gestionar los Activos	BAI09.05	Administrar Licencias.	N/A	3. Comparar el número de copias de software instalado con el número de licencias en propiedad. (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. 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.)	N/A	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
DSS01	Gestionar Operaciones	DSS01.04	Gestionar el entorno	Proceso	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. Ubicar y construir las instalaciones de TI para minimizar y mitigar la susceptibilidad ante las amenazas del entorno. Supervisar y mantener dispositivos que detecten amenazas	N/A	Políticas de entorno. Informe de póliza
DSS01	Gestionar Operaciones	DSS01.05	Gestionar las instalaciones	Proceso	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.	N/A	Informes de evaluación de instalaciones. Concienciación en salud y seguridad en el trabajo
DSS02	Gestionar Peticiones e Incidentes de Servicio	DSS02.02	Registrar, clasificar y priorizar peticiones e incidentes	Proceso	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.	• Tiques de incidentes • Reglas de supervisión de activos y condiciones de eventos	Registro de incidentes y peticiones de servicio
DSS02	Gestionar Peticiones e Incidentes de Servicio	DSS02.04	Investigar, diagnosticar y localizar incidentes.	Proceso	Identificar y describir síntomas relevantes para establecer las causas más probables de los incidentes. Hacer referencia a los recursos de conocimientos disponibles (incluyendo errores y problemas conocidos) para identificar posibles resoluciones de incidentes (soluciones temporales y/o soluciones permanentes).	7 plan de soporte adicional	Síntomas de incidentes Interno Registro de problemas

DSS02	Gestionar Peticiones e Incidentes de Servicio	DSS020.05	Resolver y recuperarse de incidentes.	Proceso	4. Documentar la resolución del incidente y evaluar si puede usarse como una fuente de conocimiento en el futuro.	Comunicación de conocimiento aprendido	Resoluciones de incidentes
DSS03	Gestionar Problemas	DSS03.03	Levantar errores conocidos.	N/A	1. Tan pronto como las causas raíz de los problemas se han identificado, crear registros de errores conocidos y desarrollar una solución temporal adecuada.	N/A	Registros de errores conocidos DSS02.05 Soluciones propuestas para errores conocidos BAI06.01
DSS03	Gestionar Problemas	DSS03.03	Levantar errores conocidos.	N/A	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.	N/A	Registros de errores conocidos DSS02.05 Soluciones propuestas para errores conocidos BAI06.01
DSS03	Gestionar Problemas	DSS03.04	Resolver y cerrar problemas.	N/A	3. A través del proceso de resolución, obtener informes periódicos de gestión de cambios acerca del progreso en la resolución de problemas y errores.	DSS02.05 Resoluciones de incidentes DSS02.06 Incidentes y peticiones de servicio cerrados	Registros de problemas cerrados DSS02.06 Comunicación del conocimiento aprendido APO08.04_DSS02.05
DSS03	Gestionar Problemas	DSS03.04	Resolver y cerrar problemas.	N/A	5. Revisar y confirmar la resolución satisfactoria de problemas graves.	DSS02.05 Resoluciones de incidentes DSS02.06 Incidentes y peticiones de servicio cerrados	Registros de problemas cerrados DSS02.06 Comunicación del conocimiento aprendido APO08.04_DSS02.05
DSS04	Gestionar la continuidad	DSS04.06	Proporcionar formación en el plan de continuidad.	N/A	a. Definir y mantener los planes y requerimientos de formación para quienes realicen de manera continuada planificación de la continuidad, análisis de impacto, evaluaciones de riesgos, comunicación con los medios y respuesta a incidentes. Asegurar que los planes de formación consideren la frecuencia de formación y los mecanismos de entrega de la formación.	a. Lista del personal que requiere formación	a. Resultados de la supervisión de habilidades y competencias
DSS04	Gestionar la continuidad	DSS04.08	Ejecutar revisiones post-reanudación.	N/A	a. Identificar debilidades u omisiones en el plan y las capacidades y hacer recomendaciones para la mejora. b. Obtener la aprobación de la dirección para los cambios en el plan y aplicarlos mediante el proceso de control de cambios de la empresa.	N/A	N/A
MEA01	Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad	MEA01.01	Establecer un enfoque de la supervisión.	N/A	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).	EDM05.01 •Principios de comunicación e informes •Evaluación de los requisitos de información de la organización EDM05.02 Reglas de validación y aprobación de los informes preceptivos EDM05.03 Evaluación de la efectividad de los informes	Requisitos de supervisión Interno Métricas y objetivos de supervisión aprobado. Interno

MEA01	Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad	MEA 01.02	Establecer los objetivos de cumplimiento y rendimiento.	N/A	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.	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
MEA01	Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad	MEA 01.02	Establecer los objetivos de cumplimiento y rendimiento.	N/A	4. Evaluar si los objetivos y métricas son adecuados, es decir, específicos, medibles, alcanzables, relevantes y limitados en el tiempo (SMART).	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
MEA01	Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad	MEA 01.05	Asegurar la implantación de medidas correctivas.	N/A	1. Revisar las respuestas, alternativas y recomendaciones de la dirección con el fin de tratar los problemas y desviaciones mayores.	EDM05.02 Directrices de escalado Acciones y asignaciones correctivas APO01.08 Acciones correctivas de incumplimientos	Acciones y asignaciones correctivas_Todo APO_Todo BAI_Todo DSS_Todo MEA Estado y resultado de las acciones_EDM01.03
MEA01	Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad	MEA 01.05	Asegurar la implantación de medidas correctivas.	N/A	2. Asegurar que se mantiene la asignación de responsabilidades en las acciones correctivas.	EDM05.02 Directrices de escalado Acciones y asignaciones correctivas APO01.08 Acciones correctivas de incumplimientos	Acciones y asignaciones correctivas_Todo APO_Todo BAI_Todo DSS_Todo MEA Estado y resultado de las acciones_EDM01.03
MEA01	Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad	MEA 01.05	Asegurar la implantación de medidas correctivas.	N/A	3. Hacer seguimiento de los resultados de las acciones comprometidas.	EDM05.02 Directrices de escalado Acciones y asignaciones correctivas APO01.08 Acciones correctivas de incumplimientos	Acciones y asignaciones correctivas Todo APO_Todo BAI_Todo DSS_Todo MEA Estado y resultado de las acciones_EDM01.03
MEA01	Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad	MEA 01.05	Asegurar la implantación de medidas correctivas.	N/A	4. Informar de los resultados a las partes interesadas.	EDM05.02 Directrices de escalado Acciones y asignaciones correctivas APO01.08 Acciones correctivas de incumplimientos	Acciones y asignaciones correctivas_Todo APO_Todo BAI_Todo DSS_Todo MEA Estado y resultado de las acciones_EDM01.03

MEA02	Supervisar, evaluar y valorar el sistema de control interno	MEA 02.03	Realizar autoevaluaciones de control.	N/A	a. 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. b. Determinar la frecuencia de las autoevaluaciones periódicas, considerando la efectividad y eficiencia conjuntas de la supervisión continua. c. Asignar la responsabilidad de la autoevaluación a las personas oportunas con el fin de asegurar la objetividad y la competencia. d. Proporcionar revisiones independientes para asegurar la objetividad de la autoevaluación y hacer posible compartir las buenas prácticas de control interno con otras compañías. e. Comparar los resultados de las autoevaluaciones con estándares y buenas prácticas de la industria. f. Resumir y comunicar los resultados de las autoevaluaciones y los estudios comparativos para considerar acciones correctivas.	N/A	a. Planes y criterios de autoevaluación b, Resultados de las autoevaluaciones c. Resultados de las revisiones de las autoevaluaciones
MEA02	Supervisar, evaluar y valorar el sistema de control interno	MEA 02.04	Identificar y comunicar las deficiencias de control.	N/A	a. Identificar, comunicar y registrar las excepciones de los controles y asignar responsabilidad de su resolución y comunicación de los resultados. b. Considerar el riesgo para la empresa al establecer umbrales para el escalado de las excepciones y desajustes de los controles. c. 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. d. 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. e. Hacer seguimiento de todas las excepciones para asegurar que se han contemplado las acciones acordadas. f. Identificar, iniciar, rastrear e implementar acciones correctivas que surjan de la evaluación de control e informes.	a. Causa raíz de los fallos relacionada con la calidad de la entrega b. a. Causa raíz de los fallos relacionada con el riesgo	a. Deficiencias de control b. Acciones correctivas
MEA02	Supervisar, evaluar y valorar el sistema de control interno	MEA 02.06	Planificar iniciativas de aseguramiento.	N/A	a, 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. b. 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.	a. Planes de auditorías de programas	a. Criterios de evaluación b. Evaluaciones de alto nivel
MEA02	Supervisar, evaluar y valorar el sistema de control interno	MEA 02.07	Estudiar las iniciativas de aseguramiento.	N/A	a. 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). b. Donde la efectividad del control no es aceptable, definir prácticas para identificar el riesgo residual (en preparación para los informes).	a. Informes de incidentes de incumplimiento y causas raíz.	a. Prácticas de revisión del aseguramiento
MEA02	Supervisar, evaluar y valorar el sistema de control interno	MEA 02.08	Ejecutar las iniciativas de aseguramiento.	N/A	a. Refinar el alcance de los objetivos de control clave en materia de aseguramiento de TI. b. Probar la efectividad del diseño de control de los objetivos clave de control. c. Documentar el impacto de las debilidades de control.	a. Análisis de riesgo e informes de perfil de riesgo para las partes interesadas	N/A

MEA03	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos	MEA 03.03	Confirmar el cumplimiento de requisitos externos.	Proceso	Evaluar regularmente las políticas, estándares, procedimientos y metodologías de la organización para todas las funciones corporativas con objeto de asegurar el cumplimiento de los requisitos legales y regulatorios aplicables al procesamiento de información. Gestionar las deficiencias de cumplimiento en las políticas, estándares y procedimientos dentro de plazos razonables.	Resultados auditorías de cumplimiento. Resultados auditoría de licencias	Deficiencias de cumplimiento identificadas. Confirmación de cumplimiento
EDM01	Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno	EDM 01.01	Evaluar el sistema de gobierno.	Proceso	Consideraciones regulaciones externas, obligaciones, factores del entorno externo e interno, procesamiento ético de la información. Cultura empresarial	Comunicaciones de los requerimientos de cumplimiento modificados, tendencia en el entorno del negocio, regulaciones, gobierno	Principios, directrices, niveles de autoridad
EDM02	Asegurar la Entrega de Beneficios	EDM 02.01	Evaluar la Optimización de valor	Proceso/05	Evaluar la efectividad de la integración y alineamiento de las estrategias de TI en la empresa y con los objetivos de la empresa para aportar valor.	Hoja de ruta estratégica	Evaluación de alineación estratégica
EDM02	Asegurar la Entrega de Beneficios	EDM 02.02	Orientar la Optimización de valor	Proceso	Recomendar la consideración de innovaciones potenciales, cambios organizativos o mejoras operativas que desde las iniciativas TI pudieran impulsar un incremento de valor para la empresa.	No posee entradas	Requerimientos para las revisiones de cambio de fase (stage-gate)
EDM02	Asegurar la Entrega de Beneficios	EDM 02.03	Supervisar la Optimización de valor	Proceso	3. Conseguir informes habituales y relevantes de la cartera, programa y desempeño de TI (tecnológico y funcional). Revisar el progreso de la empresa hacia los objetivos identificados y el grado en el que los objetivos previstos son alcanzados, los entregables obtenidos, los objetivos de rendimiento alcanzados y el riesgo mitigado.	Informes de rendimiento de la cartera de inversiones	Comentarios sobre el rendimiento de la cartera y del programa Acciones para mejorar la entrega de valor
EDM02	Asegurar la Entrega de Beneficios	EDM 02.03	Supervisar la Optimización de valor	Proceso	4. Tras la revisión de los informes, tomar las medidas de gestión apropiadas según sea necesario para asegurar que el valor sea optimizado.	Informes de rendimiento de la cartera de inversiones	Comentarios sobre el rendimiento de la cartera y del programa Acciones para mejorar la entrega de valor
EDM02	Asegurar la Entrega de Beneficios	EDM 02.03	Supervisar la Optimización de valor	Proceso	5. Tras la revisión de los informes, asegúrese de que las medidas correctivas apropiadas son iniciadas y controladas.	Informes de rendimiento de la cartera de inversiones	Comentarios sobre el rendimiento de la cartera y del programa Acciones para mejorar la entrega de valor
EDM02	Asegurar la Entrega de Beneficios	Genér ico	Realización de beneficios del portafolio de inversiones y servicios relacionados con las TI	TI/05	• Porcentaje de servicios TI en los que se realizan los beneficios esperados.	N/A	N/A

EDM03	Asegurar la Optimización del Riesgo	Genér ico	N/A	TI/04	Porcentaje de evaluaciones de riesgo de la empresa que incluyen los riesgos relacionados con TI	N/A	N/A
APO01	Gestionar el Marco de Gestion de TI	APO0 1.01	Definir la estructura organizativa.	Proceso	1. Desarrollar y mantener un entendimiento de las estrategias y objetivos del negocio, así como del entorno y los retos operativos actuales 2. Desarrollar y mantener un entendimiento del entorno externo a la empresa	Principios guía para la asignación de recursos y capacidades Oportunidades de innovación vinculadas con los motivadores de la industria Estrategia y análisis de las fortalezas, debilidades, oportunidades, amenazas de la empresa (DAFO)	Fuentes y prioridades para cambios
APO02	Gestionar la Estrategia	APO0 2.03	Definir el objetivo de las capacidades de TI	N/A	1. Considerar la aprobación de tecnologías emergentes e ideas innovadoras.	APO04.05 • Análisis de las iniciativas rechazadas • Resultados y recomendaciones de las iniciativas de pruebas de concepto.	Objetivos de TI a alto nivel Interno Requerimientos del negocio y capacidades de TI Interno Propuesta de cambio en la arquitectura del negocio APO03.03
APO02	Gestionar la Estrategia	APO0 2.04	Realizar un análisis de diferencias.	N/A	1. Identificar todas las diferencias y cambios necesarios para realizar en el entorno deseado.	EDM02.01 Evaluación de la alineación estratégica APO04.06 Evaluaciones sobre el uso de enfoques innovadores APO05.02 Expectativas sobre el retorno de inversión BAI01.05 Resultados del programa de supervisión de consecución de objetivos BAI01.06 Revisión de los resultados de cambios de fase (stage- gate) BAI01.13 Resultados de la revisión post-implementación	Diferencias y cambios requeridos para alcanzar la meta de capacidad_EDM04.01_APO13.0 2_BAI03.11 Declaración del valor beneficio para el entorno deseado_BAI03.11
APO02	Gestionar la Estrategia	APO0 2.05	Definir el plan estratégico y la hoja de ruta.	N/A	1. Definir las iniciativas necesarias para cerrar las diferencias y migrar del entorno actual al deseado, incluyendo el presupuesto de inversión/operativo, fuentes de financiación y estrategia de provisión.		
APO02	Gestionar la Estrategia	APO0 2.05	Definir el plan estratégico y la hoja de ruta.	N/A	4. Identificar los requerimientos de recursos, planificación y presupuestos de inversión/operacional de cada iniciativa.		

APO02	Gestionar la Estrategia	APO02.05	Definir el plan estratégico y la hoja de ruta.	N/A	7. Obtener formalmente soporte de las partes interesadas y obtener aprobación del plan.		
APO03	Gestionar la Arquitectura empresarial	APO03.02	Definir la arquitectura referencia	N/A	a. Finalizar la arquitectura de los dominios de negocio, información, datos, aplicaciones y tecnología y crear un documento de definición de la arquitectura.	a. Definición de la estructura de la organización y funciones b. Guía para la clasificación de los datos	a. Modelo de arquitectura de procesos b. Modelo de arquitectura de información
APO04	Gestionar la Innovación	APO04.01	Crear un entorno favorable para la innovación	Proceso	Crear un plan de innovación que incluya apetito por el riesgo, presupuesto para invertir, objetivos Proveer una infraestructura que permita innovar Programas que permita a los empleados presentar ideas innovadoras y crear una estructura adecuada de toma de decisiones	N/A	Plan de innovación y programa de reconocimiento y recompensa
APO04	Gestionar la Innovación	APO04.02	Mantener un entendimiento del entorno de la empresa	Proceso	Mantener una comprensión de los motores de negocio y de la industria Realizar reuniones periódicas con las unidades de negocio para entender los problemas actuales	Estrategia corporativa y análisis DAFO	Oportunidades de innovación vinculadas a los motivadores del negocio
APO04	Gestionar la Innovación	APO04.03	Supervisar y explorar el entorno tecnológico	Proceso	Comprender el interés de la empresa y su potencial para adoptar nuevas innovaciones. Consultar estudios y analizar el entorno exterior	Tecnologías emergentes	Análisis de investigación de posibilidades de innovación
APO04	Gestionar la Innovación	APO04.05	Recomendar iniciativas apropiadas adicionales	Proceso	Comunicar las oportunidades de innovación viables en la estrategia TI y en procesos de arquitectura	N/A	Resultados y recomendaciones de las pruebas de concepto Análisis de las iniciativas rechazadas
APO04	Gestionar la Innovación	APO04.06	Supervisar la implementación y el uso de la innovación	Proceso	Valorar la implementación de nuevas tecnologías o innovaciones TI adoptadas Capturar lecciones aprendidas y oportunidades de mejora	N/A	Valoración del uso de enfoques innovadores Evaluación de beneficios de la innovación Planes de innovación ajustados
APO05	Gestionar el Portafolio	APO05.01	Establecer la mezcla del objetivo de inversión.	Proceso	Validar que las inversiones TI y los servicios TI actuales están alineados con la visión y los principios corporativos, metas y objetivos estratégicos, visión de la arquitectura empresarial y prioridades. 2. Conseguir un entendimiento común entre TI y otras funciones de negocio sobre las potenciales oportunidades de TI para conducir y sustentar la estrategia corporativa.	Priorización y clasificación de las iniciativas TI	Identificar recursos y capacidades necesarias para soportar la estrategia
APO05	Gestionar el Portafolio	APO05.02	Determinar la disponibilidad y las fuentes de fondos	Proceso	Entender la disponibilidad y el compromiso de los fondos actuales, el gasto actual aprobado y la cantidad real gastada hasta la fecha. 2. Identificar las opciones para obtener financiación adicional para las inversiones TI internamente o de fuentes externas.	N/A	Opciones de financiación

APO05	Gestionar el Portafolio	APO05.04	Supervisar, optimizar e informar sobre el rendimiento del portafolio de inversiones	Proceso	8. Desarrollar métricas para medir la contribución de TI a la empresa, y establecer objetivos de rendimiento adecuados que reflejen las metas de capacidades corporativas y de TI. Utilizar asistencia de expertos externos y de datos de análisis comparativos para desarrollar métricas.	Evaluación de los beneficios de la innovación	Informes de rendimiento del portafolio de inversiones
APO05	Gestionar el Portafolio	APO05.05	Mantener los portafolios	Proceso	Trabajar con los responsables de entrega del servicio para mantener los portafolios de servicio y con los responsables de operaciones y arquitectos para mantener el portafolio de activos. Apoyar los planes tácticos y estratégicos de TI.	Comunicación de retiro del programa y responsabilidades en curso	Portafolios de programas, servicios y activos actualizados
APO05	Gestionar el Portafolio	APO05.06	Gestionar la consecución de beneficios.	Proceso	3. Considerar obtener orientación de expertos externos, líderes de la industria y datos de análisis comparativos para probar y mejorar las métricas y los objetivos	Presupuesto del programa y registro de beneficios Resultados de la supervisión de la realización de beneficios	Resultados de los beneficios y comunicaciones relacionadas Acciones correctivas para mejorar la producción de beneficio
BAI01	Gestión de Programas y Proyectos	BAI01.05	Lanzar y ejecutar el programa.	N/A	Administrar cada programa o proyecto para asegurar que la toma de decisiones y las actividades de entrega están enfocadas en el valor mediante la consecución de los beneficios y las metas del negocio de una manera consistente, considerando el riesgo y alcanzando los requerimientos de las partes interesadas.	BAI05.03 Comunicaciones de la visión	Resultados de la supervisión de la realización de beneficios APO05.06 APO06.05 Resultados de la supervisión del logro de metas del programa APO02.04 Planes de auditoría del programa MEA02.06
BAI02	Gestionar la definición de requisitos	BAI02.02	Realizar un estudio de viabilidad y proponer soluciones alternativas.	N/A	a. 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.	N/A	a. Informe de estudio de viabilidad
BAI02	Gestionar la definición de requisitos	BAI02.04	Obtener la aprobación de los requerimientos y soluciones.	N/A	a. 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.	Plan de gestión de la calidad	Aprobaciones de revisiones de calidad
BAI03	Gestionar la Identificación y Construcción de Soluciones	BAI03.01	Diseñar soluciones de alto nivel	Proceso	Crear un diseño acorde a los estándares de diseño de la organización, a un nivel de detalle que sea apropiado para la solución y el método de desarrollo y en consonancia con el negocio, empresa, estrategias TI, la arquitectura empresarial, el plan de seguridad, leyes aplicables, regulaciones y contratos.	Confirmar los criterios de aceptación por las partes interesadas Plan de alto nivel de adquisiciones/desarrollo	Aprobación de las especificaciones del diseño de alto nivel

