UNIVERSIDAD DE COSTA RICA

Facultad de Ciencias Económicas
Escuela de Administración de Negocios

Propuesta de un modelo de Control Interno para el proceso contable de la Junta Administradora del Fondo de Ahorro y Préstamos de la Universidad de Costa Rica (JAFAP) mediado por tecnologías de información, con base en un estudio de COBIT 5 y la normativa vigente aplicada por la Contraloría General de la República.

Seminario de graduación para optar por el grado de Licenciatura en Contaduría Pública

Estudiantes:

Jose Manuel Matew Soto	A53328
Wendy Natalia Mora Mora	B14416
Estefany Rodríguez Gamboa	B15558

Ciudad Universitaria Rodrigo Facio

San José, Costa Rica

Diciembre de 2021

UNIVERSIDAD DE COSTA RICA
FACULTAD DE CIENCIAS ECONÓMICAS

Acta #25-2021

Acta de la Sesión 25-2021 del Comité Evaluador de la Escuela de Administración de Negocios, celebrada el 09 de diciembre del 2021, a las 4:00 p.m., por medio de la Plataforma Zoom, con el fin de proceder a la Exposición del Trabajo Final de Graduación de: **Wendy Natalia Mora Mora, carné B14416, Estefany Rodríguez Gamboa, carné B15558, Jose Manuel Matew Soto, carné A53328** quienes optaron por la modalidad de Seminario de Graduación.

Presentes: Rony Cordero Vargas, representante del Director de la Escuela de Administración de Negocios, quien presidió; Michel Angulo Sosa Tutor; Walter González León, John Rojas Soto lectores, Jose Luis Araya Quesada 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 los 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 un modelo de control interno para el proceso contable de la Junta Administradora del Fondo de Ahorro y Préstamo de la Universidad de Costa Rica (JAFAP) mediado por tecnologías de información, con base en un estudio de COBIT 5 y la normativa vigente aplicada por la Contraloría General de la República".**

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.

(satisfactorias/insatisfactorias)

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.

(Satisfactorio /insatisfactorio)

(Aprobado /no aprobado)

Artículo 6

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

Rony Cordero Vargas
Representante del Director de la Escuela de Administración de Negocios

Wendy Natalia Mora Mora
Carné B14416

Michel Angulo Sosa
Tutor

Estefany Rodríguez Gamboa
Carné B15558

Walter González León
Lector

Jose Manuel Matew Soto
Carné A53328

John Rojas Soto
Lector

Jose Luis Araya Quesada
Secretario de la Sesión

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".

◯ Se aprueba con Distinción

Observaciones: _____

_____

Ciudad Universitaria Rodrigo Facio

San José, 10 de diciembre 2021

Escuela de Administración de Negocios, UCR

Estimados señores:

Por la presente, hago constar que los estudiantes Wendy Natalia Mora Mora, carné, B14416, Estefany Tatiana Rodríguez Gamboa, carné, B15558 y Jose Manuel Matew Soto, carné, A53328, presentaron el proyecto de graduación titulado "***Propuesta de un modelo de control interno para el proceso contable de la Junta Administradora del Fondo de Ahorro y Préstamos de la Universidad de Costa Rica (JAFAP) mediado por tecnologías de información, con base en un estudio de COBIT 5 y la normativa vigente aplicada por la Contraloría General de la República"***, dicho proyecto fue aprobado en la defensa el día 9 de diciembre sin solicitud de corrección alguna, por lo tanto les informo que la versión aprobada y la cuál será entregada por los estudiantes es la versión definitiva.