BAI03	Gestionar la Identificación y Construcción de Soluciones	BAI03.02	Diseñar los componentes detallados de la solución	Proceso	Diseñar progresivamente las actividades del proceso de negocio y los flujos de trabajo necesarios para llevar a cabo conjuntamente con el nuevo sistema de aplicación para alcanzar los objetivos de la empresa, incluyendo el diseño de las actividades de control manuales. Diseñar las etapas de procesamiento de la aplicación, incluyendo especificaciones de tipos de transiciones y reglas de negocio	Confirmar los criterios de aceptación por parte de las partes interesadas Repositorio de definición de los requerimientos Informe de estudio de viabilidad	Especificaciones de diseño detalladas y aprobadas
BAI03	Gestionar la Identificación y Construcción de Soluciones	BAI03.03	Desarrollar los componentes de la solución	Proceso	Desarrollar procesos de negocio, servicios de soporte, aplicaciones e infraestructura y repositorios de información basados en las especificaciones acordadas y requerimientos técnicos, funcionales y de negocio. Registrar las peticiones de cambio y revisar el diseño, rendimiento y calidad, asegurando una participación activa de las partes interesadas afectadas.	Aprobaciones de los patrocinadores de los requerimientos y soluciones propuestas Informe de estudio de viabilidad	Documentar los componentes de la solución
BAI03	Gestionar la Identificación y Construcción de Soluciones	BAI03.04	Obtener los componentes de la solución	Proceso	Revisar y aprobar todos los planes de adquisiciones, considerando riesgos, costes, beneficios y conformidad técnica con los estándares de arquitectura empresarial. Realizar seguimiento de las aprobaciones requeridas en puntos de decisión clave durante los procesos de contratación.	Aprobación del patrocinador de los requerimientos y soluciones propuestas	Plan de adquisiciones aprobado Actualizaciones del inventario de activos
BAI03	Gestionar la Identificación y Construcción de Soluciones	BAI03.05	Construir soluciones	Proceso	Completar y actualizar cuando sea necesario el proceso de negocio y los manuales de operaciones para registrar cualquier personalización o condiciones especiales únicas en la implementación. Implementar pistas de auditoría durante la configuración e integración del hardware e infraestructura del software para proteger los recursos y asegurar la disponibilidad e integridad. Configurar que el software de aplicación adquirido cumple con los requerimientos de proceso de negocio.	N/A	Componentes de la solución integrados y configurados
BAI03	Gestionar la Identificación y Construcción de Soluciones	BAI03.06	Realizar controles de calidad	Proceso	Supervisar todas las excepciones de calidad y tratar todas las acciones correctivas. Mantener un registro con todas las revisiones, resultados, excepciones y correcciones. Repetir las evaluaciones de calidad cuando sea necesario, basándose en la cantidad de reelaboración (rework) y acciones correctivas.	Plan de gestión de calidad	Resultados de la revisión de calidad, excepciones y correcciones
BAI03	Gestionar la Identificación y Construcción de Soluciones	BAI03.07	Preparar pruebas de la solución	Proceso	Crear un plan de pruebas integradas y prácticas acordes al entorno de la empresa y planes estratégicos de tecnología que catalizarán la realización de pruebas apropiadas en entornos de simulación para ayudar a verificar que la solución estará operativa satisfactoriamente en el entorno real y entregar los resultados esperados y que los controles son adecuados.	N/A	Plan de pruebas. Procedimientos de pruebas
BAI03	Gestionar la Identificación y Construcción de Soluciones	BAI03.08	Ejecutar pruebas de la solución	Proceso	Realizar las pruebas de las soluciones y sus componentes en concordancia con el plan de pruebas. Incluir probadores independientes del equipo de la solución, con representación de los dueños de los procesos y usuarios finales del negocio. Asegurar que las pruebas son realizadas solo en los entornos de desarrollo y pruebas.	Análisis de las iniciativas rechazadas	Registros de resultados de pruebas y pistas de auditoría. Comunicaciones del resultado de las pruebas

BAI03	Gestionar la Identificación y Construcción de Soluciones	BAI03.09	Gestionar cambios a los requerimientos	Proceso	Hacer seguimiento de los requerimientos, facilitando a las partes interesadas la supervisión, revisión y aprobación de los cambios. Asegurar que los resultados de los procesos de cambio están completamente entendidos y están de acuerdo todos las partes interesadas y el patrocinador/ propietario del proceso de negocio.	Resultados y recomendaciones de las iniciativas de pruebas de concepto. Registro de peticiones de cambio de los requerimientos	Registro de todas las peticiones de cambio aprobadas y aplicadas
BAI03	Gestionar la Identificación y Construcción de Soluciones	BAI03.10	Mantener soluciones	Proceso	Desarrollar y ejecutar un plan para el mantenimiento de los componentes de la solución que incluya revisiones periódicas respecto a las necesidades de negocio y requerimientos operacionales tales como la gestión de parches, estrategias de actualización, riesgos, análisis de vulnerabilidades y requerimientos de seguridad.	N/A	Componentes de la solución actualizados y documentación relacionada. Plan de mantenimiento
BAI03	Gestionar la Identificación y Construcción de Soluciones	BAI03.11	Definir los servicios TI y mantener el catálogo de servicios	Proceso	Proponer cambios o nuevas opciones de niveles de servicios (franjas horarias del servicio, satisfacción del usuario, disponibilidad, rendimiento, capacidad, seguridad, continuidad, cumplimiento regulatorio, usabilidad) para asegurar que los servicios TI son adecuados para su uso. Documentar las opciones de niveles de servicio propuestas en el catálogo de servicios.	Directrices para la asignación de recursos y capacidades, valorar beneficios, asignaciones de presupuesto	Catálogo de servicios actualizado. Definiciones de servicio
BAI05	Gestionar la Facilitación del Cambio Organizativo	BAI05.02	Formar un equipo de implementación efectivo.	N/A	1. Identificar y montar un equipo de implementación principal efectivo que incluya miembros adecuados de TI y del negocio con la capacidad de invertir el tiempo necesario y contribuir con conocimiento, pericia, experiencia, credibilidad y autoridad. Considerar incluir a terceros externos, tales como consultores, para proveer una visión independiente o para abordar las brechas en habilidades. Identificar agentes de cambio potenciales dentro de las diferentes partes de la empresa con quienes el equipo principal pueda trabajar para que den soporte a la visión y los cambios vayan en cascada hacia abajo.	Criterios de aceptación confirmados por las partes interesadas (BAI02.01)	Equipo de implementación y roles BAI01.04 Visión y objetivos comunes BAI01.02
BAI06	Gestionar los cambios	BAI06.01	Evaluar, priorizar y autorizar peticiones de cambio.	N/A	a. Categorizar todas las peticiones de cambio (ej. procesos de negocio, infraestructura, sistemas operativos, redes, sistemas de aplicación, software externo adquirido) y relacionarlas con los elementos de configuración afectados.	a. Analisis de causas raíz y recomendaciones	a. Planes de cambio y programa b. Evaluaciones de impacto
BAI06	Gestionar los cambios	BAI06.03	Hacer seguimiento e informar de cambios de estado.	N/A	a. Categorizar las peticiones de cambio en el proceso de seguimiento (ej. rechazados, aprobados, pero aún no iniciados, aprobados y en proceso y cerrados).	a. Registro de todas las peticiones de cambio aprobadas	a. Reporte del estado de cambio de petición
BAI07	Gestionar la Aceptación del Cambio y la Transición	BAI07.03	Planificar pruebas de aceptación.	Proceso	Desarrollar y documentar el plan de pruebas, de forma que esté alineado con el programa y plan de calidad del proyecto y estándares relevantes de la organización. Comunicar y consultar con los propietarios de procesos de negocio y grupos de interés de TI adecuados.	Requisitos para la verificación independiente de los entregables Procedimientos de prueba Planes de prueba Comunicaciones de los resultados	Plan de pruebas de aceptación aprobado

BAI07	Gestionar la Aceptación del Cambio y la Transición	BAI07.07	Proporcionar soporte en producción desde el primer momento.	Proceso	Proporcionar recursos adicionales, según sea necesario, a los usuarios finales y al personal de soporte hasta que el lanzamiento sea estable.	Resultados de la revisión de calidad de servicio, incluyendo observaciones del cliente. métricas y resultados de éxito	Plan de soporte adicional
BAI08	Gestionar el Conocimiento	BAI04.05	Evaluar y retirar la información.	Proceso	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. 2. Definir las reglas para la retirada de conocimiento y retirar el mismo de forma acorde	N/A	Resultados de la evaluación de uso del conocimiento Interno Reglas para la retirada de conocimiento
BAI10	Gestionar la configuración	BAI10.01	Establecer y mantener un modelo de configuración.	N/A	a. Definir y acordar el alcance y nivel de detalle para la gestión de la configuración (p.ej., qué servicios, activos y elementos configurables de la infraestructura se incluyen).	N/A	a. Modelo de configuración lógica
BAI10	Gestionar la configuración	BAI10.02	Establecer y mantener un repositorio de configuración y una base de referencia.	N/A	a. Crear, revisar y formalizar un acuerdo sobre las bases de referencia de configuración de un servicio, aplicación o infraestructura.	a. Registro de licencias de software	a. Repositorio de configuración
BAI10	Gestionar la configuración	BAI10.03	Mantener y controlar los elementos de configuración.	N/A	a. Revisar los cambios propuestos a los elementos de configuración respecto a la base de referencia para garantizar su integridad y precisión.	a. Resultados de controles físicos b. Registro actualizado de activos	N/A
BAI10	Gestionar la configuración	BAI10.04	Generar informes de estado y configuración.	N/A	a. Enlazar todos los cambios de configuración con las peticiones de cambio aprobadas para identificar cualquier cambio no autorizado. Informar de cambios no autorizados a la gestión de cambios.	a. Resultados de los controles físicos de inventario	a. Informe de estado de configuración
BAI10	Gestionar la configuración	BAI10.05	Verificar y revisar la integridad del repositorio de configuración.	N/A	a. Verificar periódicamente que todos los elementos físicos de configuración, tal como se definen en el repositorio, existen físicamente. Informar de cualquier desviación a la Dirección.	N/A	a. Desviaciones de licencias
DSS01	Gestionar Operaciones	DSS01.01	Ejecutar procedimientos operativos	Proceso	Desarrollar y mantener procedimientos operativos y actividades relacionadas para dar apoyo a todos los servicios entregados.	Plan de operación y uso	Registro de copia de respaldo, programación operativa
DSS01	Gestionar Operaciones	DSS01.03	Supervisar la infraestructura de TI	Proceso	Registrar eventos, identificando el nivel de información a ser grabada sobre la base de una consideración del riesgo y el rendimiento. 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.	Definiciones de servicio	Reglas de monitorización de activos y condiciones de eventos. Registro de eventos

DSS02	Gestionar Peticiones e Incidentes de Servicio	DSS020.03	Verificar, aprobar y resolver peticiones de servicio.	Proceso	2. Obtener aprobación financiera y funcional o firmada, si se requiere, o aprobaciones predefinidas para cambios estándar acordados. 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	Causas raíz relacionadas con riesgos	Peticiones de servicio aprobadas Peticiones de servicio completas
DSS02	Gestionar Peticiones e Incidentes de Servicio	DSS020.07	Seguir el estado y emitir informes.	Proceso	Producir y distribuir informes en tiempo o proporcionar acceso controlado a datos online.	Informes de resolución de problemas	Informe de estado y tendencias de incidentes
DSS03	Gestionar Problemas	DSS03.01	Identificar y clasificar problemas.	N/A	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.	APO12.06 Causas raíz relacionadas con riesgos DSS02.01 Criterios para el registro de problemas DSS02.04 Registro de problemas	Esquema de clasificación de problemas DSS02.01 Informes de estado de problemas DSS02.07 Registro de problemas Interno
DSS03	Gestionar Problemas	DSS03.01	Identificar y clasificar problemas.	N/A	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).	APO12.06 Causas raíz relacionadas con riesgos DSS02.01 Criterios para el registro de problemas DSS02.04 Registro de problemas	Esquema de clasificación de problemas DSS02.01 Informes de estado de problemas DSS02.07 Registro de problemas Interno
DSS03	Gestionar Problemas	DSS03.05	Realizar una gestión de problemas proactiva.	N/A	5. Optimizar el uso de recursos y reducir las soluciones temporales y hacer seguimiento de las tendencias de problemas.	N/A	Registros de monitorización de resolución de problemas DSS02.07 Identificar soluciones sostenibles BAI06.01
DSS03	Gestionar Problemas	DSS03.05	Realizar una gestión de problemas proactiva.	N/A	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.	N/A	Registros de monitorización de resolución de problemas DSS02.07 Identificar soluciones sostenibles BAI06.01
MEA02	Supervisar, evaluar y valorar el sistema de control interno	MEA02.05	Garantizar que los proveedores de aseguramiento son independientes y están cualificados.	N/A	a. Establecer la independencia de los proveedores de aseguramiento. b. 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. c. 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.	N/A	N/A

MEA03	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos	MEA 03.04	Obtener garantía de cumplimiento de requisitos externos.	Proceso	Obtener confirmación regularmente del cumplimiento de las políticas internas por parte de los propietarios de procesos de TI y de negocio, así como de los directores de las unidades. Realizar revisiones regulares internas y externas (y, si procede, independientes) para evaluar los niveles de cumplimiento.	Reglas de validación y aprobación de informes obligatorios. Valoración de la efectividad de las evaluaciones.	Informe de garantía de cumplimiento. Informe de incidentes
EDM01	Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno	Genér ico	Alineamiento de TI y estrategia de negocio	TI	Nivel de satisfacción de las partes interesadas con el alcance del portafolio de programas y servicios planeados	N/A	N/A
EDM01	Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno	Genér ico	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	TI	Porcentaje de los roles de la gestión ejecutiva con responsabilidades claramente definidas para las decisiones de TI Ratio de ejecución de las decisiones ejecutivas relativas a TI	N/A	N/A
EDM01	Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno	Genér ico	Entrega de servicios de TI de acuerdo a los requisitos del negocio	TI	Número de interrupciones del negocio debidas a incidentes en el servicio de TI Porcentaje de usuarios satisfechos con la calidad de los servicios de TI entregados	N/A	N/A
EDM03	Asegurar la Optimización del Riesgo	Genér ico	N/A	TI/10	Número de incidentes de seguridad causantes de pérdidas financieras, interrupciones del negocio o pérdida de imagen pública	N/A	N/A
EDM03	Asegurar la Optimización del Riesgo	Genér ico	N/A	TI/10	Tiempo para otorgar, modificar y eliminar los privilegios de acceso, comparado con los niveles de servicio acordados	N/A	N/A
EDM03	Asegurar la Optimización del Riesgo	Genér ico	N/A	TI/15	Número de incidentes relacionados con el incumplimiento de la política	N/A	N/A
EDM03	Asegurar la Optimización del Riesgo	Genér ico	N/A	TI/15	Frecuencia de revisión y actualización de las políticas	N/A	N/A

EDM03	Asegurar la Optimización del Riesgo	Genérico	N/A	Proceso/01	Nivel de alineamiento entre riesgo TI y riesgo de negocio	N/A	N/A
EDM03	Asegurar la Optimización del Riesgo	Genérico	N/A	Proceso/01	Número de potenciales riesgos TI identificados y gestionados	N/A	N/A
EDM04	Asegurar la optimización de los Recursos	Genérico	Genérico	TI	• Número de procesos de negocio críticos soportados por infraestructuras y aplicaciones actualizadas • Frecuencia de evaluaciones de la madurez de la capacidad y de la optimización de costes • Porcentaje del personal cuyas habilidades TI son suficientes para las competencias requeridas para su función	N/A	N/A
EDM04	Asegurar la optimización de los Recursos	Genérico	Genérico	Procesos	• 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" • Número de desviaciones (y excepciones) de los principios de gestión de recursos • 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	N/A	N/A
EDM05	Asegurar la Transparencia de las partes interesadas	Genérico	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	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	N/A	N/A
EDM05	Asegurar la Transparencia de las partes interesadas	Genérico	Transparencia de los costes, beneficios y riesgos de las TI	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.	N/A	N/A
EDM05	Asegurar la Transparencia de las partes interesadas	Genérico	Entrega de servicios de TI de acuerdo a los requisitos del negocio	TI	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	N/A	N/A
APO01	Gestionar el Marco de Gestion de TI	Genérico	01 alineamiento de TI y estrategias de negocio	TI	• 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.	N/A	N/A

APO01	Gestionar el Marco de Gestion de TI	Genér ico	Entrega de servicios de TI de acuerdo a los requisitos del negocio	TI	• 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	N/A	N/A
APO02	Gestionar la Estrategia	Genér ico	N/A	TI/07	Porcentaje de usuarios satisfechos con la calidad de los servicios de TI entregados	N/A	N/A
APO02	Gestionar la Estrategia	Genér ico	N/A	TI/17	Número de iniciativas aprobadas resultantes de ideas innovadoras de TI	N/A	N/A
APO02	Gestionar la Estrategia	Genér ico	N/A	Proceso/01	Porcentaje de los objetivos del negocio considerados en la estrategia de TI	N/A	N/A
APO02	Gestionar la Estrategia	Genér ico	N/A	Proceso/02	Porcentaje de iniciativas en la estrategia de TI autofinanciadas (los beneficios superan los costes)	N/A	N/A
APO03	Gestionar la Arquitectura empresarial	Genér ico	Genérico	TI	a. Número de procesos de negocio críticos soportados por infraestructuras y aplicaciones actualizadas. b. Tiempo medio para convertir los objetivos estratégicos de TI en una iniciativa acordada y aprobada	N/A	N/A
APO03	Gestionar la Arquitectura empresarial	Genér ico	Genérico	Procesos	a. Beneficios aportados por el proyecto que pueden ser trazados a la implicación de la arquitectura (por ejemplo, reducción de costes debido a la reutilización) b. Número de deficiencias detectadas en los modelos a lo largo de los dominios de empresa, información, datos, aplicaciones y arquitectura de tecnología. c. Número de personas formadas en la metodología y en el manejo del conjunto de herramientas.	N/A	N/A
APO04	Gestionar la Innovación	Genér ico	Realización de beneficios del portafolio de inversiones y servicios relacionados con TI	TI	Porcentaje de servicios TI en los que se realizan los beneficios esperados.	N/A	N/A
APO04	Gestionar la Innovación	Genér ico	Uso adecuado de aplicaciones, información y soluciones tecnológicas	TI	Valor presente neto (NPV) mostrando el nivel de satisfacción del negocio con la calidad y utilidad de las soluciones tecnológicas	N/A	N/A

APO04	Gestionar la Innovación	Genérico	Agilidad de las TI	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	N/A	N/A
APO04	Gestionar la Innovación	Genérico	Optimización de activos, recursos y capacidades de las TI	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	N/A	N/A
APO04	Gestionar la Innovación	Genérico	Conocimiento, experiencia e iniciativas para la innovación de negocio	TI	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	N/A	N/A
APO05	Gestionar el Portafolio	Genérico	Alineamiento de TI y estrategia de negocio	TI	• 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	N/A	N/A
APO05	Gestionar el Portafolio	Genérico	5 realización de beneficios del portafolio de servicios y Servicios relacionados con TI	TI	Porcentaje de servicios TI en los que se realizan los beneficios esperados.	N/A	N/A
APO05	Gestionar el Portafolio	Genérico	Entrega de programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	TI	• Número de programas/proyectos ejecutados en plazo y en presupuesto • Porcentaje de partes interesadas satisfechas con la calidad del programa/proyecto • Coste del mantenimiento de aplicaciones respecto al coste total de TI	N/A	N/A
APO06	Gestionar el Presupuesto y los Costes	Genérico	N/A	TI/05	Porcentaje de servicios TI en los que se realizan los beneficios esperados.	N/A	N/A

APO06	Gestionar el Presupuesto y los Costes	Genérico	N/A	TI/05	Porcentaje de las inversiones en TI donde los beneficios demandados son alcanzados o excedidos.	N/A	N/A
APO06	Gestionar el Presupuesto y los Costes	Genérico	N/A	Proceso/04	Porcentaje de variación entre los presupuestos, previsiones y los costes reales	N/A	N/A
APO07	Gestionar los recursos humanos	Genérico	Genérico	TI	a. Frecuencia de evaluaciones de la madurez de la capacidad y de la optimización de costes b. Porcentaje del personal cuyas habilidades TI son suficientes para las competencias requeridas para su función	N/A	N/A
APO07	Gestionar los recursos humanos	Genérico	Genérico	Procesos	a. Duración media de las vacantes b. Porcentaje de puestos de TI vacantes	N/A	N/A
APO08	Gestionar las relaciones	Genérico	Alineamiento de TI y estrategia de negocio	TI	Nivel de satisfacción de las partes interesadas con el alcance del portafolio de programas y servicios planeados	N/A	N/A
APO08	Gestionar las relaciones	Genérico	Entrega de servicios TI de acuerdo a los requisitos del negocio	TI	Número de interrupciones del negocio debidas a incidentes en el servicio de TI, porcentaje de partes interesadas satisfechas con el cumplimiento y calidad del servicio	N/A	N/A
APO08	Gestionar las relaciones	Genérico	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	TI	Número de incidentes en los procesos debido a errores de integración tecnológica. Número de procesos de negocio habilitados por TI que se retrasen o incurran en un mayor coste	N/A	N/A
APO08	Gestionar las relaciones	Genérico	Conocimiento, experiencia e iniciativas para la innovación de negocio	TI	Nivel de concienciación y comprensión de las posibilidades de innovación	N/A	N/A

APO09	Gestionar los acuerdos de servicio	Genérico	Entrega de servicios de TI de acuerdo a los requisitos del negocio	TI	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	N/A	N/A
APO09	Gestionar los acuerdos de servicio	Genérico	Disponibilidad de información útil y relevante para la toma de decisiones	TI	• 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	N/A	N/A
APO10	Gestionar los Proveedores	Genérico	N/A	TI/04	Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos	N/A	N/A
APO10	Gestionar los Proveedores	Genérico	N/A	TI/04	Frecuencia de actualización del perfil de riesgo	N/A	N/A
APO10	Gestionar los Proveedores	Genérico	N/A	TI/09	Nivel de satisfacción de los ejecutivos de la empresa con la capacidad de respuesta de TI a nuevos requerimientos	N/A	N/A
APO10	Gestionar los Proveedores	Genérico	N/A	Proceso/01	Porcentaje de proveedores que cumplen con los requisitos acordados	N/A	N/A
APO10	Gestionar los Proveedores	Genérico	N/A	Proceso/01	Número de infracciones de servicio causadas por los proveedores	N/A	N/A
APO10	Gestionar los Proveedores	Genérico	N/A	Proceso/03	Numero de reuniones de revisión con proveedores	N/A	N/A
APO11	Gestionar la calidad	Genérico	Genérico	TI	a. Número de interrupciones del negocio debidas a incidentes en el servicio de TI b. Número de programas/proyectos ejecutados en plazo y en presupuesto c. Número de programas que necesitan ser revisados significativamente debido a defectos de calidad d. Coste del mantenimiento de aplicaciones respecto al coste total de TI	N/A	N/A
APO11	Gestionar la calidad	Genérico	Genérico	Procesos	a. Porcentaje de proyectos revisados que cumplen con las metas y objetivos de calidad b. Número de procesos con un informe de evaluación formal de la calidad	N/A	N/A
APO12	Gestionar el riesgo	Genérico	Cumplimiento y soporte de las TI al cumplimiento del negocio de las leyes y regulaciones externas	TI	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	N/A	N/A

APO12	Gestionar el riesgo	Genérico	Riesgos de negocio relacionados con las TI gestionados	TI	Frecuencia de actualización del perfil de riesgo. Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos	N/A	N/A
APO12	Gestionar el riesgo	Genérico	Transparencia de los costes, beneficios y riesgo de las TI	TI	Porcentaje de inversión en casos de negocio con costes y beneficios esperados relativos a TI claramente definidos y aprobados. Encuestas de satisfacción	N/A	N/A
APO12	Gestionar el riesgo	Genérico	Seguridad de la información, infraestructura de procesamiento y aplicaciones	TI	Número de incidentes de seguridad causantes de pérdidas financieras, interrupciones del negocio o pérdida de imagen pública. Frecuencia de la evaluación de seguridad frente a los últimos estándares y guías	N/A	N/A
APO12	Gestionar el riesgo	Genérico	Entrega de programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	TI	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	N/A	N/A
APO013	Gestionar la Seguridad	Genérico	Disponibilidad de información útil y relevante para la toma de decisiones	TI	• 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	N/A	N/A
APO013	Gestionar la Seguridad	Genérico	Riesgos de negocio relacionados con las TI gestionados	TI	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	N/A	N/A

APO013	Gestionar la Seguridad	Genérico	Transparencia de los costes, beneficios y riesgo de las TI	TI	Porcentaje de servicios de TI que tienen claramente definidos y aprobados los costes operacionales y los beneficios esperados	N/A	N/A
APO013	Gestionar la Seguridad	Genérico	Seguridad de la información, infraestructura de procesamiento y aplicaciones	TI	• 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 • Frecuencia de la evaluación de seguridad frente a los últimos estándares y guías	N/A	N/A
APO013	Gestionar la Seguridad	Genérico	Disponibilidad de información útil y relevante para la toma de decisiones	TI	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	N/A	N/A
BAI01	Gestión de Programas y Proyectos	Genérico	N/A	TI/01	Porcentaje de las metas y requerimientos estratégicos de la empresa soportados por las metas estratégicas para TI	N/A	N/A
BAI01	Gestión de Programas y Proyectos	Genérico	N/A	TI/04	Frecuencia de actualización del perfil de riesgo	N/A	N/A
BAI02	Gestionar la definición de requisitos	Genérico	Genérico	TI	• 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	N/A	N/A
BAI02	Gestionar la definición de requisitos	Genérico	Genérico	Procesos	• Números de incidentes no identificados como riesgo • Porcentaje de riesgos no mitigado exitosamente	N/A	N/A
BAI03	Gestionar la Identificación y Construcción de Soluciones	Genérico	Entrega de servicios de TI de acuerdo a los requisitos del negocio	TI	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	N/A	N/A

BAI04	Gestionar la Disponibilidad y la Capacidad	Genér ico	Entrega de servicios de TI de acuerdo a los requisitos del negocio	TI	• 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	N/A	N/A
BAI04	Gestionar la Disponibilidad y la Capacidad	Genér ico	Optimización de activos, recursos y capacidades de TI	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 T	N/A	N/A
BAI04	Gestionar la Disponibilidad y la Capacidad	Genér ico	Disponibilidad de información útil y relevante para la toma de decisiones	TI	• 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	N/A	N/A
BAI05	Gestionar la Facilitación del Cambio Organizativo	Genér ico	N/A	TI/08	Nivel de comprensión de los usuarios de negocio sobre cómo las soluciones tecnológicas soportan sus procesos	N/A	N/A
BAI05	Gestionar la Facilitación del Cambio Organizativo	Genér ico	N/A	TI/13	Número de programas/proyectos ejecutados en plazo y en presupuesto	N/A	N/A
BAI05	Gestionar la Facilitación del Cambio Organizativo	Genér ico	N/A	TI/13	Porcentaje de partes interesadas satisfechas con la calidad del programa/proyecto	N/A	N/A
BAI05	Gestionar la Facilitación del Cambio Organizativo	Genér ico	N/A	TI/13	Número de programas que necesitan ser revisados significativamente debido a defectos de calidad	N/A	N/A

BAI05	Gestionar la Facilitación del Cambio Organizativo	Genérico	N/A	Proceso/02	Numero de habilidades identificadas o cuestiones de capacidad (El equipo de implementación es competente y está habilitado para conducir el cambio.)	N/A	N/A
BAI05	Gestionar la Facilitación del Cambio Organizativo	Genérico	N/A	Proceso/06	Porcentaje de usuarios adecuadamente formados en el cambio	N/A	N/A
BAI06	Gestionar los cambios	Genérico	Genérico	TI	• Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos • Frecuencia de actualización del perfil de riesgo	N/A	N
BAI06	Gestionar los cambios	Genérico	Genérico	Procesos	• Cantidad de trabajo rehecho debido a cambios fallidos	N/A	N
BAI07	Gestionar la Aceptación del Cambio y la Transición	Genérico	Uso adecuado de aplicaciones, información y soluciones tecnológicas	TI	Porcentaje de propietarios de procesos de negocio satisfechos con los productos y servicios TI que dan soporte a estos procesos Nivel de comprensión de los usuarios de negocio sobre cómo las soluciones tecnológicas soportan sus procesos	N/A	N/A
BAI07	Gestionar la Aceptación del Cambio y la Transición	Genérico	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	TI	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	N/A	N/A
BAI08	Gestionar el Conocimiento	Genérico	Agilidad de las TI	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 aprobado	N/A	N/A
BAI08	Gestionar el Conocimiento	Genérico	Agilidad de las TI	TI	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	N/A	N/A

BAI09	Gestionar los Activos	Genérico	N/A	TI/06	Porcentaje de servicios TI con costes operativos y beneficios esperados claramente definidos y aprobados.	N/A	N/A
BAI09	Gestionar los Activos	Genérico	N/A	TI/11	Frecuencia de evaluaciones de la madurez de la capacidad y de la optimización de costes	N/A	N/A
BAI09	Gestionar los Activos	Genérico	N/A	Proceso/01	Porcentaje de licencias usadas respecto a licencias pagadas	N/A	N/A
BAI09	Gestionar los Activos	Genérico	N/A	Proceso/02	Número de activos no utilizados	N/A	N/A
BAI09	Gestionar los Activos	Genérico	N/A	Proceso/02	Número de activos obsoletos	N/A	N/A
BAI10	Gestionar la configuración	Genérico	Genérico	TI	• 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 • Frecuencia de evaluaciones de la madurez de la capacidad y de la optimización de costes	N/A	N/A
BAI10	Gestionar la configuración	Genérico	Genérico	Procesos	• Número de desviaciones ente el repositorio de configuración y la configuración real.	N/A	N/A
DSS01	Gestionar Operaciones	Genérico	Riesgos de negocio relacionados con las TI gestionados	TI	Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos	N/A	N/A
DSS01	Gestionar Operaciones	Genérico	Entrega de servicios de TI de acuerdo a los requisitos del negocio	TI	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	N/A	N/A
DSS01	Gestionar Operaciones	Genérico	Optimización de activos recursos y capacidades de TI	TI	Frecuencia de evaluaciones de la madurez de la capacidad y de la optimización de costes	N/A	N/A

DSS02	Gestionar Peticiones e Incidentes de Servicio	Genér ico	Riesgos de negocio relacionados con las TI gestionados	TI	• Porcentaje de procesos de negocio críticos, servicios TI y programas de negocios habilitados por las TI cubiertos por evaluaciones de riesgos • Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos • Porcentaje de evaluaciones de riesgo de la empresa que incluyen los riesgos relacionados con TI • Frecuencia de actualización del perfil de riesgo	N/A	N/A
DSS02	Gestionar Peticiones e Incidentes de Servicio	Genér ico	Entrega de servicios de TI de acuerdo a los requisitos del negocio	TI	• Número de interrupciones del negocio debidas a incidentes en el servicio de TI	N/A	N/A
DSS03	Gestionar Problemas	Genér ico	N/A	TI/04	Porcentaje de procesos de negocio críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos	N/A	N/A
DSS03	Gestionar Problemas	Genér ico	N/A	TI/04	Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos	N/A	N/A
DSS03	Gestionar Problemas	Genér ico	N/A	TI/04	Porcentaje de evaluaciones de riesgo de la empresa que incluyen los riesgos relacionados con TI	N/A	N/A
DSS03	Gestionar Problemas	Genér ico	N/A	TI/04	Frecuencia de actualización del perfil de riesgo	N/A	N/A
DSS03	Gestionar Problemas	Genér ico	N/A	TI/07	Número de interrupciones del negocio debidas a incidentes en el servicio de TI	N/A	N/A
DSS03	Gestionar Problemas	Genér ico	N/A	TI/07	Porcentaje de usuarios satisfechos con la calidad de los servicios de TI entregados	N/A	N/A
DSS03	Gestionar Problemas	Genér ico	N/A	TI/11	Frecuencia de evaluaciones de la madurez de la capacidad y de la optimización de costes	N/A	N/A
DSS03	Gestionar Problemas	Genér ico	N/A	TI/14	Relación o cantidad de decisiones de negocio erróneas en las que la falta de información o la información errónea ha sido la principal causa	N/A	N/A
DSS03	Gestionar Problemas	Genér ico	N/A	Proceso/01	Descenso del número de incidentes recurrentes causados por problemas no resueltos	N/A	N/A
DSS03	Gestionar Problemas	Genér ico	N/A	Proceso/01	Número de problemas para los que se ha encontrado una solución satisfactoria que apunta a causas raíz	N/A	N/A

DSS04	Gestionar la continuidad	Genérico	Genérico	TI	• Porcentaje de procesos de negocio críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos • Porcentaje de evaluaciones de riesgo de la empresa que incluyen los riesgos relacionados con TI • Frecuencia de actualización del perfil de riesgo • Nivel de satisfacción de los usuarios del negocio y puntualidad (o disponibilidad) de la información de gestión • Relación o cantidad de decisiones de negocio erróneas en las que la falta de información o la información errónea ha sido la principal causa	N/A	N/A
DSS04	Gestionar la continuidad	Genérico	Genérico	Procesos	• Porcentaje de restauraciones satisfactorias y en tiempo de copias alternativas o de respaldo	N/A	N/A
DSS05	Asegurar la Transparencia de las partes interesadas	Genérico	Cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externas	TI	Coste y número de problemas de la no conformidad de TI, incluidos arreglos y multas, e impacto de la pérdida de reputación	N/A	N/A
DSS05	Asegurar la Transparencia de las partes interesadas	Genérico	Riesgos de negocio relacionados con las TI gestionados	TI	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	N/A	N/A
DSS05	Asegurar la Transparencia de las partes interesadas	Genérico	Seguridad de la información, infraestructura de procesamiento y aplicaciones	TI	Número de incidentes de seguridad causantes de pérdidas financieras, interrupciones del negocio o pérdida de imagen pública	N/A	N/A
DSS06	Gestionar Controles de Proceso de Negocio	Genérico	04 riesgos de negocio relacionados con las TI gestionados	TI	Porcentaje de evaluaciones de riesgo de la empresa que incluyen los riesgos relacionados con TI Frecuencia de actualización del perfil de riesgo	N/A	N/A
DSS06	Gestionar Controles de Proceso de Negocio	Genérico	07 entrega de servicios TI de acuerdo a los requisitos del negocio	TI	Número de interrupciones del negocio debidas a incidentes en el servicio de TI	N/A	N/A

MEA01	Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad	Genér ico	N/A	TI/04	Porcentaje de procesos de negocio críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos	N/A	N/A
MEA01	Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad	Genér ico	N/A	TI/04	Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos	N/A	N/A
MEA01	Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad	Genér	N/A	TI/04	Porcentaje de evaluaciones de riesgo de la empresa que incluyen los riesgos relacionados con TI	N/A	N/A
MEA01	Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad	Genér ico	N/A	TI/04	Frecuencia de actualización del perfil de riesgo	N/A	N/A
MEA01	Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad	Genér ico	N/A	TI/07	Número de interrupciones del negocio debidas a incidentes en el servicio de TI	N/A	N/A
MEA01	Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad	Genér ico	N/A	TI/07	Porcentaje de usuarios satisfechos con la calidad de los servicios de TI entregados	N/A	N/A
MEA01	Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad	Genér ico	N/A	TI/11	Frecuencia de evaluaciones de la madurez de la capacidad y de la optimización de costes	N/A	N/A
MEA01	Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad	Genér ico	N/A	TI/15	Número de incidentes relacionados con el incumplimiento de la política	N/A	N/A
MEA01	Supervisar, Evaluar y Valorar el	Genér ico	N/A	TI/15	Frecuencia de revisión y actualización de las políticas	N/A	N/A

	Rendimiento y la Conformidad						
MEA01	Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad	Genérico	N/A	Proceso/02	Porcentaje de procesos con objetivos y métricas definidas.	N/A	N/A
MEA01	Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad	Genérico	N/A	Proceso/03	Porcentaje de procesos con efectividad de objetivos y métricas revisadas y mejoradas	N/A	N/A
MEA02	Supervisar, evaluar y valorar el sistema de control interno	Genérico	Genérico	TI	• Coste de la no conformidad de TI, incluidos arreglos y multas, e impacto de la pérdida de reputación	N/A	N/A
MEA02	Supervisar, evaluar y valorar el sistema de control interno	Genérico	Genérico	Procesos	• Porcentaje de procesos con la seguridad de que las salidas cumplen el objetivo dentro de los márgenes de tolerancia • Porcentaje de procesos bajo revisión independiente • 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	N/A	N/A
MEA03	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos	Genérico	Cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externas	TI	Coste y número de problemas de la no conformidad de TI, incluidos arreglos y multas, e impacto de la pérdida de reputación	N/A	N/A
MEA03	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos	Genérico	Riesgos del negocio relacionados con las TI gestionados	TI	Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos	N/A	N/A

Anexo H.

Homologación componentes de control interno COSO 2013 y los principios de COBIT 5

COBIT/PRNCIPIOS COSO				Entorno de Control					Valoración del Riesgo				Actividades de Control			Información y Comunicación			Supervisión del sistema de control – Monitoreo	
				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
				1.1 La organización demuestra compromiso con la integridad y los valores éticos	1.2 El consejo de administración demuestra independencia de la dirección y ejerce la supervisión del desempeño del sistema de control interno.	1.3 La dirección establece con la supervisión del Consejo, las estructuras, líneas de reporte y los niveles de autoridad y responsabilidad apropiados para la consecución de los objetivos.	1.4 La organización demuestra compromiso para atraer, desarrollar y retener a profesionales competentes, en concordancia con los objetivos de la organización	1.5 La organización define las responsabilidades de las personas a nivel de control interno para la consecución de los objetivos	2.1 La organización define los objetivos con suficiente claridad para permitir la identificación y evaluación de los riesgos relacionados	2.2 La organización identifica los riesgos para la consecución de sus objetivos en todos los niveles de la entidad y los analiza como base sobre la cual determina cómo se deben gestiona	2.3 La organización considera la probabilidad de fraude al evaluar los riesgos para la consecución de los objetivos	2.4 La organización identifica y evalúa los cambios que podrían afectar significativamente al sistema de control interno	3.1 La organización define y desarrolla actividades de control que contribuyen a la mitigación de los riesgos hasta niveles aceptables para la consecución de los objetivos	3.2 La organización define y desarrolla actividades de control a nivel de entidad sobre la tecnología para apoyar la consecución de los objetivos	3.3 La organización despliega las actividades de control a través de políticas que establecen las líneas generales del control interno y procedimientos.	4.1 La organización obtiene o genera y utiliza información relevante y de calidad para apoyar el funcionamiento del control interno.	4.2 La organización comunica la información internamente, incluidos los objetivos y responsabilidades que son necesarios para apoyar el funcionamiento del sistema de control interno	4.3 La organización se comunica con los grupos de interés externos sobre los aspectos clave que afectan al funcionamiento del control interno.	5.1 La organización selecciona, desarrolla y realiza evaluaciones continuas y/o independientes para determinar si los componentes del sistema están presentes y funcionando.	5.2 La organización evalúa y comunica las deficiencias de control interno de forma oportuna a las partes responsables de aplicar medidas correctivas, incluyendo la alta dirección y el consejo, según corresponda.
	ED M02	EDM 02.01	**Asegurar la entrega de beneficios**			**S**			**S**					**S**		**S**	**P**			
		EDM 02.02					**S**										**P**			
		EDM 02.03							**S**							**P**				**S**
	ED M03	EDM 03.01	**Asegurar la Optimiza**							**P**				**S**						
		EDM 03.02				**S**			**S**				**P**		**S**		**S**			

		EDM 03.03	**ción del Riesgo**													**P**			**S**
	ED M04	EDM 04.01	**Asegurar la Optimización de los Recursos**												**P**		**S**		
		EDM 04.02						**S**									**P**			
		EDM 04.03																		**P**
	ED M05	EDM 05.01	**Asegurar la Transparencia hacia las Partes Interesadas**													**P**	**S**	**S**		
		EDM 05.02														**S**	**P**	**S**		
		EDM 05.03														**S**	**P**	**S**	**S**	**S**
Alinear, Planificar y Organizar	AP O01	APO0 1.03	**Gestionar el marco de gestión de TI**	**P**		**S**	**S**										**S**			
		APO0 1.04		**S**	**S**	**S**	**S**	**S**									**P**			
		APO0 1.06											**S**	**S**	**P**					
		APO0 1.07											**S**	**S**	**P**					
		APO0 1.08													**S**					**P**
	AP O02	APO0 2.01	**Gestionar la Estrategia**						**S**	**P**	**S**	**S**								
		APO0 2.02							**S**	**P**	**S**	**S**								
	AP O03	APO0 3.01	**Administrar la Arquitectura**						**S**	**P**		**S**								
		APO0 3.03								**P**										

		APO03.04	**Empresarial**											**S**	**P**				
		APO03.05												**S**	**P**				
	APO08	APO08.02	**Gestionar las relaciones**									**S**				**P**		**S**	
		APO08.04				**S**										**S**	**P**		
	APO10	APO10.01	**Gestionar los proveedores**																**P**
		APO10.02													**P**				
		APO10.03														**S**		**P**	
		APO10.04							**P**						**S**				
	APO12	APO12.01	**Gestionar el Riesgo**							**P**						**S**			
		APO12.02								**P**						**S**			
		APO12.03								**P**									
		APO12.04								**P**							**S**	**S**	**S**
		APO12.05													**P**				
		APO12.06													**P**				
	APO13	APO13.01	**Gestionar la seguridad**			**S**										**P**	**S**	**S**	
		APO13.02												**P**					

		APO13.03														P			S
3.1	BAI02	BAI02.01	**Gestionar la definición de requisitos**													P	S	S		
		BAI02.03							S							P				
	BAI04	BAI04.01	**Gestionar la disponibilidad y la capacidad**						S	P										
		BAI04.02								P										
		BAI04.05														P				
		BAI04.06														P				
	BAI07	BAI07.01	**Gestionar la aceptación de Cambio**																S	P
		BAI07.04										P	S	S						
		BAI07.05										P	S	S						
	BAI08	BAI08.01	**Gestionar el conocimiento**			S	P	S				S	S	S					S	
		BAI08.03											S		P		S			
	BAI09	BAI09.01	**Gestionar los activos**									S	P	S						
		BAI09.02										P							S	S
		BAI09.03										P	S	S						
Entregar, dar	DSS02	DSS02.01	**Gestionar Peticiones**											S			P			

Servicio y Soporte		DSS02.06	**e Incidentes de Servicio**																**P**
	DSS04	DSS04.01	**Gestionar la Continuidad**											**P**	**S**				
		DSS04.02							**S**	**P**		**S**							
		DSS04.03													**P**	**S**	**S**	**S**		
		DSS04.04							**P**											
		DSS04.05													**S**					**P**
		DSS04.07												**P**	**S**					
	DSS05	DSS05.01	**Gestionar Servicios de Seguridad**											**S**	**S**		**P**			
		DSS05.02												**S**	**S**		**P**			
		DSS05.03												**P**						
		DSS05.04												**P**						
		DSS05.05												**P**						
		DSS05.06											**S**	**S**	**S**					**P**
		DSS05.07																**S**		**P**
	DSS06	DSS06.01	**Gestionar controles**										**S**	**S**	**P**					

		DSS06.02	**de proceso de negocios**										**S**		**P**				**S**
		DSS06.03				**S**								**P**					
		DSS06.04														**S**			**P**
		DSS06.05											**S**		**P**				
		DSS06.06												**P**					
Supervisar, Evaluar y Valorar	ME A02	MEA02.01	**Supervisar, evaluar y valorar el sistema de control interno**										**S**	**S**	**S**				**P**
		MEA02.02						**S**				**P**			**S**				**S**
	ME A03	MEA03.01											**P**						
		MEA03.02											**P**					**S**	

Anexo I.

Actividad realizada con el personal de CODEA 05 de noviembre de 2021

1

¿Quiénes somos?

01 Daniela Arrieta Arrieta
Contraloría General de la República
8779-7318
danarrietaa@gmail.com

02 Marilyn Castro Quesada
Grant Thornton
8610-6813
marilyn.castroque96@gmail.com

04 Jesús Murillo Vargas
KPMG
7023-7053
jemuva2014@gmail.com

03 Yerlin Navarro Brenes
BAC LATAM
8318-7959
yerlinnb19@gmail.com

2

AGENDA

01 Presentación
02 Objetivo de la reunión
03 Control Interno (Ley de CI)
04 ¿Qué es COSO?
05 ¿Qué es COBIT?
06 Metodología de trabajo
07 Aplicación cuestionario

3

Objetivo de la reunión

01 Conocernos
02 ¿Qué es lo que vamos a hacer?
03 ¿Por qué CODEA?
04 Alinearnos
05 Aspectos relevantes
06 Iniciar trabajo de campo

4

Control Interno

El control interno consta de una serie de acciones que dan acompañamiento de forma continua a las diferentes actividades de la entidad.

Ley General de Control Interno N. 8292 ley busca establecer los criterios mínimos de control interno, que deben implementar las diferentes instituciones públicas en Costa Rica.

5

Marcos internacionales de buenas prácticas que ayudan y orientan a cualquier entidad a fortalecer sus sistemas de control interno.

Marcos a utilizar:

- COSO 2013
- COBIT 5

6

COSO 2013 : Marco de referencia para la implementación, gestión y control de un adecuado Sistema de Control Interno

01 COSO

Comité de Organizaciones Patrocinadoras de la Comisión Treadway (COSO, por sus siglas en inglés.

02 ¿Qué hacen?

Es una comisión voluntaria que se encarga de desarrollar las **mejores prácticas** en temas de fraude, gestión de riesgo empresarial y el control interno.

03 Objetivo de COSO

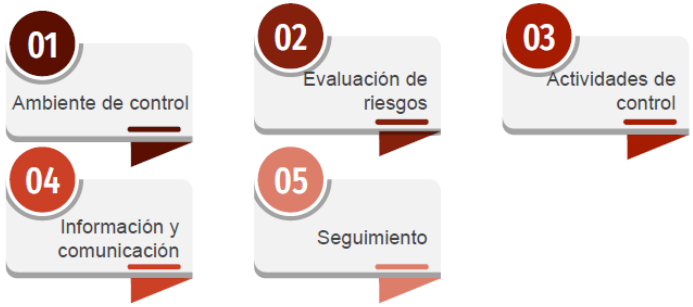
Proporcionar liderazgo intelectual a través del desarrollo de marcos generales y orientaciones sobre la Gestión del Riesgo, Control Interno y Disuasión del Fraude, diseñado para mejorar el desempeño organizacional y reducir el alcance del fraude en las organizaciones.

04 Composición

5 componentes de control y 17 principios

7

Componentes de COSO:



8

COBIT 5

"...un marco de referencia de Gobierno de TI y un conjunto de herramientas de soporte que permite a los gerentes reducir la brecha entre los requerimientos de control, los temas técnicos y los riesgos del negocio. Además, permite el desarrollo de una política clara y una buena práctica para el control de TI en las organizaciones". (Saavedra & Torres,2012, p.25)

Procesos de Gobierno y de Gestión de TI Empresarial

10

Recolección de datos

Al realizar la homologación de los dos marcos anteriores, se procede a realizar las siguientes actividades:

11

Aplicación de cuestionario

12

Anexo J.

Preguntas realizadas al personal del CODEA para la evaluación de los riesgos

COSO	COSO - S1	COSO - S2	COSO - S3	COSO - S4	COSO - S5	COSO - S6	COBIT	COBIT - S	Orden	Pregunta	Nota
1.1	1.3	1.4	4.2				APO01	APO01.03	1	¿Existe un código de ética documentado?	0,00%
1.1	1.3	1.4	4.2				APO01	APO01.03	2	Si la respuesta anterior fue sí, conteste lo siguiente ¿El Código de ética ha sido difundido y explicado internamente?	0,00%
1.1	1.3	1.4	4.2				APO01	APO01.03	3	¿El CODEA ha exigido la aceptación formal del Código de Ética por parte de todos los empleados sin distinción de jerarquías?	0,00%
1.1	1.3	1.4	4.2				APO01	APO01.03	4	Si la respuesta de la pregunta 1 fue no, ¿Toman medidas para que el personal demuestre y mantenga buenos valores?	33,33%
1.1	1.3	1.4	4.2				APO01	APO01.03	5	¿Presentan buenas prácticas en cuanto a la contratación, entrenamiento, evaluación y cuando se deben tomar acciones disciplinarias en el personal?	55,56%
1.1	1.3	1.4	4.2				APO01	APO01.03	6	¿Conoce la estructura organizacional del CODEA?	100,00%
1.1	1.3	1.4	4.2				APO01	APO01.03	7	¿La dirección del CODEA propicia una cultura organizacional con énfasis en la integridad y el comportamiento ético?	77,78%
1.1	1.3	1.4	4.2				APO01	APO01.03	8	¿Se investigan y documentan las posibles faltas a la Ética?	44,44%
1.1	1.3	1.4	4.2				APO01	APO01.03	9	¿Se sancionan los comportamientos contrarios a la Ética?	77,78%

1.1	1.3	1.4	4.2				APO01	APO01.03	10	¿Se comunican a lo interno de la entidad las acciones disciplinarias que se toman sobre vulneraciones al Código de Ética?	44,44%
1.1	1.3	1.4	4.2				APO01	APO01.03	11	¿Los objetivos estratégicos son consistentes con la misión de la entidad?	88,89%
1.1	1.3	1.4	4.2				APO01	APO01.03	12	¿Existen líneas de reporte que permitan realizar comunicaciones anónimas por parte de los funcionarios de CODEA?	0,00%
1.4							BAI04	BAI04.05	13	¿Se cuenta con cronogramas para la capacitación del personal en diversas temáticas?	11,11%
1.4	1.3	1.5	3.1	3.2	3.3	5.1	BAI08	BAI08.01	14	¿Se tiene la cultura de compartir y transferir conocimiento? (Ejemplo: Capacitaciones entre los mismos funcionarios)	11,11%
1.4	1.3	1.5	3.1	3.2	3.3	5.1	BAI08	BAI08.01	15	¿En caso de que se presente una ausencia de personal para puestos relevantes existe algún registro de funcionarios que se encuentren en capacidad de solventar dicha ausencia?	55,56%
1.4	1.3	1.5	3.1	3.2	3.3	5.1	BAI08	BAI08.01	16	¿Existe un Manual de Puestos definido y documentado?	0,00%
1.4	1.3	1.5	3.1	3.2	3.3	5.1	BAI08	BAI08.01	17	¿Se tiene políticas de RR. HH definidas y al alcance? (ascensos, vacaciones, despidos, contrataciones)	11,11%
1.4	1.3	1.5	3.1	3.2	3.3	5.1	BAI08	BAI08.01	18	¿Se realizan revisiones y actualizaciones (cuando lo requiera) de la descripción del puesto?	44,44%
1.4	1.3	1.5	3.1	3.2	3.3	5.1	BAI08	BAI08.01	19	¿Se realizan revisiones y actualizaciones (cuando lo requiera) de las políticas de Recursos Humanos?	22,22%
1.2							APO01	N/I	20	¿La junta directiva supervisa el funcionamiento del control interno?	55,56%

1.4	1.3	1.5	3.1	3.2	3.3	5.1	BAI08	BAI08.01	21	¿Las expectativas de desempeño definidas y medibles se reflejan en las revisiones de los empleados?	77,78%
2.2	2.1	2.3	2.4				APO02	APO02.01	1	¿El CODEA realiza un proceso de identificación de riesgos?	25,00%
2.2	2.1	2.3	2.4				APO02	APO02.01	2	¿Se utiliza SEVRI para la identificación de riesgos?	0,00%
2.2	2.1	2.3	2.4				APO02	APO02.01	9	¿Se tiene identificadas las partes interesadas de CODEA?	50,00%
2.2	2.1	2.3	2.4				APO02	APO02.02	4	¿Se identifican las fortalezas, oportunidades, debilidades y amenazas en el entorno actual y su impacto en el logro de los objetivos del CODEA?	0,00%
2.2	3.3						APO10	APO10.04	14	¿Se identifican y se gestionan los riesgos relacionados con la capacidad del proveedor de entregar el servicio de forma eficiente, eficaz, segura, fiable y continua?	100,00%
2.2	3.3						APO10	APO10.04	15	¿Al definir el contrato, se incluye una descripción clara de todos los requisitos de servicio con base a la Ley 7494 Contratación Administrativa?	75,00%
2.2	4.2	4.3	5.2				APO12	APO12.04	8	¿Se informa los resultados del análisis de riesgos a la Junta Directiva?	0,00%
2.2	2.1						BAI04	BAI04.01	11	¿Las actividades, proyectos, iniciativas, cambios, etc. se realizan tomando como base la capacidad de presupuesto y recursos?	75,00%
2.2	2.1						BAI04	BAI04.01	12	¿Se han dado incidentes asociados con la capacidad de recursos (humanos, materiales y presupuestarios)?	75,00%
2.2							BAI04	BAI04.02	13	¿Se tiene mapeado de previo algunas soluciones a incidentes relacionados con los recursos (humanos, materiales y presupuestarios) que se puedan generar?	25,00%

2.2	2.1	2.4					DSS04	DSS04.02	5	¿Con los riesgos identificados, se ha determinado alguna afectación en la continuidad de las actividades del CODEA?	0,00%
2.2	2.1	2.4					DSS04	DSS04.02	10	¿Tienen establecido el tiempo mínimo de recuperación ante una disrupción importante, así como medidas para reducir el impacto?	25,00%
2.2	3.2						EDM03	EDM03.01	6	2. ¿Se tiene definido y documentado el apetito al riesgo por la Junta Directiva?	0,00%
2.2	3.2						EDM03	EDM03.01	7	1. ¿Se tienen identificados y valorados los riesgos relacionados con el uso de las TI?	0,00%
2.2							APO12	N/I	3	Los riesgos identificados se analizan a través de un proceso que incluye estimar la importancia potencial del riesgo y considerar la probabilidad y frecuencia de ocurrencia y el impacto del riesgo si ocurriera.	0,00%
3.1	3.2	3.3					BAI07	BAI07.04	24	¿Las narrativas o los diagramas de flujo demuestran una combinación de controles dentro de cada proceso?	0,00%
3.1	3.2	3.3					BAI07	BAI07.05	1	¿Se detectaron errores en la fase de prueba o posterior a ello en la implementación del nuevo sistema?	100,00%
3.1	3.2	3.3					BAI07	BAI07.05	2	¿Se tiene documentación soporte del error y como se solventó?	100,00%
3.1	3.2	3.3					BAI07	BAI07.05	13	¿Se desarrolla y conserva evidencia que respalde la investigación la resolución de asuntos (Quejas/ temas legales)?	75,00%
3.1	5.1	5.2					BAI09	BAI09.02	33	¿Se identifica de manera oportuna incidentes o activos en mal estado?	50,00%
3.1	5.1	5.2					BAI09	BAI09.02	34	¿Se reacciona inmediatamente al reemplazo, reparación y/o mantenimiento de los activos?	50,00%

3.1	5.1	5.2					BAI09	BAI09.02	35	¿Se realiza mantenimiento preventivo con el fin de preservar los activos fijos del CODEA?	75,00%
3.1	3.2	3.3.					BAI09	BAI09.03	36	¿Existen prácticas adecuadas como un debido proceso para la adquisición de nuevos activos? (solicitud, revisión, y aprobación)	100,00%
3.1	3.2	3.3.					BAI09	BAI09.03	37	¿Se tienen paqueados TODOS los activos fijos?	100,00%
3.1	1.3	2.1	3.3	4.2			EDM03	EDM03.02	6	¿Se cuenta con políticas de prevención y detección de riesgos?	25,00%
3.1	1.3	2.1	3.3	4.2			EDM03	EDM03.02	7	¿Específicamente se cuenta con una política de prevención y detección de riesgos ante el uso de TI para los colaboradores?	25,00%
3.1	1.3	2.1	4.2	3.3			EDM03	EDM03.02	27	¿CODEA comunica a los usuarios los posibles riesgos por el uso de los sistemas de información y promueve una cultura de prevención y detección de los mismos?	75,00%
3.1	2.1	4.1	5.2				MEA02	MEA02.02	20	¿Mantienen documentado la efectividad o deficiencias de los controles que poseen?	0,00%
3.2	3.1	3.3					BAI09	BAI09.01	25	¿Se tienen claramente identificados y registrados en un auxiliar TODOS los activos del CODEA?	100,00%
3.2	3.1	3.3					BAI09	BAI09.01	26	¿Esta información se encuentra registrada en el nuevo ERP?	50,00%
3.2	3.1	3.3					BAI09	BAI09.01	27	¿Se ha realizado conteo de activos en el último periodo 2020/2021? (parciales o al 100%)	87,50%
3.2	3.1	3.3					BAI09	BAI09.01	28	¿Se tiene documentación soporte de estos conteos?	75,00%
3.2	3.1	3.3					BAI09	BAI09.01	29	¿Se valida la vida útil de los activos?	75,00%

3.2	3.1	3.3					BAI09	BAI09.01	30	¿Estas validaciones se hacen de manera recurrente? (mensual, semestral, anual)	75,00%
3.2	3.1	3.3					BAI09	BAI09.01	31	¿Se tienen los procesos de activo identificados mediante diagramas de flujo?	0,00%
3.2	3.1	3.3					BAI09	BAI09.01	32	¿Cuándo se dan violaciones de seguridad referidas a activos se monitorean, se informan y resuelven adecuadamente?	75,00%
3.2	3.2	3.3.					BAI09	BAI09.03	38	¿Se tiene registrado las bajas de activo por desuso, obsolescencia, falla, etc.?	50,00%
3.2	3.3						DSS04	DSS04.01	21	¿Tienen definido y documentado alguna política sobre la continuidad de las actividades del CODEA?	0,00%
3.2	3.3						DSS04	DSS04.01	22	¿Identifican procesos de soporte de los servicios de TI que eventualmente el CODEA requiera?	75,00%
3.2	3.3						DSS04	DSS04.07	16	¿Realizan copias de seguridad de los archivos con los que trabajan?	50,00%
3.2							DSS05	DSS05.03	17	¿Tienen controles de seguridad sobre los accesos, contraseñas y responsables de información confidencial?	75,00%
3.2							DSS05	DSS05.04	18	¿Mantienen los accesos de los usuarios de acuerdo con los requerimientos de las funciones y procesos de negocio?	100,00%
3.2							MEA03	MEA03.01	8	¿Identifican y supervisan los cambios legales y regulatorios que les afectan?	75,00%
3.2							MEA03	MEA03.01	9	¿Se tiene definidos a los funcionarios encargados de realizar evaluaciones de los cambios legales y regulatorios?	75,00%
3.2	5.1						MEA03	MEA03.02	10	¿Actualizan las políticas, principios procedimientos y estándares para mantener la eficiencia y el cumplimiento de los procesos del CODEA?	75,00%

3.2	5.1						MEA03	MEA03.02	11	¿Se realizan con frecuencia?	25,00%
3.2	5.1						MEA03	MEA03.02	12	¿Se tiene definidos a los funcionarios encargados de actualizar estás políticas, principios, procedimientos y estándares?	50,00%
3.3	3.1	3.2					APO01	APO01.06	14	¿Se establecen políticas y procedimientos que permitan asegurar la confidencialidad, integralidad y seguridad de la información (datos) de CODEA?	50,00%
3.3	3.1	3.2					APO01	APO01.06	15	¿Se tiene un inventario que incluya un listado de los propietarios y custodios de la información (sistemas y datos)?	75,00%
3.3	3.1	3.2					APO01	APO01.07	4	¿Se tienen identificados procesos críticos de negocio?	50,00%
3.3	3.1	3.2					APO01	APO01.07	5	¿Se evalúa el rendimiento y capacidad de estos procesos?	25,00%
3.3							APO10	APO10.02	3	¿Se tiene establecida alguna política de selección de proveedores que asegure un adecuado y transparente proceso?	100,00%
3.3	1.3						DSS06	DSS06.03	19	¿Tienen asignado roles y responsabilidades cuando se realizan traslados de datos de un sistema a otro?	100,00%
3.3	4.2						EDM04	EDM04.01	3	¿Se cuentan con políticas para uso adecuado de los sistemas de información? (Políticas de seguridad de información, políticas de uso de los equipos de TI, Políticas de riesgos de seguridad de la información)	80,00%
3.3	4.2						EDM04	EDM04.01	23	¿Se cuenta con una planeación para la asignación y gestión de los recursos (presupuesto, personas, procesos y tecnologías) de acuerdo con los límites presupuestarios?	75,00%

4.2	1.4						EDM02	EDM02.02	1	¿Los usuarios a través de sus roles, responsabilidades, y asignaciones cumplen con sus funciones de acuerdo con el manual de puestos?	60,00%
4.1	4.2	4.3					BAI02	BAI02.01	2	¿Existe una persona que realiza validaciones de que la información cumpla con la normativa y legislación aplicable, así como que sea entregada en tiempo y forma?	80,00%
4.2	5.2						EDM03	EDM03.03	2	¿Se cuenta con informes, métricas u objetivos que permitan evaluar la gestión de riesgos del CODEA?	60,00%
4.1	4.2	4.3					EDM05	EDM05.01	4	¿Los sistemas de información permiten cumplir con los requerimientos (legales, regulatorios, o normativos) de las partes interesadas?	100,00%
4.1	4.2	4.3					BAI02	BAI02.01	5	¿Está claramente identificada la información que se debe generar (diaria, semanal, mensual, trimestral, semestral y anualmente) a las partes interesadas (funcionarios de CODEA, Junta Directiva, CGR, Hacienda, Municipalidad)?	80,00%
4.3	4.1						APO10	APO10.03	6	¿Se tiene definido algún proceso de comunicación formal y de revisión de términos contractuales y de servicio con los proveedores de CODEA?	100,00%
4.1	4.2	4.3	1.3				APO13	APO13.01	7	¿Se tiene establecido un sistema de gestión de la seguridad de la información (SGSI) y políticas de seguridad documentadas formalmente?	80,00%
4.2	5.2						APO13	APO13.03	8	¿Ese SGSI es revisado periódicamente y actualizado cuando es necesario? (Considerando incidentes ocurridos, recomendaciones de las partes interesadas, o auditorias)	60,00%
4.3	3.3						DSS02	DSS02.01	9	¿Presentan y documentan controles y/o registros de los incidentes de seguridad que han tenido con el sistema para evaluar las posibilidades de mejora?	60,00%

4.2	3.2	3.3					DSS05	DSS05.01	10	¿Poseen controles de seguridad ante software maliciosos? (Mediante políticas de uso de las TI, instalación de software no autorizado, correos o descargas de fuentes sospechosas)	60,00%
4.2	3.2	3.3					DSS05	DSS05.02	11	¿Los dispositivos autorizados para tener acceso a la información y a la red de la empresa están configurados para forzar la solicitud de contraseña?	80,00%
4.1	4.2	4.3					BAI02	BAI02.01	12	¿Cuándo la información se obtiene de sistemas de información de terceros, la administración considera los controles establecidos por el proveedor de servicios y dentro de la empresa para evaluar la integridad y precisión de la información?	60,00%
4.1	5.2	2.1					EDM02	EDM02.03	13	¿Los sistemas de información permiten generar informes sobre los resultados financieros y no financieros de CODEA para la toma de decisiones?	100,00%
4.2	4.1						APO08	APO08.04	14	¿Los sistemas de información producen información oportuna, actual, precisa, completa, accesible, protegida, verificable y retenida?	70,00%
4.1	2.1						BAI02	BAI02.03	15	¿Se realiza revisión de los estados financieros por los niveles apropiados de administración para verificar su integridad y fiabilidad?	60,00%
4.1	2.1						BAI02	BAI02.03	16	¿La revisión de la Información presentada a la Junta directiva queda debidamente documentada en las minutas y/o actas?	100,00%
4.1	5.2						BAI04	BAI04.04	17	¿Se prepara y comunica información referente al desempeño y disponibilidad de los recursos (humanos, materiales y presupuestarios) a la Junta Directiva?	100,00%
4.1	3.2	4.3					BAI08	BAI08.03	18	¿Existe algún mecanismo que permita generar información integrada entre los diferentes departamentos?	80,00%

4.1	3.2	4.3					BAI08	BAI08.03	19	¿Existen medios de publicación de información donde los funcionarios de CODEA y usuarios externos puedan consultarla? (Ejemplo: Página web)	100,00%
4.2	3.2	4.1					EDM02	EDM02.01	20	¿Se tienen identificados estrategias de mejoras o inversiones de los sistemas de información en el mediano y largo plazo para mejorar los procesos?	60,00%
4.2	1.4						EDM02	EDM02.02	21	¿Las inversiones en sistemas de información (SAP Business One) han permitido lograr mejores resultados en la gestión operativa y financiera de CODEA?	60,00%
4.1	2.4	4.3					APO08	APO08.02	22	¿Se realizan estudios del entorno que ayuden a identificar las tendencias tecnológicas y cómo pueden aplicarse al CODEA de modo innovador para mejorar el rendimiento de los procesos de negocio?	40,00%
4.2	1.4						EDM02	EDM02.02	23	¿Existe comunicación interna que permita evaluar el cumplimiento de objetivos y con ello proponer mejoras a las deficiencias detectadas para mejorar el Control Interno?	80,00%
4.1	2.1						BAI02	BAI02.03	24	¿Se han dado situaciones donde la información no cumple con los requerimientos o no fue entregada en tiempo y forma?	40,00%
4.1	2.1						BAI02	BAI02.03	25	¿Se han dado implicaciones (multas, sanciones, etc.) por algún tipo de incumplimiento de los requerimientos tanto interno como externo?	80,00%
4.1	2.1						BAI02	BAI02.03	26	¿Tienen mecanismos para evitar incumplimientos o errores en la información entregada?	40,00%
4.1	4.3	4.1					EDM05	EDM05.02	28	¿CODEA cuenta con canales que permita una comunicación eficiente con las partes interesadas?	100,00%

4.1	3.2	5.2					DSS06	DSS06.02	29	¿Han ocurrido interrupciones inesperadas en el nuevo sistema SAP del CODEA?	20,00%
4.1	3.2	5.2					DSS06	DSS06.02	29	¿Se han logrado solventar de manera oportuna?	40,00%
4.2	5.2						EDM03	EDM03.03	5.1	¿Se comunica a la Junta Directiva los resultados de la gestión integral de riesgos?	40,00%
5.2	3.2	3.3	4.1				MEA02	MEA02.01	1	¿Se realiza autoevaluaciones de control Interno para conocer su nivel de madurez en el CODEA?	40,00%
5.2	3.2	3.3	4.1				MEA02	MEA02.01	3	¿Se comunican, priorizan y realizan acciones correctivas cuando se identifican riesgos claves?	80,00%
5.2	4.2						DSS06	DSS06.04	4	¿Revisan errores, los documentan y los informan, para mantener seguimiento de ellos?	80,00%
5.2	3.2	3.3	3.1				DSS05	DSS05.06	5	¿Poseen medidas para retener información por un periodo adecuado, en caso de que se requieran para futuras investigaciones o revisiones para partes interesadas internas y externas?	80,00%
5.2	5.1						BAI07	BAI07.01	6	¿Existe un proceso para garantizar que las deficiencias identificadas a través de todas las fuentes (evaluación de la gestión, auditorias, partes externas) se mantengan documentadas y generen un historial?	100,00%
5.2							APO10	APO10.01	7	¿Se tienen establecidos criterios de evaluación del rendimiento de los proveedores?	60,00%
5.2	3.2	3.3	4.1				MEA02	MEA02.01	8	¿Les realizan auditorías ya sea por empresas contratadas o por entidades públicas (incluida la Municipalidad de Alajuela)?	100,00%
5.2	5.1						BAI07	BAI07.01	9	¿Se procede a solicitar aprobación por parte de la JD para la implementación de nuevos sistemas de TI?	100,00%

Anexo K.

Procesos de Gobierno de TI Empresarial de COBIT 5

Sigla	Nombre completo
APO01	**Gestionar el marco de gestión de TI**
APO01.03	Mantener los elementos catalizadores del sistema de gestión.
APO01.06	Definir la propiedad de la información (datos) y del sistema.
APO01.07	Gestionar la mejora continua de los procesos.
APO02	**Gestionar la estrategia**
APO02.01	Comprender la dirección de la empresa.
APO02.02	Evaluar el entorno, capacidades y rendimiento actuales.
APO08	**Gestionar las relaciones**
APO08.02	Identificar oportunidades, riesgos y limitaciones de TI para mejorar el negocio
APO08.04	Coordinar y comunicar.
APO10	**Gestionar los proveedores**
APO10.01	Identificar y evaluar las relaciones y contratos con proveedores.
APO10.02	Seleccionar proveedores.

APO10.03 Gestionar contratos y relaciones con proveedores.

APO10.04 Gestionar el riesgo en el suministro.

APO12 Gestionar el riesgo

APO12.04 Expresar el riesgo.

APO13 Gestionar la seguridad

APO13.01 Establecer y mantener un SGSI.

APO13.03 Supervisar y revisar el SGSI.

BAI02 Gestionar la definición de requisitos

BAI02.01 Definir y mantener los requerimientos técnicos y funcionales de negocio.

BAI02.03 Gestionar los riesgos de los requerimientos.

BAI04 Gestionar la disponibilidad y la capacidad

BAI04.01 Evaluar la disponibilidad, rendimiento y capacidad actual y crear una línea de referencia

BAI04.02 Evaluar el impacto en el negocio

BAI04.04 Supervisar y revisar la disponibilidad y la capacidad

BAI04.05 Investigar y abordar cuestiones de disponibilidad, rendimiento y capacidad

BAI07 Gestionar la aceptación del cambio y la transición

BAI07.01 Establecer un plan de implementación

BAI07.04 Establecer un entorno de pruebas

BAI07.05 Ejecutar pruebas de aceptación

BAI08	**Gestionar el conocimiento**
BAI08.01	Cultivar y facilitar una cultura de intercambio de conocimientos
BAI08.03	Organizar y contextualizar la información, transformándola en conocimiento
BAI09	**Gestionar los activos**
BAI09.01	Identificar y registrar activos actuales
BAI09.02	Gestionar activos críticos
BAI09.03	Gestionar el ciclo de vida de los activos
DSS02	**Gestionar peticiones e incidentes de servicio**
DSS02.01	Definir esquemas de clasificación de incidentes y peticiones de servicio
DSS04	**Gestionar la continuidad**
DSS04.01	Definir la política de continuidad del negocio, objetivos y alcance
DSS04.02	Mantener una estrategia de continuidad
DSS04.07	Gestionar acuerdos de respaldo
DSS05	**Gestionar servicios de seguridad**
DSS05.01	Proteger contra software malicioso (malware)
DSS05.02	Gestionar la seguridad de la red y las conexiones
DSS05.03	Gestionar la seguridad de los puestos de usuario final
DSS05.04	Gestionar la identidad del usuario y el acceso lógico
DSS05.06	Gestionar documentos sensibles y dispositivos de salida

DSS06 Gestionar controles de proceso de negocio

DSS06.02 Controlar el procesamiento de la información.

DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.

DSS06.04 Gestionar errores y excepciones.

EDM02 Asegurar la entrega de beneficios

EDM02.01 Evaluar la optimización del valor.

EDM02.02 Orientar la optimización del valor.

EDM02.03 Supervisar la optimización del valor

EDM03 Asegurar la optimización del riesgo

EDM03.01 Evaluar la gestión de riesgos.

EDM03.02 Orientar la gestión de riesgos.

EDM03.03 Supervisar la gestión de riesgos.

EDM04 Asegurar la optimización de recursos

EDM04.01 Evaluar la gestión de recursos.

EDM05 Asegurar la transparencia hacia las partes interesadas

EDM05.01 Evaluar los requisitos de elaboración de informes de las partes interesadas.

EDM05.02 Orientar la comunicación con las partes interesadas y la elaboración de informes.

MEA02 Supervisar, evaluar y valorar el sistema de control interno

MEA02.01 Supervisar el control interno

MEA02.02 Revisar la efectividad de los controles sobre los procesos de negocio.

MEA03 Supervisar, evaluar y valorar la conformidad con los requerimientos externos.

MEA03.01 Identificar requisitos externos de cumplimiento.

MEA03.02 Optimizar la respuesta a requisitos externos.

CAPÍTULO IV

Anexo L.

Documentación de la propuesta suministrada al CODEA con la Herramienta de Evaluación de Riesgos Transitoria

Sistema de Valoración de Riesgos Transitorio

Junio, 2022

ÍNDICE

1.Objetivo

Establecer un sistema de valoración de riesgos que le permita al CODEA identificar, analizar y definir acciones de administración de los riesgos a los cuales está expuesto durante el desarrollo de su gestión.

2.Introducción

La mejora del control interno es un eje fundamental para mejorar la eficiencia y economía de la gestión pública, con la ayuda de las mejores prácticas en la materia con el fin de obtener una seguridad razonable del cumplimiento de los objetivos institucionales.

A partir de la entrada en vigencia de la Ley General de Control Interno Ley Nº 8292 del 31 de julio del 2002, los diferentes órganos deberán disponer de sistemas de control interno, los cuales deberán ser aplicables, completos, razonables, integrados y congruentes con sus competencias y atribuciones institucionales. Como parte de lo dispuesto en dicha Ley se establece la obligatoriedad de contar con un Sistema Específico de Valoración de Riesgo Institucional (SEVRI) que permita identificar el nivel de riesgo institucional y adoptar los métodos de uso continuo y sistemático, a fin de analizar y administrar el nivel de dicho riesgo. También existe un régimen sancionatorio para los jerarcas, los titulares subordinados y los demás funcionarios que no efectúen las acciones necesarias para establecer y mantener el SEVRI.

A la fecha el CODEA no cuenta con una planeación estratégica de la cual se puedan derivar objetivos institucionales que permitan desarrollar e implementar un Sistema Específico de

Valoración de Riesgo Institucional tal como lo establece el Legislador. Como respuesta a la necesidad del CODEA, la presente metodología cuenta con el fin de servir de insumo para que la institución comience a implementar este tipo de prácticas hasta que establezca las bases para la implementación de un SEVRI de acuerdo con los requerimientos de la Ley.

También, mediante el oficio R-CO-64-2005 emitido por la Contraloría General de la República implantó directrices generales para el establecimiento y funcionamiento del SEVRI, dentro de las cuales menciona que se deberá establecer una herramienta para la gestión y documentación de la información que utilizará y generará el SEVRI, la cual podrá ser de tipo manual, computarizada o una combinación de ambos. Y que la misma deberá contar con un sistema de registros de información que permita el análisis histórico de los riesgos institucionales y de los factores asociados a dichos riesgos.

Por ello adicional a la metodología, se brinda una herramienta tecnológica que agilice el proceso de valoración de riesgos de la entidad y que sea de fácil uso para los usuarios.

Dicha herramienta tiene como propósito que el CODEA esté en posibilidad de realizar el registro de los riesgos que enfrenta, analizarlos conforme a su impacto y probabilidad de ocurrencia y así mismo asignar controles y responsables específicos de su implementación.

Con la metodología y herramienta se busca fortalecer el control interno de la institución.

3.Marco orientador

3.1 Marco Orientador General

El CODEA como una institución adscrita a una entidad pública tiene una serie de reglamentos y/o leyes a los que se debe apegar y alinear dentro de sus actividades, con el fin de garantizar el cumplimiento de los objetivos y metas institucionales.

- *Constitución Política de Costa Rica*

Es la ley fundamental vigente en Costa Rica y es definida como aquella que " fija los límites y define las relaciones entre los poderes del Estado, de estos con sus ciudadanos estableciendo así las bases para su gobierno y para la organización de las instituciones en que tales poderes se asientan" **(** Ministerio de Educación Pública [MEP]).

- *Disposiciones generales de la Contraloría General de la República***.**

La Contraloría General de la República (CGR) es el órgano constitucional, auxiliar de la Asamblea Legislativa que fiscaliza el uso de los fondos públicos para mejorar la gestión de la Hacienda Pública y contribuir al control político y ciudadano. En línea con lo anterior dicha entidad es la encargada de generar los lineamientos y/o directrices que van a regir a las entidades públicas y a sus actividades en cuanto al tema de control interno.

3.2 Marco Orientador Control Interno

En línea con el marco orientador general es importante resaltar que a nivel de Control Interno existen leyes costarricenses que lo sustentan, así como, marcos normativos que permiten y ayudan como guía para su correcto desempeño y cumplimiento.

- *Ley General de Control Interno N. 8292*

La Ley busca establecer los criterios mínimos de control interno, que deben implementar las diferentes instituciones públicas en Costa Rica. Esta Ley contempla una serie de elementos con el fin de apoyar la gestión de las organizaciones. Estos elementos son el ambiente de control, la evaluación del riesgo, los sistemas de información, las actividades de control y el seguimiento.

- Normas de Control Interno para el sector Público

La valoración de riesgos institucional es un proceso que de acuerdo con las Normas de Control Interno para el sector Público (N-2-2009-CO-DFOE) y reforma Resoluciones N° R-CO-64-2005, N° R-CO-26-2007, N° R-CO-10-2007 estipulados en su capítulo III; los jerarcas y titulares deben definir, implementar, verificar y perfeccionar para que el efecto se establezca.

También se menciona que “debe presentar las características e incluir los componentes y las actividades que define la normativa específica aplicable. Asimismo, debe someterse a las verificaciones y revisiones que correspondan a fin de corroborar su efectividad continua y promover su perfeccionamiento”. (CGR, 2009, p.11)

- *COSO 2013*

El modelo COSO es un marco de buenas prácticas desarrollado por el Comité de Organizaciones Patrocinadoras de la Comisión Treadway (COSO, por sus siglas en inglés), esta es una comisión voluntaria que se encarga de desarrollar las mejores prácticas en temas de fraude, gestión de riesgo empresarial y control interno.

COSO III fue publicado en el año 2013, de acuerdo con el Resumen Ejecutivo facilitado por COSO (2013), este marco se enfoca en considerar elementos del mercado global y en ampliar el alcance de la información financiera y no financiera, tanto interna como externa. Considera 17 principios de control interno, categorizados en cinco componentes de control interno de COSO los cuales deben operar de manera conjunta: 1) entorno de control, 2) evaluación de riesgos, 3) actividades de control, 4) información y comunicación y 5) actividades de supervisión.

- *COBIT 5*

COBIT (Control Objectives for Information and related Technology), es un modelo para el buen gobierno y la gestión de las tecnologías de información y la tecnología de la empresa, el cual está basado en cinco principios claves para el gobierno y la gestión, los cuales son: 1) Satisfacer las necesidades de las partes interesadas, 2) Cubrir a la empresa de extremo a extremo, 3) Aplicar un marco de referencia único integrado, 4) Hacer posible un enfoque holístico y 5) Separar el gobierno de la gestión. Según Vanegas (2013), estos cinco principios unidos “habilitan a la empresa a construir un marco de gestión de gobierno y gestión efectivo que optimiza la inversión y el uso de información y tecnología para el beneficio de las partes interesadas” (2013, p. 46).

4.Metodología de valoración de riesgos

4.1 Generalidades

El sistema de valoración de riesgos se desarrollará utilizando las siguientes herramientas:

- Cuenta de gmail: controlinternocodea@gmail.com
- Dirección *Site* de Valoración de riesgos: https://sites.google.com/view/codeariesgos/inicio
- Dirección carpeta de google CODEA_RIESGOS: https://sites.google.com/view/codeariesgos/inicio

Inicialmente se deberá definir a la persona encargada de desarrollar el proceso de valoración de riesgos, esta deberá ingresar a la cuenta de controlinternocodea@gmail.com con el fin de poder acceder a las demás herramientas.

Seguidamente, mediante el Site la persona podrá guiarse con los pasos ahí descritos o bien, seguir los pasos que acá se describen.

La información generada es almacenada automáticamente en la carpeta de google CODEA_RIESGOS.

Finalmente, de acuerdo con lo indicado por la Ley General de Control Interno, es importante que este proceso de valoración de riesgos se lleve a cabo como mínimo una vez al año.

4.2 Definición del apetito y tolerancia al riesgo

De acuerdo con COSO 2013, el apetito al riesgo es la cantidad de riesgo de base amplia que una entidad está dispuesta a aceptar en la búsqueda de su misión, visión y cumplimiento de sus objetivos.

Sus características son las siguientes:

- Es una aprobación de alto nivel de aceptación de un riesgo en el logro de los objetivos.
- Se puede expresar por medio de mapas de calor.

En este sentido, el apetito al riesgo del CODEA es definido tomando en consideración los parámetros establecidos para identificar el nivel de impacto y probabilidad de los riesgos que esta metodología señalará más adelante.

El cálculo corresponde al siguiente:

Valor máximo de probabilidad	X	Valor máximo de impacto	=	**Apetito al riesgo**
5	**X**	**5**	**=**	**25**

Por otra parte, de acuerdo con COSO 2013 la tolerancia al riesgo es el nivel aceptable de variación en relación con el logro de objetivos.

Sus características son las siguientes:

- Debe ser definido formalmente por la Alta Dirección.
- Debe mantener coherencia con el apetito al riesgo (qué nivel de riesgo está dispuesto a aceptar).
- Establecer riesgos que la institución no está dispuesta a aceptar.

A raíz de lo anterior se instruye al CODEA definir el valor de Tolerancia al riesgo, siempre respetando el Apetito al riesgo definido previamente.

Para efectos de esta metodología se procederá a sugerir una Tolerancia al riesgo de 10.

4.3 Identificación de riesgos

La primera fase de la valoración de riesgos consiste en la identificación de los mismos, para esto se procede a sugerir las siguientes técnicas de identificación de riesgos:

1) Preguntas predeterminadas

   Se procede a generar un inventario de riesgos en el cual cada riesgo contiene una pregunta asociada, de esta forma se agiliza la identificación del riesgo mediante la respuesta a la pregunta. Es importante que las preguntas se encuentren redactadas de manera dicotómica, es decir, con respuestas de Sí y No únicamente. De manera que, al contestar No, se estaría identificando riesgos asociados.

   En el caso de la presente metodología, se presenta un inventario de riesgos predeterminado, el cual fue generado con base en la teoría expuesta por COSO 2013

y por COBIT 5 en Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa y en el documento llamado Procesos Catalizadores.

2) Mapeos de procesos

El mapeo de procesos se puede realizar mediante el diseño de flujogramas de manera que permita identificar puntos críticos que pueden significar un riesgo presente o futuro dentro de cada uno de los procesos.

3) Talleres de autoevaluación:

Los talleres de autoevaluación se pueden realizar mediante reuniones o grupos focales con los colaboradores de CODEA de diversos puestos y niveles jerárquicos sobre procesos clave dentro de la entidad, con el objetivo de identificar riesgos relacionados con sus actividades y funciones a cargo. Los talleres buscan analizar a detalle posibles eventos que se perciben en sus actividades diarias, que puedan materializar riesgos.

4) Otras técnicas:

a) Entrevista con el Jerarca: Consiste en una reunión con el Jerarca de CODEA, para identificar eventos puntuales derivados de la administración de la entidad, su estado actual y futuro, así como conocimiento de riesgos materializados en el pasado. Así como tener un enfoque de administración de riesgos desde el punto de vista de los altos jerarcas y su importancia en el CODEA.

b) Análisis comparativo con entidades del Sector Público: Consiste en realizar investigación y análisis de riesgos con comités cantonales de deportes o

entidades públicas donde se puedan identificar riesgos principalmente asociados a la gestión de recursos públicos, o identificar bases de datos con los riesgos materializados en el pasado en dichas instituciones.

c) Investigación Web: Comprende el análisis de noticias, documentales, o informes publicados en internet sobre instituciones públicas que se deriven del manejo de recursos públicos y riesgos de fraude, los cuales son riesgos materializados y que se encuentran documentados.

d) Entrevista con funcionario externo: Consiste en realizar una entrevista con un funcionario externo con experiencia en el Sector Público sobre los principales y más frecuentes riesgos identificados en este tipo de entidades desde la experticia de un profesional en auditorías.

Para efectos de esta metodología, la técnica a utilizar es "Preguntas predeterminadas", sin embargo, la institución puede aplicar cualquiera de las otras técnicas de forma previa con el fin de contar con un conocimiento más ampliado y argumentado al momento de responder dichas preguntas.

4.3.4 Inventario de riesgos CODEA

El inventario de riesgos contiene una variedad de riesgos que se encuentran clasificados de acuerdo con los siguientes dos marcos: en el Modelo de Riesgo Proviti y en el Modelo de Estructura de Riesgos de la Contraloría General de la República.

El Modelo de Riesgo Proviti estructura los riesgos en tres grandes bloques: 1) Riesgos del medio ambiente o entorno, 2) Riesgos de procesos y 3) Riesgo de información para la toma

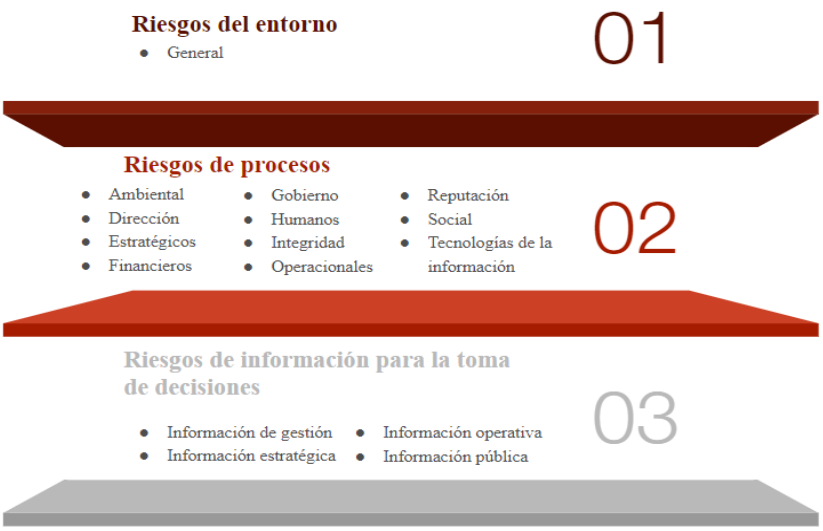
de decisiones. Es importante destacar, que algunas definiciones de riesgo de este modelo fueron eliminadas dado que no aplican al CODEA.

Por otra parte, a partir del Modelo de Estructura de Riesgos de la Contraloría General de la República, se extrae una subclasificación y definición de riesgos. De igual forma, también se excluyen algunos riesgos señalados en este Modelo, dado que no aplican al CODEA.

A raíz de lo anterior se obtiene la siguiente estructura de riesgos para el CODEA:

Imagen 1:

Estructura de riesgos CODEA



Fuente: Elaboración propia

Adicionalmente, además de contar con un listado de riesgos clasificados, cada riesgo posee una pregunta asociada con el fin de facilitar la identificación del riesgo y también, cuentan con un control o acción de respuesta asociado, fundamentados en la teoría expuesta por COSO 2013 y COBIT 5.

El archivo llamado Inventario de Riesgos es el que alimenta el formulario de preguntas a llenar por parte del CODEA durante el proceso de Identificación de Riesgos.

Como bien se indicó en la sección anterior, para iniciar el proceso de Valoración de riesgos la persona deberá seguir los siguientes pasos:

1) Ingresar a la cuenta de google: controlinternocodea@gmail.com.
2) Ingresar al Site de Valoración de Riesgos: https://sites.google.com/view/codeariesgos/inicio
3) Ubicar la carpeta llamada CODEA_RIESGOS en la sección de Drive.
4) Ubicar el archivo llamado 1.INVENTARIO DE RIESGOS en la carpeta CODEA_RIESGOS.
    a) El archivo 1.INVENTARIO DE RIESGOS posee una única pestaña que contiene una tabla con 6 columnas:
        i) PREGUNTA: Corresponde a la pregunta que permite identificar el riesgo.
        ii) RIESGO: Corresponde al nombre del riesgo asociado a la pregunta anterior.
        iii) DETALLE: Corresponde a una descripción del riesgo.

iv) CLASIFICACION_1: Corresponde a la clasificación del riesgo según el Modelo de Riesgo Proviti.

v) CLASIFICACION_2: Corresponde a la clasificación del riesgo según el Modelo de Estructura de Riesgos de la Contraloría General de la República.

vi) CONTROL: Corresponde al control sugerido por la herramienta para dar respuesta al riesgo.

b) La persona **ÚNICAMENTE podrá eliminar o agregar FILAS**. Si desea agregar o eliminar columnas debe considerar que deberá realizar un ajuste en la programación de Apps Script del archivo.

c) El CODEA debe definir si el Inventario de Riesgos deberá actualizarse o no, es decir; agregar, eliminar o modificar riesgos.

5) Una vez que el Inventario de Riesgos se encuentre aprobado, en caso de que se hicieran cambios la persona deberá ubicar la pestaña “Herramienta Riesgos” ubicada en la parte de arriba del archivo.

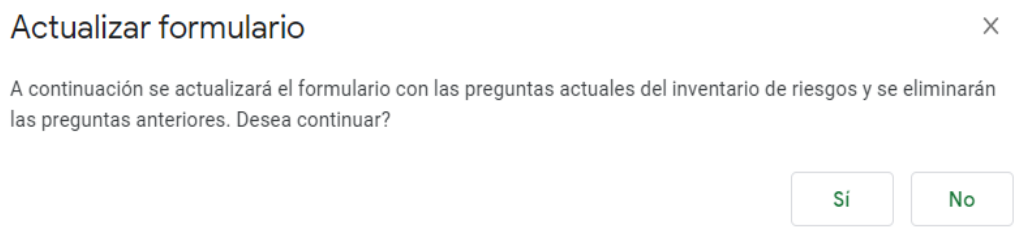
a) Dar clic a “Herramienta Riesgos".

b) Dar clic en 1- Actualizar formulario. Si la herramienta le solicita permisos entonces deberá brindarlos según las instrucciones que le muestre.

c) Una vez que dio clic a la opción 1- Actualizar formulario, se desplegará el siguiente mensaje:

Imagen 3:

Mensaje de actualización de formulario



d) La persona deberá dar clic a la opción "Sí" con el fin de que actualice de forma automática los cambios realizados al Inventario de Riesgos en el Formulario_Riesgos.

   i) El **Formulario_Riesgos NO debe actualizarse de forma manual**, únicamente se deberá actualizar de la manera descrita en los puntos anteriores.

6) No es necesario realizar los pasos detallados en el punto 5 en caso de que el Inventario de Riesgos NO fuera modificado.

7) Ubicar el archivo 4.HERRAMIENTA_RIESGOS y completar la pestaña llamada "CONFIG" con la siguiente información:

   a) RESPONSABLE: Ingresar el nombre completo de la persona o personas encargadas del proceso de Valoración de Riesgos.

   b) FECHA_INICIO: Indicar la fecha de inicio del proceso de Valoración de Riesgos.

c) FECHA_FINAL: Indicar la fecha de finalización del proceso de Valoración de Riesgos.

d) ASUNTO_CORREO: Corresponde al asunto del correo que se enviará al finalizar el proceso de Valoración de Riesgos.

e) CUERPO: Corresponde al cuerpo del correo que se enviará al finalizar el proceso de Valoración de Riesgos.

f) TOLERANCIA_RIESGO: Corresponde a un número entero definido como tolerancia al riesgo de acuerdo con el apetito al riesgo definido previamente.

g) Es importante mencionar que la persona **NO DEBERÁ modificar las celdas A1:A5, ni agregar o eliminar filas entre las mismas.** Debe considerar que si desea hacer alguna modificación deberá modificar las fórmulas ubicadas en el archivo Plantillas[10] y actualizar la programación en Apps Script para el envío de correo.

8) Completar el Formulario_Riesgos respondiendo a las preguntas marcando Si o No según corresponda.

9) En el archivo 4.HERRAMIENTA RIESGOS, en la pestaña 1-IDENTIFICACIÓN podrá observar los riesgos identificados de manera automática según las respuestas enviadas mediante el formulario.

[10] Este archivo es la plantilla que finalmente se imprime en formato PDF para generar el reporte final. Mediante la fórmula `IMPORTRANGE` se extraen los datos del archivo 4. Herramienta RIESGOS.

10) Finalmente, en el Site de Valoración de Riesgos, específicamente en la pestaña Identificación de riesgos, mediante un DataStudio, también podrá visualizar los riesgos identificados e interactuar con los mismos.

4.4 Análisis de riesgos

La segunda etapa del proceso consiste en el análisis de riesgos, el objetivo de la misma consiste en establecer una valoración y priorización de los riesgos de acuerdo con la información obtenida en la etapa anterior de identificación de riesgos.

En la 4.HERRAMIENTA RIESGOS se ingresa en la pestaña 2-ANALISIS, la cual se compone de la siguiente manera:

- RIESGO (Columna A): Se compone de cada uno de los riesgos identificados por el usuario, al cual se le realizará el análisis de riesgo. Este es un campo **no** editable.
- DETALLE (Columna B): Consiste en la descripción detallada de cada uno de los riesgos de la columna A. Este es un campo **no** editable.
- CLASIFICACIÓN_1 (Columna C): Se refiere a la primera categoría de la clasificación de riesgos, la cual es la más general. Este es un campo **no** editable. El cual puede ser cualquiera de los siguientes:
    - Riesgos del entorno: Surge cuando hay fuerzas externas que podrían afectar la viabilidad del modelo de negocios de la institución incluyendo aspectos básicos que guían objetivos globales y estrategias que definen a ese modelo. (Modelo de Riesgos Proviti)

- Riesgo de procesos: Es el riesgo que los procesos de negocios de la institución no están adquiriendo, administrando, renovando y disponiendo eficazmente los recursos del negocio. No están claramente definidos ni alineados con sus estrategias. No están operando eficaz y eficientemente para satisfacer las necesidades del cliente. (Modelo de Riesgos Proviti)
- Riesgos de información para la toma de decisiones: Es el riesgo de que la información utilizada para apoyar la ejecución del modelo de negocios, la generación de reportes internos y externos sobre la *perfomance* y la evaluación continua de la efectividad del modelo de negocios de la organización no sea relevante o confiable. Estos riesgos se relacionan con todos los aspectos de las actividades de creación de valor de la institución. (Modelo de Riesgos Proviti)

- CLASIFICACIÓN_2 (Columna D): Consiste en subdivisiones de las clasificaciones de riesgo generales del punto anterior. Este es un campo **no** editable. Ver Imagen 1. Estructura de riesgos CODEA.
- VALOR_PROBABILIDAD (Columna E): Es el valor de la probabilidad de que un evento suceda. El valor de la probabilidad de riesgo se encuentra en una escala de 1 a 5, donde el 1 representa riesgo de ocurrencia muy bajo, y 5 siendo una ocurrencia muy altamente probable. Este es un campo **editable**.

  En el campo VALOR_PROBABILIDAD se despliega una lista de valores del 1 al 5. El usuario define el valor de acuerdo con el riesgo analizado. Ver Tabla 1 Valor, categoría y descripción de la probabilidad.

- CATEGORÍA_PROBABILIDAD (Columna F): Consiste en la categoría de probabilidad asignada de acuerdo con el valor asignado por el usuario. Puede ser rara, inusual, poco probable, muy probable o recurrente. Este es un campo **no** editable. La Tabla 1 Valor, categoría y descripción de la probabilidad.

Tabla 1.

Valor, categoría y descripción de la probabilidad

Valor	Categoría	Probabilidad
5	**Recurrente**	Riesgo cuya probabilidad de ocurrencia es muy alta, es decir, se tiene plena seguridad que éste se materialice, tiende a estar entre 90% y 100%.
4	**Muy probable**	Riesgo cuya probabilidad de ocurrencia es alta, es decir, se tiene entre 75% a 95% de seguridad que éste se materialice.
3	**Poco probable**	Riesgo cuya probabilidad de ocurrencia es media, es decir, se tiene entre 51% a 74% de seguridad que éste se materialice
2	**Inusual**	Riesgo cuya probabilidad de ocurrencia es baja, es decir, se tiene entre 25% a 50% de seguridad que éste se materialice.
1	**Rara**	Riesgo cuya probabilidad de ocurrencia es muy baja, es decir, se tiene entre 1% a 25% de seguridad que éste se materialice.

Fuente: Elaboración propia con base en la *Guía de Autoevaluación de Riesgos en el Sector Público* (Auditoría Superior de la Federación, 2014, p.22).

- VALOR_IMPACTO (Columna J): Se refiere al nivel de impacto que asigna el usuario de acuerdo con el riesgo. Puede tomar valores en una escala de 1 a 5, siendo nivel 1 el más bajo, como categoría menor, y 5 como el nivel más alto, como categoría catastrófica. Este es un campo **no** editable.

  Para definir el VALOR_IMPACTO, se toman en consideración tres factores: impacto operativo (Columna G), impacto legal y regulatorio (Columna H), e impacto de imagen y credibilidad pública (Columna I). Estos campos son **editables**. Ver Tabla 2. Factores que influyen en el impacto.

Tabla 2.

Factores que influyen en el impacto

Operativo	Legal y regulatorio	Imagen y credibilidad pública
Se refiere a la operación normal de los procesos del CODEA, considerando los términos de productividad, eficiencia, eficacia y economía.	Se refiere al cumplimiento de la normativa legal y regulatoria vigente y sus consecuencias en caso de incumplimiento.	Se refiere al nivel de impacto que la situación puede generar sobre la percepción de la imagen institucional del CODEA en el público.

  Para cada uno de los factores se despliega una lista de valores del 1 al 5. El usuario define el valor de acuerdo con el riesgo analizado. Cada factor posee un porcentaje de ponderación. Ver Tabla 3 Valor, categoría y descripción del impacto.

- CATEGORÍA_IMPACTO (Columna K): Consiste en la categoría de impacto asignada de acuerdo con el valor asignado por el usuario. Puede ser menor, bajo, moderado, grave o catastrófico. Este es un campo **no** editable. Ver Tabla 3 Valor, categoría y descripción del impacto.

Tabla 3.

Valor, categoría y descripción del impacto

Valor	Categoría	Impacto
5	**Catastrófico**	Riesgo cuya materialización influye directamente en el cumplimiento de la misión, visión y objetivos de la institución; asimismo puede implicar pérdida patrimonial o daño de la imagen, dejando además sin funciones total o parcialmente por un periodo importante de tiempo, afectando los programas o servicios que entrega la institución.
4	**Grave**	Riesgo cuya materialización podría dañar de manera significativa el patrimonial institucional, daño a la imagen o logro de los objetivos estratégicos. Asimismo, se necesita un periodo de tiempo considerable para restablecer la operación o corregir los daños.
3	**Moderado**	Riesgo cuya materialización causaría una pérdida importante en el patrimonio o un daño en la imagen institucional.
2	**Bajo**	Riesgo que no afecta el cumplimiento de los objetivos estratégicos y que en caso de materializarse podría causar daños al patrimonio o imagen, que se puede corregir en poco tiempo
1	**Menor**	Riesgo que en caso de materializarse podría tener efectos muy pequeños en la institución.

Fuente: Elaboración propia con base en la *Guía de Autoevaluación de Riesgos en el Sector Público* (Auditoría Superior de la Federación, 2014, p.22).

- RIESGO_INHERENTE (Columna M): Es la multiplicación aritmética del valor del impacto por el valor de la probabilidad. Este es un campo **no** editable. La fórmula es la siguiente:

RIESGO_INHERENTE = VALOR_IMPACTO * VALOR_PROBABILIDAD

Tabla 4.

Clasificaciones del riesgo inherente

Categoría	Definición
Extremo	Riesgo cuya materialización influye directamente en el cumplimiento de logros objetivos, metas, imagen, continuidad y negocio en marcha del CODEA.
Alto	Su materialización podría dañar de manera significativa a la institución.
Moderado	Efectos no afectan en gran medida a la institución si el riesgo llega a materializarse.
Bajo	Efectos menores a la institución si el riesgo llega a materializarse.

Fuente: Elaboración propia.

- CATEGORÍA_RIESGO (Columna N): Es la categoría asignada de acuerdo con el valor de riesgo inherente. El cual puede ser clasificado como bajo, moderado, alto y extremo. Este es un campo **no** editable.

Tabla 5.

Escala para determinar el riesgo inherente

Escala	Nivel de riesgo	Descripción
16-25	Extremo	Riesgo cuya materialización influye directamente en el cumplimiento de logros objetivos, metas, imagen, continuidad y negocio en marcha del CODEA.
11-15	Alto	Su materialización podría dañar de manera significativa a la institución.
6-10	Moderado	Los efectos no afectan en gran medida a la institución si el riesgo llega a materializarse.
1-5	Bajo	Efectos menores a la institución si el riesgo llega a materializarse.

Fuente: Elaboración propia

Finalmente, en el Site de Valoración de Riesgos, específicamente en la pestaña Análisis de riesgos, mediante un DataStudio, podrá visualizar los resultados obtenidos de dicho análisis e interactuar con los mismos.

4.5 Riesgo residual

La tercera etapa corresponde al análisis de riesgo residual. Se le conoce como riesgo residual al riesgo que permanece aún con la existencia de controles a los riesgos identificados.

Esto se debe a que los riesgos a los que está expuestos una entidad rara vez se pueden erradicar por completo; y, por ende, siempre se debe de buscar un equilibrio entre los recursos que se requieren adquirir para minimizar el riesgo y el nivel de riesgo que se considera manejable para continuar operando.

El cálculo del riesgo residual se realiza de la siguiente manera:

RIESGO RESIDUAL = VALOR DE LA PROBABILIDAD (considerando controles existentes) * VALOR DEL IMPACTO (considerando controles existentes)

Para llevar a cabo el cálculo del riesgo residual se debe ingresar al archivo llamado 4.HERRAMIENTA RIESGOS, y completar la pestaña llamada 3-RIESGO_RESIDUAL.

Acá se procederá a evaluar el riesgo inherente que se mantiene aún con el control existente al riesgo evaluado.

Los campos manuales y automáticos de esta pestaña son los siguientes:

- RIESGO (Columna A): Se compone de cada uno de los riesgos identificados por el usuario, al cual se le realizará el análisis de riesgo residual. Este es un campo **no** editable.
- DETALLE (Columna B): Consiste en la descripción detallada de cada uno de los riesgos de la columna A. Este es un campo **no** editable.
- CLASIFICACIÓN_1 (Columna C): Se refiere a la primera categoría de la clasificación de riesgos, la cual es la más general. Este es un campo **no** editable.
- CLASIFICACIÓN_2 (Columna D): campo automático. Consiste en subdivisiones de las clasificaciones de riesgo generales del punto anterior. Este es un campo **no** editable. Ver Imagen 1. Estructura de riesgos CODEA.
- ¿EXISTEN CONTROLES? (Columna E): Consiste en especificar si la entidad cuenta con controles o no para cada riesgo. Este es un campo **editable**.
- CONTROLES EXISTENTES (Columna F): Descripción detallada de los controles existentes para dicho riesgo. Este es un campo **editable**.

- VALOR_PROBABILIDAD (Columna G): Es el nuevo valor de la probabilidad de que un evento suceda considerando los controles existentes. El valor de la probabilidad de riesgo se encuentra en una escala de 1 a 5, donde el 1 representa riesgo de ocurrencia muy bajo, y 5 siendo una ocurrencia muy altamente probable. Este es un campo **editable**.

  En el campo VALOR_PROBABILIDAD se despliega una lista de valores del 1 al 5. El usuario define el valor de acuerdo con el riesgo analizado. Ver Tabla 1 Valor, categoría y descripción de la probabilidad.

- CATEGORÍA_PROBABILIDAD (Columna H): Consiste en la categoría de probabilidad asignada de acuerdo con el valor asignado por el usuario. Puede ser rara, inusual, poco probable, muy probable o recurrente. Este es un campo **no** editable. Ver Tabla 1 Valor, categoría y descripción de la probabilidad.

- VALOR_IMPACTO (Columna L): Se refiere al nuevo nivel de impacto que asigna el usuario de acuerdo con el riesgo tomando en consideración los controles existentes. Puede tomar valores en una escala de 1 a 5, siendo nivel 1 el más bajo, como categoría menor, y 5 como el nivel más alto, como categoría catastrófica. Este es un campo **no** editable.

  Para definir el VALOR_IMPACTO, se toman en consideración tres factores: impacto operativo (Columna I), impacto legal y regulatorio (Columna J), e impacto de imagen y credibilidad pública (Columna K). Estos campos son **editables**. Ver Tabla 2. Factores que influyen en el impacto.

Para cada uno de los factores se despliega una lista de valores del 1 al 5. El usuario define el valor de acuerdo con el riesgo analizado. Cada factor posee un porcentaje de ponderación. Ver Tabla 3 Valor, categoría y descripción del impacto.

- CATEGORÍA_IMPACTO (Columna M): Consiste en la categoría de impacto asignada de acuerdo con el valor asignado por el usuario. Puede ser menor, bajo, moderado, grave o catastrófico. Este es un campo **no** editable. Ver Tabla 3 Valor, categoría y descripción del impacto.
- RIESGO_RESIDUAL (Columna N): Es el riesgo inherente que permanece aún con la existencia de controles a los riesgos identificados. Este es un campo **no** editable. La fórmula es la siguiente:

RIESGO RESIDUAL = VALOR DE LA PROBABILIDAD (considerando controles existentes) * VALOR DEL IMPACTO (considerando controles existentes)

- CATEGORÍA_RIESGO (Columna O): Es la categoría asignada de acuerdo con el valor de riesgo residual. El cual puede ser clasificado como bajo, moderado, alto y extremo. Este es un campo **no** editable.

Por otra parte, en la 4.HERRAMIENTA RIESGOS, se incluye una pestaña llamada 4-MATRICES, esta pestaña NO es editable, cuenta con el único fin de ilustrar de forma comparativa, los resultados obtenidos del análisis de riesgos y del análisis de riesgo residual, esto mediante mapas de calor y un gráfico comparativo.

Finalmente, en el Site de Valoración de Riesgos, específicamente en la pestaña Riesgo residual, mediante un DataStudio, podrá visualizar los resultados obtenidos de dicho análisis

e interactuar con los mismos, así como, también observar en la pestaña Matrices, las matrices de calor generadas a raíz de los análisis realizados.

4.6 Respuesta al riesgo

La respuesta al riesgo consiste en la cuarta etapa, el objetivo de la misma es, establecer una respuesta a aquellos riesgos que superan la tolerancia al riesgo establecida inicialmente por la institución, de manera que ayude establecer acciones para dar respuesta a los mismo.

En el archivo 4.HERRAMIENTA RIESGOS una vez completado el punto anterior 3-RIESGO RESIDUAL, se procede a ingresar a la pestaña 4-RESPUESTA.

Los campos manuales y automáticos de esta pestaña son los siguientes:

- RIESGO (Columna A): Se compone de cada uno de los riesgos analizados que superan la tolerancia al riesgo establecida por el CODEA. Este es un campo **no** editable.
- DETALLE (Columna B): Consiste en la descripción detallada de cada uno de los riesgos de la columna A. Este es un campo **no** editable.
- CATEGORÍA RIESGO (Columna C): Es la categoría asignada de acuerdo con el valor de riesgo residual. El cual puede ser clasificado como bajo, moderado, alto y extremo. Este es un campo **no** editable.

- RESPUESTA (Columna D): Este es un campo **editable**. La persona encargada de la entidad deberá darle una respuesta al riesgo, tomando en cuenta las cuatro acciones que se pueden ejecutar como respuesta al riesgo y valorando que es lo más factible en cada uno de los casos, para ello a continuación se brinda un detalle de las posibles acciones:
    - **Aceptar el Riesgo**: La entidad decide no ejecutar acciones ya sean preventivas o correctivas de los riesgos y decide aceptar las consecuencias, según la Antología Curso PC-0425 Control Interno y Auditorias Especiales V3.1 2018 pg. 59 generalmente las entidades toman esta acción cuando las "consecuencias son pequeñas y el esfuerzo para mitigarlo o transferirlo es mucho o no es posible dar otro tipo de respuesta"
    - **Transferir el riesgo**: Se da en los casos que existe la posibilidad de "trasladar el impacto total o parcial de un riesgo a un tercero, junto con la responsabilidad por la respuesta" (Antología Curso PC-0425 Control Interno y Auditorias Especiales V3.1, 2018, pg. 59) genera un costo asociado y generalmente hace referencia a seguros, contratos, garantías.
    - **Mitigar el riesgo**: El impacto del riesgo se puede disminuir mitigando sus consecuencias, si se hace realidad, a través de la creación y aplicación de controles que permitan tal fin. (Antología Curso PC-0425 Control Interno y Auditorias Especiales V3.1, 2018, pg. 60)
    - **Prevenir el riesgo**: Se considera una de las mejores acciones ya que hace referencia a un enfoque proactivo, es decir es más sencillo y económico prevenir que posteriormente reparar daños causados. "El riesgo se puede prevenir atacando la causa (fuente) que lo produce para reducir su

probabilidad de ocurrencia". (Antología Curso PC-0425 Control Interno y Auditorias Especiales V3.1, 2018, pg. 60)

- CONTROL SUGERIDO (Columna E): Es un control sugerido viene de manera automática del archivo de 1.INVENTARIO DE RIESGOS, y tiene como fin solventar las afectaciones de los riesgos, en este caso la entidad valora si el control es acorde a sus objetivos y si se puede implementar. La entidad para el establecimiento de controles debe tomar en cuenta cuales son las características requeridas para un efectivo sistema de administración de los riesgos su propósito y las acciones a implementar por la entidad. Este es un campo **no** editable.
- ACEPTA CONTROL SUGERIDO (Columna F): En línea con el punto anterior, el encargado deberá valorar si el control que sugiere la herramienta de manera automática puede ejecutarse en la entidad, en caso de ser positivo deberá dar respuesta "Si" en caso contrario "No". Este es un campo **editable**.

- INDIQUE CONTROL A IMPLEMENTAR (Columna G): Esta columna, está directamente relacionada con el punto anterior, si la respuesta es que la entidad "Si" acepta el control sugerido, este espacio se debe dejar en blanco, debido a que ya se tiene dado el control que se implementara, en caso contrario, si la respuesta es que la entidad "No" acepta el control sugerido, la persona encargada deberá proponer el control que se implementara como respuesta al riesgo. Este es un campo **editable**.
- TIPO DE CONTROL (Columna H): Este es un campo **editable**. Hace referencia al tipo de control que la entidad determina, ya sea el sugerido de manera automática o

el propuesto por el encargado de este proceso, a continuación, se detallan los tipos de control

- **Control detectivo**: un control diseñado para descubrir un evento no deseado o resultado después de que haya ocurrido el procesamiento inicial pero antes de que haya concluido el objetivo final. (COSO, 2013, p.140)
- **Control preventivo**: Un control diseñado para evitar un evento o resultado no deseado en el momento de la ocurrencia inicial. (COSO, 2013, p.142)
- **Control Correctivo**: cuando los controles anteriores no son suficientes y se presenta la falla, se debe corregir el error específico y asegurar la no repetición de este hecho.

- RESPONSABLE ASIGNADO (Columna I): Esta columna hace referencia a la asignación de una persona interna de la entidad que sea dueño del control, quien tendrá la responsabilidad de velar por su ejecución y cumplimiento adecuado del mismo, así como de informar cualquier aspecto relevante. Este es un campo **editable**.

Finalmente, en el Site de Valoración de Riesgos, específicamente en la pestaña Respuesta a los riesgos, mediante un DataStudio, podrá visualizar los resultados obtenidos de esta etapa e interactuar con los mismos.

4.7 Comunicación de resultados al jerarca

Esta corresponde a la última etapa, luego del proceso de valoración de riesgos, se procede a revisar y documentar la información, para que de esta manera se le informe al Jerarca del CODEA los resultados más relevantes, así como las acciones definidas para abordarlos.

Los resultados se informarán como se describe a continuación:

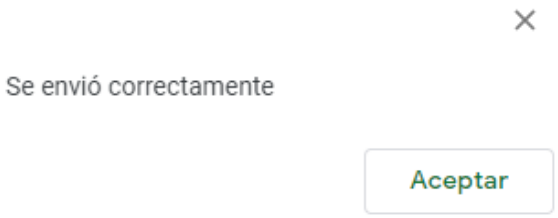
1. Se comentarán en una reunión con el Jerarca de la entidad.
2. Se presentará un expediente del proceso de valoración de riesgos realizado con el objetivo de determinar las acciones correspondientes para la administración de riesgos.
3. Una vez discutido el expediente, se deberán girar las instrucciones necesarias a los responsables designados en la implementación de los controles de tratamiento a los riesgos.

Para esta fase, la 4.HERRAMIENTA RIESGOS incluye una programación que permite generar un *reporte automatizado de los análisis realizados*, los pasos para generar este reporte son los siguientes:

1) Ubicar la opción "Herramienta riesgos" en la parte superior del archivo 4.HERRAMIENTA RIESGOS.
2) Verificar el correo digitado en la pestaña CONF en la celda B7.
3) Dar clic a la opción "Enviar resultados del análisis por correo". Si la herramienta le solicita permisos entonces deberá brindarlos según las instrucciones que le muestre.
4) Una vez que dio clic a la opción "Enviar resultados del análisis por correo", se desplegará el siguiente mensaje:

Imagen X:

Aviso de envío correcto del reporte al correo



5) Una vez realizado los pasos anteriores, también se podrá ubicar el reporte final del proceso de valoración de riesgos en la carpeta llamada 01.REPORTES y en el Site de Valoración de Riesgos, específicamente en la pestaña Comunicación de resultados.

Anexo M.

Inventario de Riesgos suministrado al CODEA con la Herramienta de Evaluación de Riesgos Transitoria

}	Tema	Riesgo	Detalle	Pregunta de identificación	Control sugerido
Riesgos del entorno	General	Requerimiento de la población objetivo	Las necesidades y deseos de la población objetivo cambian, y la organización no es consciente de ello; por ejemplo, mayor demanda por una entrega más rápida de productos y servicios. La población objetivo es la receptora del valor público que la entidad genera.	¿El CODEA realiza diagnósticos de actualización de necesidades e intereses de la población objetivo?	Realizar diagnósticos de necesidades de la población objetivo del CODEA
Riesgos del entorno	General	Incumplimiento de objetivos asignados por Ley	Fallar en el cumplimiento de los objetivos establecidos por Ley y por ende en la generación de valor público.	¿El CODEA se asegura de alcanzar sus objetivos según lo designado por Ley?	Generar indicadores que permitan al CODEA medir su cumplimiento de objetivos
Riesgos del entorno	General	Disponibilidad de recursos	Acceso insuficiente a los recursos, amenaza la capacidad de la institución de crecer y ejecutar su modelo de negocios.	¿El CODEA cuenta con un plan de acción ante eventuales limitaciones de recursos? (Humanos, monetarios, tecnológicos etc.)	Realizar la adecuada preparación y presentación de informes referentes al desempeño y disponibilidad de los recursos (humanos, materiales y presupuestarios).
Riesgos del entorno	General	Regulatorio	Regulaciones cambiantes amenazan la posición competitiva de la institución y su capacidad para operar eficazmente.	¿El CODEA se mantiene actualizado respecto a los posibles cambios que se puedan originar en la normativa?	Definir un procedimiento de comunicación e información que permita mantener informado a todo el personal del CODEA sobre actualizaciones y nueva normativa que les compete.
Riesgos del entorno	General	Catástrofes	Un desastre significativo amenaza la habilidad de la organización de sostener sus operaciones en funcionamiento, proporcionar servicios y productos esenciales.	¿El CODEA cuenta con un plan de acción que les permita identificar las principales amenazas que les afecta, así como las acciones que debería llevar a cabo ante las mismas?	Realizar un plan de acción para detectar principales amenazas de origen externo.
Riesgos de procesos	Gobierno	Riesgo de Cultura Organizacional	Riesgo a que la organización presente un comportamiento disfuncional debido a que los mandos altos (Junta Directiva y Dirección Administrativa) no quieran tomar riesgos o tomen riesgos más allá del normal.	¿Se comunican, priorizan y realizan acciones correctivas cuando se identifican riesgos claves?	Establecer e implementar un Código de Ética que permita la ejecución de acciones correctivas ante comportamientos disfuncionales del personal.
Riesgos de procesos	Tecnologías de la información	Incidentes de TI	El no establecer esquemas de clasificación de incidentes y peticiones de servicio limita a la entidad a establecer acciones de mejora eficientes y oportunas.	¿Se definen esquemas de clasificación de incidentes y peticiones de servicio de TI?	Definir esquemas de clasificación de incidentes y peticiones de servicio.
Riesgos de procesos	Tecnologías de la información	Riesgo de ciberseguridad	La ausencia de medidas efectivas, preventivas, de detección y corrección puede poner en riesgo la protección de los sistemas información y tecnología de la entidad ante softwares maliciosos.	¿Se implementar y mantienen efectivas medidas, preventivas, de detección y corrección para proteger los sistemas de información y tecnología del software malicioso?	Implementar y mantener efectivas medidas, preventivas, de detección y correctivas (especialmente parches de seguridad actualizados y control de virus) en el CODEA para proteger los sistemas de información y tecnología del software malicioso (por ejemplo, virus, gusanos, software espía –spyware- y correo basura).

Riesgos de procesos	Gobierno	Riesgo comportamiento ético	La organización, a través de sus acciones o la inacción, demuestra que no tiene el compromiso de un comportamiento institucional ético y responsable.	¿La organización, a través de la acción, demuestra que tiene el compromiso de un comportamiento institucional ético y responsable?	Establecer e implementar un Código de Ética que permita la ejecución de acciones correctivas ante comportamientos disfuncionales del personal.
Riesgos de procesos	Gobierno	Riesgo de efectividad	Los niveles superiores de la entidad no participan de manera constructiva en la gestión, además no supervisan en forma anticipada, proactiva e interactiva las actividades de la institución y los asuntos, con integridad, visión, sentido común e independencia incuestionable.	¿Los niveles superiores de la entidad participan de manera constructiva en la gestión de riesgos, además supervisan en forma anticipada, proactiva e interactiva las actividades de la institución y los asuntos, con integridad, visión, sentido común e independencia incuestionable?	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.
Riesgos de procesos	Gobierno	Riesgo de planificación de la sucesión	El talento de liderazgo dentro de la organización no está suficientemente desarrollado para proporcionar una sucesión ordenada en el futuro.	¿El CODEA cuenta con un plan de sucesión de personal?	Generar un plan de sucesión de personal.
Riesgos de procesos	Reputación	Riesgo de imagen	Riesgo de que el CODEA no satisfaga las expectativas y necesidades de su población objetivo.	¿El CODEA realiza frecuentemente diagnósticos de satisfacción de su población objetivo?	Establecer una metodología para realizar diagnósticos de satisfacción de la población objetivo del CODEA.
Riesgos de procesos	Operacionales	Recursos Humanos	Falta de conocimientos, habilidades y experiencias requeridas entre el personal clave de la institución, amenaza la ejecución de su modelo de negocios y el logro de sus objetivos.	¿El personal del CODEA cuenta con los conocimientos, habilidades y experiencias requeridas para la generación de valor público y el logro de sus objetivos?	Establecer e implantar un Plan de Capacitación Institucional, así como un sistema de medición del desempeño.
Riesgos de procesos	Operacionales	Capital de Conocimiento	Los procesos por capturar e institucionalizar el aprendizaje a través de la institución son inexistentes o ineficaces, produciendo un tiempo de respuesta lento, costos altos, errores repetidos, lento desarrollo de competencias, restricciones en el crecimiento y empleados desmotivados.	¿El CODEA realiza capacitaciones al personal o implementa otros mecanismos que le permita capitalizar el conocimiento a nivel institucional?	Establecer e implementar un Plan de Capacitación Institucional.
Riesgos de procesos	Operacionales	Capacidad	La capacidad insuficiente amenaza la habilidad de la organización de cubrir las demandas de su población objetivo.	¿El CODEA ha evaluado su capacidad para cubrir posibles demandas de servicios y/o productos de la población objetivo?	Realizar un análisis de la capacidad del CODEA para hacer frente a eventuales procesos legales.
Riesgos de procesos	Operacionales	Tiempo de Ciclo	Las actividades innecesarias amenazan la capacidad de la institución de desarrollar, producir y entregar bienes o servicios de manera oportuna.	¿El CODEA tiene debidamente planificado sus procesos y la duración de cada uno de estos?	Desarrollar e implementar una estrategia que permita una mayor eficiencia en el desarrollo, producción y entrega de servicios.
Riesgos de procesos	Humanos	Salud del personal	Alude al bienestar personal y su relación con el ambiente de trabajo y las normas y prácticas de	¿El CODEA cuenta con prácticas de seguridad ocupacional? (Ejemplos:	Desarrollar e implementar un manual de salud ocupacional.

			seguridad ocupacional a lo interno y externo de la institución, de conformidad con las regulaciones jurídicas y técnicas que rigen esta materia.	Planes de emergencia evacuación, sistemas contra incendios, implementos seguridad trabajos requeridos etc.)	
Riesgos de procesos	Humanos	Prácticas de seguridad	El no contar con prácticas de seguridad, la institución se expone a sanciones por daños, pérdida de reputación y otros costos.	¿El CODEA cuenta con prácticas de seguridad que aseguren el bienestar de la población que hace uso de sus instalaciones?	Desarrollar e implementar un protocolo de seguridad sobre las personas usuarias de las instalaciones del CODEA.
Riesgos de procesos	Operacionales	Abastecimiento	Fuentes limitadas de recursos de materias primas y profesionales, amenazan la habilidad de la organización para brindar servicios y productos de calidad y de manera oportuna.	¿El CODEA realiza análisis que le permitan determinar si los recursos con los que cuenta son suficientes para generar sus servicios?	Realizar un análisis de priorización de servicios.
Riesgos de procesos	Operacionales	Alianzas	Alianzas, afiliaciones y otras relaciones externas ineficientes o inefectivas afectan la capacidad de la organización para cumplir sus objetivos.	¿Los convenios con patrocinadores o con proveedores se revisan para evaluar su rendimiento y beneficios?	Generar un plan de mejoramiento en el proceso de comunicación formal y de revisión de términos contractuales y de servicio con los proveedores.
Riesgos de procesos	Operacionales	Cumplimiento	El incumplimiento con los requerimientos de la población objetivo, políticas y procedimientos organizacionales, leyes y regulaciones pueden producir baja calidad, altos costos, retrasos innecesarios, penalidades, multas, etc.	¿El CODEA se asegura de cumplir con los requerimientos de su población objetivo, políticas y procedimientos organizacionales, leyes y regulaciones?	Desarrollar e implementar una estrategia de identificación de cumplimiento de requerimientos.
Riesgos de procesos	Operacionales	Tributario	El no compilar y considerar información tributaria relevante, puede producir incumplimiento o consecuencias impositivas adversas, que podrían evitarse si se estructuran las transacciones de manera diferente.	¿El CODEA se asegura de contar con personal calificado que permita cumplir con los requerimientos tributarios de forma adecuada?	Desarrollar e implementar acciones que permita al personal de CODEA una asesoría sobre el manejo tributario.
Riesgos de procesos	Operacionales	Medio Ambiente	Actividades dañinas al medio ambiente, exponen a la organización a obligaciones por daños personales, daños materiales, costo de reparación y remoción, indemnizaciones reparatorias, etc.	¿El CODEA se asegura de no generar actividades que impacten negativamente el medio ambiente tomando en cuenta las afectaciones legales que implican?	Desarrollar e implementar un Plan de Gestión Ambiental
Riesgos de procesos	Operacionales	Riesgo de no ejercer un adecuado seguimiento a los recursos transferidos a los Comités Comunales	Mal manejo de recursos públicos que ponen en riesgo el cumplimiento de los objetivos institucionales	¿El CODEA se asegura que los recursos transferidos a los Comités Comunales sean utilizados para los fines destinados?	Desarrollar e implementar un procedimiento de monitoreo de recursos transferidos a Comités Comunales. (Informes de ejecución, liquidaciones etc.)
Riesgos de procesos	Estratégicos	Estabilidad	Uniformidad y estandarización en la aplicación de los procesos y procedimientos e instructivos de trabajo.	¿El CODEA cuenta con un Manual de Procesos debidamente actualizado, formalizado y comunicado a sus funcionarios?	Desarrollar e implementar un manual de procesos
Riesgos de procesos	Social	Medios de comunicación	Capacidad de incidencia en la imagen institucional que pueden tener los diversos medios de comunicaciones colectiva en la gestión del CODEA.	¿Se han determinado los impactos de los comentarios en medios de comunicación colectivos en la gestión de CODEA?	Realizar un análisis histórico de noticias que involucren el CODEA y su nivel de impacto.

Riesgos de procesos	Social	Cambios demográficos	Relacionados con la estructura de la población y cambios en esta (edad, sexo, inmigración, discapacidad, etc.-.) que puedan incidir en el accionar de la institución.	¿El CODEA cuenta con estudios demográficos actualizados del cantón de Alajuela que pueda ser utilizado en su planificación?	Desarrollar acciones que permitan asegurar información demográfica actualizada del cantón de Alajuela
Riesgos de procesos	Financieros	PRECIO - Interés	Movimientos significativos en las tasas de interés exponen a la institución a costos financieros, menores rendimientos en las inversiones o menores valores en los activos.	¿Se realizan análisis y estudios de los movimientos en la tasa de interés, que puedan incidir en la gestión del CODEA?	Realizar análisis y estudios de los movimientos en la tasa de interés, que puedan incidir en la gestión del CODEA.
Riesgos de procesos	Financieros	PRECIO - Precio de las materias primas	Las fluctuaciones en los precios de los materiales exponen a la institución a invertir más recursos para adquirirlos.	¿Se realizan análisis y estudios de las fluctuaciones en los precios de las materias primas que adquiere el CODEA?	Realizar análisis y estudios de las fluctuaciones en los precios de las materias primas que adquiere el CODEA.
Riesgos de procesos	Financieros	Flujo de caja	Desde la programación y manejo del flujo de caja de frente al logro de los cometidos institucionales y con la debida atención del marco normativo aplicable.	¿El flujo de caja es administrado de manera adecuada, por personal competente y tomando en cuenta las necesidades del CODEA y el marco normativo?	Desarrollar e implementar un proceso/manual/metodología de administración del flujo de caja del CODEA.
Riesgos de procesos	Dirección	Liderazgo	El personal de la organización no es liderado eficazmente, lo que puede resultar en una falta de dirección.	¿Los puestos de jefatura cuentan con medidas de desempeño y liderazgo que se implementen periódicamente?	Manual de puestos y procesos. Realizar capacitaciones internas sobre liderazgo Establecer medidas de desempeño y liderazgo a los puestos de jefatura
Riesgos de procesos	Dirección	Autoridad/Límite	Líneas de autoridad no efectivas, pueden causar que los superiores jerárquicos y su personal hagan cosas que no deben hacer o no dejen de hacer lo que deberían. El no establecer o verificar el cumplimiento de límites en las acciones del personal, puede causar que los empleados cometan actos no autorizados o no éticos, o asuman riesgos no autorizados o inaceptables.	¿Se establece o verifica el cumplimiento de límites en las acciones del personal?	Manual de puestos y procesos. Realizar capacitaciones internas sobre liderazgo Establecer medidas de desempeño y liderazgo a los puestos de jefatura
Riesgos de procesos	Dirección	Disposición al Cambio	El personal de la institución no puede implementar mejoras a procesos y productos/servicios lo suficientemente rápido, como para guardar el paso con los cambios en el mercado.	¿Se analizan cambios en el mercado que puedan significar mejoras en procesos y actividades del CODEA?	Realizar diagnósticos de cambios que se dan en el mercado que puedan tener impacto en la mejora de los procesos y actividades del CODEA (FODA)
Riesgos de procesos	Dirección	Comunicaciones	Canales de comunicación ineficaces, pueden producir mensajes que son inconsistentes con las responsabilidades autorizadas o los indicadores de performance establecidas.	¿Los canales de comunicación permiten que se logre una recepción adecuada del mensaje?	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.
Riesgos de procesos	Tecnologías de la información	Relevancia	Que el manejo y control de la información recibida, procesada y generada tenga plena justificación	¿Las TI del CODEA aseguran que la información recibida, procesada y generada sea de valor para el desarrollo	Validar con los proveedores que las TI cuenten con las especificaciones necesarias para generar los reportes actuales y futuros.

			en la utilidad para realizar los procesos y tomar decisiones.	de los diferentes procesos y toma de decisiones?	
Riesgos de procesos	Tecnologías de la información	Integridad	Todos los riesgos asociados con la autorización, integridad y exactitud de las transacciones que son ingresadas, procesadas, resumidas y reportadas por los distintos sistemas aplicativos de la institución.	¿Las TI permiten que todos los riesgos asociados con la autorización, integridad y exactitud de las transacciones son ingresados, procesadas, resumidas y reportadas de manera certera y adecuada?	Desarrollar un procedimiento de control del procesamiento de la información.
Riesgos de procesos	Tecnologías de la información	Acceso	El no restringir el acceso a la información (datos o programas) adecuadamente, puede producir el conocimiento y uso no autorizado de información confidencial. La excesiva restricción del acceso a la información puede impedir que el personal realice sus tareas asignadas.	¿Los sistemas de información permiten asegurar el acceso únicamente a personal autorizado?	Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión.
Riesgos de procesos	Tecnologías de la información	Disponibilidad	La no disponibilidad de información importante cuando se le necesita amenaza la continuidad de las operaciones y procesos críticos de la organización.	¿El CODEA establecer y mantiene un Sistema de Gestión de Seguridad de la Información (SGSI) que proporcione un enfoque estándar, formal y continuo a la gestión de seguridad para la información, tecnología y procesos estén alineados con los objetivos institucionales?	Establecer y mantener un Sistema de Gestión de Seguridad de la Información (SGSI) que proporcione un enfoque estándar, formal y continuo a la gestión de seguridad para la información, tecnología y procesos estén alineados con los objetivos institucionales.
Riesgos de procesos	Tecnologías de la información	Infraestructura	El riesgo que la institución no tenga la infraestructura de tecnología de información (p.e. hardware, redes, software, procesos y personal) que necesita para soportar eficazmente los requerimientos de información de negocios actuales y futuros del negocio, de manera eficaz, costo efectiva y bien controlada.	¿Los sistemas de información permiten cumplir con las necesidades diarias de CODEA en todas sus operaciones?	Realizar periódicamente diagnósticos de necesidades de TI.
Riesgos de procesos	Tecnologías de la información	Negocios electrónicos	Todo lo referido a las transacciones electrónicas, documentos electrónicos, firma digital y su impacto en el control de los procesos en los que se aplica.	¿Existe algún lineamiento que establezca el manejo adecuado de las transacciones electrónicas, documentos electrónicos y firma digital?	Existencia e implementación de un lineamiento que establezca el manejo adecuado de las transacciones electrónicas, documentos electrónicos y firma digital
Riesgos de procesos	Integridad	Fraude Gerencial	La presentación intencional de estados financieros incorrectos, o de información incorrecta sobre las capacidades o intenciones, pueden afectar adversamente las decisiones de las partes relacionadas.	¿Se identifican y evalúan factores de riesgo de fraude relacionados con la emisión de información financiera fraudulenta?	Evaluación anual de factores de fraude por oportunidad, presión y racionalización
Riesgos de procesos	Integridad	Fraude de Empleados/Terceros	Actividades fraudulentas perpetradas por empleados, clientes o proveedores, agentes, corredores o terceros contra la institución para beneficio personal (e.g., apropiación de activos físicos, financieros o recursos de información) exponen a la	¿Se identifican factores de fraude para todos los niveles de la entidad?	Evaluación anual de factores de fraude por oportunidad, presión y racionalización

			organización a la pérdida financiera.		
Riesgos de procesos	Integridad	Actos Ilegales	Actos ilegales cometidos por gerentes o empleados exponen a la institución a multas, sanciones, y pérdida de clientes, ganancias y reputación, etc.	¿Se identifica factores de fraude para todos los niveles de la entidad?	Evaluación anual de factores de fraude por oportunidad, presión y racionalización
Riesgos de procesos	Integridad	Uso No Autorizado	El uso no autorizado de los activos físicos, financieros e información de la institución por los empleados u otros la exponen al gasto innecesario de recursos y la pérdida financiera.	¿Los activos están debidamente asignados a sus responsables de su uso?	Inventario de activos que contenga plaqueo y responsable.
Riesgos de procesos	Ambiental	Servicios básicos	No contar con una capacidad de respuesta institucional ante eventuales recortes en el suministro de servicios básicos: agua, luz, telefonía, servicios médicos, seguridad.	¿Se cuenta con planes de contingencia o de emergencia ante eventuales recortes de suministros básicos: agua, luz, telefonía, servicios médicos, seguridad??	Diseñar un plan anual de contingencia ante eventos adversos
Riesgos de información para la toma de decisiones	Información operativa	Medición Operativa	Indicadores no financieros inexistentes, irrelevantes y/o no confiables pueden causar evaluaciones y conclusiones erróneas acerca de la performance operativa.	¿Se han desarrollado indicadores de gestión para la toma de decisiones y mejoramiento continuo del CODEA?	Supervisar los indicadores clave y sus métricas para determinar el grado en que el negocio está generando valor público. Generar sus respectivos reportes o informes.
Riesgos de información para la toma de decisiones	Información operativa	Alineamiento	El no alinear los objetivos de los procesos y los objetivos estratégicos institucionales pueden producir actividades antagónicas y descoordinadas en toda la organización.	¿Los objetivos establecidos mediante el Plan Anual Operativo se encuentran alineados con los objetivos del Plan Estratégico Institucional?	Desarrollar e implementar un Plan Estratégico.
Riesgos de información para la toma de decisiones	Información de gestión	Presupuesto y Planeamiento	Información de planeamiento y presupuesto inexistente, poco realista, irrelevante o no confiable puede causar decisiones y conclusiones financieras incorrectas.	¿Existe y se implementa una metodología/procedimiento, debidamente formalizada, sobre el proceso de elaboración del Plan Anual Operativo y el Presupuesto?	Existencia de una metodología debidamente documentada sobre el proceso de elaboración del Plan Anual Operativo y el Presupuesto
Riesgos de información para la toma de decisiones	Información de gestión	Información Contable	Énfasis excesivo en la información de contabilidad financiera para administrar el negocio, puede producir la manipulación de resultados.	¿Se audita la información financiera?	Contratación de servicios de auditoría
Riesgos de información para la toma de decisiones	Información de gestión	Evaluación del Reporte Financiero	No compilar información externa e interior relevante y confiable para evaluar, si se requieren ajustes o revelaciones en los estados financieros, puede producir la emisión de informes financieros engañosos a inversionistas y stakeholders externos.	¿Se evalúa que la información a presentar mediante informes financieros no requiera ajustes o revelaciones que en caso de su omisión puedan comprometer su relevancia y confiabilidad?	Establecer un proceso de verificación y evaluación que asegure la relevancia y confiabilidad de la información a presentar mediante informes financieros.
Riesgos de información para la toma de decisiones	Información de gestión	Evaluación de Inversiones	La falta de información relevante y/o confiable que soporte las decisiones de inversión y enlace los riesgos asumidos con el capital en	¿Se presenta a la junta directiva informes sobre el desarrollo de los programas, indicadores de gestión e inversiones en	Presentación obligatoria anual de informe de riesgos e indicadores a la Junta Directiva

			riesgo, puede producir malas decisiones de inversión.	infraestructura deportiva para la toma de decisiones?	
Riesgos de información para la toma de decisiones	Información de gestión	Reporte Regulatorio	El reporte incompleto, inexacto y/o inoportuno de información financiera y operativa requerida por entidades regulatorias, pueden exponer a la institución a multas, penalidades y sanciones.	¿Existe algún sistema que permita generar reportes oportunos y confiables sobre la información financiera del CODEA?	Realizar revisiones periódicas del Sistema de Gestión de Seguridad de la Información (SGSI), incluyendo aspectos de políticas, objetivos y prácticas de seguridad del SGSI.
Riesgos de información para la toma de decisiones	Información estratégica	Monitoreo del Entorno	La falta de monitoreo del entorno o la formulación de supuestos poco realistas o erróneos sobre los riesgos del entorno puede causar que la organización retenga estrategias a pesar de que se hayan vuelto obsoletas.	¿Se aplica regularmente un FODA (PEST) del CODEA?	Realizar una evaluación anual de los factores del entorno y su incidencia en el CODEA
Riesgos de información para la toma de decisiones	Información estratégica	Modelo de Negocios	La institución tiene un modelo de negocios obsoleto, y no lo reconoce y/o falta la información necesaria para hacer una evaluación del modelo actual y construir un caso de negocios convincente para modificarlos oportunamente.	¿El CODEA cuenta con modelo de negocio debidamente documentado y actualizado?	Establecer una definición clara y documentada del modelo de negocio del CODEA.
Riesgos de información para la toma de decisiones	Información estratégica	Estructura Organizacional	El superior jerárquico carece de la información necesaria para evaluar la efectividad de la estructura orgánica de la institución, lo que amenaza su capacidad para el cambio o para lograr sus estrategias de largo plazo. La estructura no sustenta las estrategias de negocio.	¿Se cuenta con un Reglamento Autónomo de Servicios que defina la estructura orgánica de la entidad y las funciones que debe llevar a cabo cada una de sus unidades?	Diseñar e implementar un Reglamento Autónomo de Servicios que defina la estructura orgánica de la entidad y las funciones que debe llevar a cabo cada una de sus unidades
Riesgos de información para la toma de decisiones	Tecnologías de la información	Riesgo de procesamiento de la información	El no identificar, documentar, priorizar y mitigar los riesgos funcionales y técnicos relativos al procesamiento de la información limita a la entidad a establecer acciones de mejora eficientes y oportunas.	¿Se identifican, documentan, priorizan y mitigan los riesgos funcionales y técnicos relativos a procesamiento de la información y asociados con los requerimientos de la institución?	Identificar, documentar, priorizar y mitigar los riesgos funcionales y técnicos relativos a procesamiento de la información y asociados con los requerimientos de la institución.
Riesgos de información para la toma de decisiones	Requerimientos de información	Oportunidad de la información	Se debe identificar, priorizar, especificar y acordar los requerimientos de información del CODEA, funcionales, técnicos y de control que cubra el alcance/entendimiento de todas las iniciativas necesarias para alcanzar los resultados esperados.	¿Se Identifican, priorizan, especifican y acuerdan los requerimientos de información del CODEA, funcionales, técnicos y de control que cubra el alcance/entendimiento de todas las iniciativas necesarias para alcanzar los resultados esperados.	Identificar, priorizar, especificar y acordar los requerimientos de información del CODEA, funcionales, técnicos y de control que cubra el alcance/entendimiento de todas las iniciativas necesarias para alcanzar los resultados esperados.
Riesgos de información para la toma de decisiones	Requerimientos de información	Riesgo de acceso a la información	Se debe organizar la información basándose en criterios de clasificación, identificar y crear relaciones significativas entre elementos de información y facilitar el uso de la información, así como identificar propietarios y definir e implementar niveles de acceso a los recursos de información.	¿Existe un sistema de clasificación de la información que facilite su uso, así como identificación propietarios, definición e implementación de niveles de acceso?	Organizar la información basándose en criterios de clasificación, identificar y crear relaciones significativas entre elementos de información y facilitar el uso de la información, así como identificar propietarios y definir e implementar niveles de acceso a los recursos de información.

Riesgos de información para la toma de decisiones	Información estratégica	Asignación de Recursos	Un proceso de asignación de recursos e información de soporte inadecuados puede generar que la institución desarrolle una gestión ineficiente hacia el cumplimiento de sus objetivos.	¿Existe un proceso documentado de asignación de recursos en donde se contemple las necesidades de cada una de las unidades del CODEA y su alineación con los objetivos estratégicos de la entidad?	Diseñar e implementar un proceso documentado de asignación de recursos en donde se contemple las necesidades de cada una de las unidades del CODEA y su alineación con los objetivos estratégicos de la entidad.
Riesgos de información para la toma de decisiones	Información estratégica	Planeamiento	Necesidad de contar con una planificación estratégica que permita a la institución formular planes operativos anuales alineados con la misión, visión y objetivos a cumplir a mediano y a largo plazo.	¿El CODEA cuenta con Plan Estratégico debidamente documentado y actualizado según con los requerimientos del MIDEPLAN?	Diseñar un Plan Estratégico debidamente documentado y actualizado según con los requerimientos del MIDEPLAN.
Riesgos de información para la toma de decisiones	Información pública	Riesgo Evaluación de Control Interno	Si no se acumula suficiente información relevante y confiable, para evaluar la eficacia del diseño y funcionamiento del control interno sobre los informes financieros, dando lugar a afirmaciones inexactas por la administración en el informe de control interno.	¿Se tienen identificados las deficiencias de control (Carta a la Gerencia) que puedan generar incorrecciones materiales en los Estados Financieros de CODEA?	Ejecutar las recomendaciones surgidas mediante informes de auditorías externas mediante planes de acción.

Anexo N.

Herramienta de Evaluación de Riesgos Transitoria suministrada al CODEA

¡Bienvenido al sistema de valoración de riesgos del CODEA!

Antes de iniciar se le solicita leer lo siguiente:

1

Debe considerar que este sistema de valoración de riesgos está diseñado con el fin de identificar riesgos por medio de preguntas que contienen asociado un riesgo, su respectivo detalle y clasificación. Y además, un control sugerido para dar respuesta a dicho riesgo.

2

Si desea agregar y/o modificar riesgos, deberá hacer los ajustes en el Inventario de Riesgos, siempre y cuando se **RESPETE** lo indicado en la Guía elaborada para este sistema.

3

Debe llenar sus datos en la pestaña llamada CONFIG de la Herramienta de Riesgos. En especial los siguientes:

- RESPONSABLE
- FECHA _INICIO
- TOLERANCIA_RIESGO
- CORREO_REPORTE

Al finalizar deberá completar el campo FECHA_FINAL y verificar el asunto y cuerpo de correo a enviar.

4

No olvide que la Herramienta de Riesgos **permite enviar un reporte final al correo**, así como guardar una copia de dicho reporte en la carpeta 01.REPORTES **para su respectiva documentación**.

5

Finalmente, mediante este Site podrá visualizar DataStudios que permiten al usuario interactuar con los resultados obtenidos en cada una de las fases del proceso de valoración de riesgos.

NOTA: La información del DataStudio se actualizará automáticamente al comenzar un nuevo proceso de valoración de riesgos.

CODEA

Identificación de riesgos

Para realizar el proceso de identificación de riesgos debe completar el siguiente formulario.

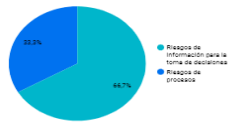
Resultados identificación de riesgos

RIESGO | CLASIFICACION_1 | CLASIFICACION_2

RIESGO	DETALLE	CLASIFICACION_1	CLASIFICACION_2
1. Estructura Organizacional	El superior jerárquico carece de la información necesaria para evaluar la efectividad de la estructura orgánica de la institución, lo que amenaza su capacidad para el cambio o para lograr sus estrategias de largo plazo. La estructura no sustenta las estrategias de negocio.	Riesgos de información para la toma de decisiones	Información estratégica
2. Modelo de Negocios	La institución tiene un modelo de negocios obsoleto, y no lo reconoce y/o falta la información necesaria para hacer una evaluación del modelo actual y construir un caso de negocios convincente para modificarlos oportunamente.	Riesgos de información para la toma de decisiones	Información estratégica
3. Capital de Conocimiento	Los procesos por capturar e institucionalizar el aprendizaje a través de la institución son inexistentes o ineficaces, produciendo un tiempo de respuesta lento, costos altos, errores repetidos, lento desarrollo de competencias, restricciones en el crecimiento y empleados desmotivados.	Riesgos de procesos	Operacionales

1 - 3 / 3

Riesgos según clasificación 1



Riesgos según clasificación 2

CODEA

Análisis de riesgos

Para realizar el análisis de riesgos por favor proceda a completar la pestaña **2-ANALISIS**.

Resultados análisis de riesgos

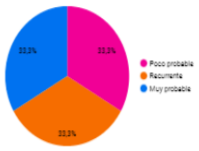
RIESGO | CLASIFICACION_1 | CLASIFICACION_2

PROBABILIDAD | IMPACTO | RIESGO INHERENTE

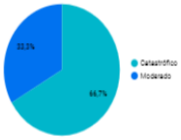
RIESGO	DETALLE	PROBABILIDAD	IMPACTO	RIESGO_INHERENTE
1. Modelo de Negocios	La institución tiene un modelo de negocios obspleto, y no lo reconoce y/o falta la información necesaria para hacer una evaluación del modelo actual y construir un caso de negocios convincente para modificarlos oportunamente.	5	5	25
2. Estructura Organizacional	El superior jerárquico carece de la información necesaria para evaluar la efectividad de la estructura orgánica de la institución, lo que amenaza su capacidad para el cambio o para lograr sus estrategias de largo plazo. La estructura no sustenta las estrategias de negocio.	3	3	9
3. Capital de Conocimiento	Los procesos por capturar e institucionalizar el aprendizaje a través de la institución son inexistentes o ineficaces, produciendo un tiempo de respuesta lento, costos altos, errores repetidos, lento desarrollo de competencias, restricciones en el crecimiento y empleados desmotivados.	4	5	20

1 - 3 / 3

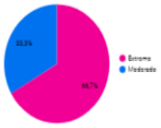
Riesgos según probabilidad



Riesgos según impacto



Riesgos según riesgo inherente



CODEA

Riesgo residual

Para realizar el análisis de riesgos por favor proceda a completar la pestaña **3-RIESGO_RESIDUAL**.

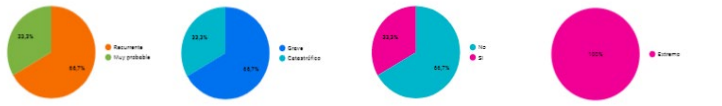
Resultados análisis riesgo residual

RIESGO | CLASIFICACION_1 | CLASIFICACION_2 | ¿EXISTEN CONTROLES? | RIESGO RESIDUAL

	RIESGO	¿EXISTEN CONTROLES?	PROBABILIDAD	IMPACTO	RIESGO_RESIDUAL
1.	Modelo de Negocios	No	Recurrente	Grave	20
2.	Estructura Organizacional	No	Muy probable	Grave	16
3.	Capital de Conocimiento	Si	Recurrente	Catastrófico	25

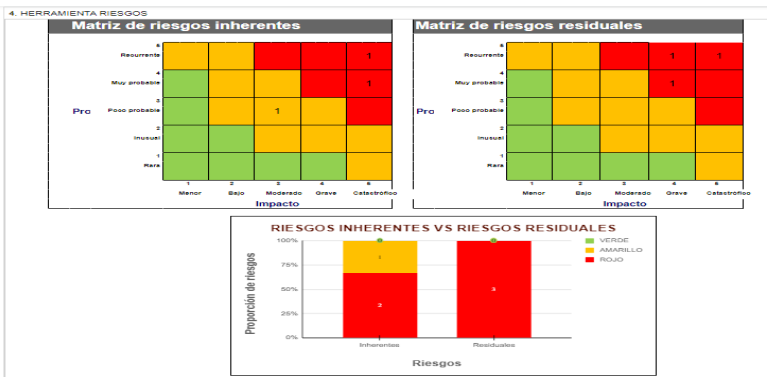
1 - 3 / 3

Riesgos según probabilidad | Riesgos según impacto | Riesgos según existencia de control | Riesgos según riesgo residual



CODEA

Matrices



CODEA

Respuesta a los riesgos

Para realizar el proceso de respuesta a los riesgos por favor proceda a completar la pestaña **4-RESPUESTA**.

Respuesta a los riesgos

RIESGO | RESPUESTA | TIP_CONTROL | RESPONSABLE

	RIESGO	DETALLE	CONTROL	RESPUESTA	TIPO CONTROL	RESPONSABLE ASIGNADO
1.	Modelo de Negocios	La institución tiene un modelo de negocios obsoleto, y no lo reconoce y/o falta la información necesaria para hacer una evaluación del modelo actual y construir un caso de negocios convincente para modificarlos oportunamente.	Establecer una definición clara y documentada del modelo de negocio del CODEA.	Mitigar	Correctivo	Pepita
2.	Estructura Organizacional	El superior jerárquico carece de la información necesaria para evaluar la efectividad de la estructura orgánica de la institución, lo que amenaza su capacidad para el cambio o para	null	null	null	null

1 - 3 / 3

Respuesta | Tipo de control

CODEA

Comunicación de resultados

A continuación los reportes históricos del proceso de valoración de riesgos desarrollados por el CODEA:

Recuerde que al finalizar debe comunicar estos resultados a su superior jerárquico.