Cordialmente,

MICHEL ANGULO SOSA (FIRMA)

Firmado digitalmente por MICHEL ANGULO SOSA (FIRMA)
DN: SERIALNUMBER=CPF-01-0838-0047, SN=ANGULO SOSA, G=MICHEL, C=CR, O=PERSONA FISICA, OU=CIUDADANO, CN=MICHEL ANGULO SOSA (FIRMA)
Razón: Soy el autor de este documento
Ubicación: la ubicación de su firma aquí
Fecha: 2021.12.13 19:34:43-06'00'
Foxit PDF Editor Versión: 11.1.0

Michel Angulo Sosa

Tutor

Derechos propiedad intelectual

Dedicatorias

Este trabajo está dedicado a mi esposa Laura y a mis padres, don Víctor y doña Enid, por brindarme el apoyo y consejos necesarios para seguir adelante siempre.

A mis compañeras Estefany y Natalia por el todo el esfuerzo realizado para terminar nuestro proyecto.

Jose Manuel Matew Soto

A mi Dios, por darme la vida y permitirme culminar este proceso, darme la paciencia que he necesitado en todo momento y ser mi guía día con día.

A mis padres, por darme la oportunidad de estudiar, brindarme su apoyo incondicional y estar presente en cada una de las metas que me he propuesto, enseñarme el valor de la responsabilidad, el esfuerzo, el trabajo duro y brindarme su amor y cariño todos los días.

A mis hermanos y mejores amigas por darme su amor y apoyo de alguna u otra manera y brindarme palabras de aliento para poder culminar este proceso.

A mis compañeros Estefany y Jose, por confiar en mi trabajo, brindarme su apoyo, palabras de aliento, trasmitirme su conocimiento y estar a mi lado durante todo este tiempo, mil gracias.

A nuestros profesores, por aceptar ser parte de esta meta, ser una guía durante todo el proceso y compartir con nosotros su sabiduría.

Natalia Mora Mora

A mi Dios, por ser mi guía, por estar presente en cada uno de los momentos en los que necesite fuerzas y aliento para lograr culminar este proyecto y por poner personas en nuestro camino que fueron guías en todo este proceso.

A mi madre preciosa, por todo su esfuerzo para darme la oportunidad de estudiar y poder alcanzar uno de mis mayores anhelos, por enseñarme que con amor, paciencia y valentía se logran las metas que tengamos, por su amor, comprensión y estar presente en cada uno de los momentos en los que la he necesitado y por inculcarme luchar por cada uno de mis sueños.

A mi tita y mis hermanas, por cada una de las palabras de aliento que me dieron, por ser un apoyo incondicional en mi vida y recordarme que, con dedicación, esfuerzo y teniendo a Dios presente se logran cada una de nuestras metas.

A mi novio, que ha estado a mi lado en todo este largo proceso, por acompañarme y estar presente en cada uno de los momentos en los que necesitaba aliento, por su paciencia, amor y transmitirme su positivismo que fue un gran impulso para lograr finalizar este proyecto.

A mi amiga Naty, que fue mi compañera de este proyecto, por estar a mi lado desde que iniciamos este sueño, por creer y confiar en que juntas lo lograríamos y darme el aliento, las fuerzas, el positivismo y el coraje para lograr nuestro anhelo, lo logramos amiga.

A mi compañero Jose, por darnos las palabras de motivación y aliento que necesitamos, por creer y confiar en nosotras sin conocernos y por ser un gran apoyo en nuestro proyecto.

A nuestros profesores, que fueron guía para nosotros, por ayudarnos con su sabiduría y conocimiento, por estar en cada uno de los momentos en los que necesitamos de sus consejos, por cada recomendación que nos brindaron y por la motivación que nos dieron para poder culminar nuestro proyecto.

Estefany Rodríguez Gamboa

Índice

Índice de Figuras

Índice de Tablas

Resumen Ejecutivo

Título: Propuesta de un modelo de Control Interno para el proceso contable de la Junta Administradora del Fondo de Ahorro y Préstamos de la Universidad de Costa Rica (JAFAP) mediado por tecnologías de información, con base en un estudio de COBIT 5 y la normativa vigente aplicada por la Contraloría General de la República

Estudiantes: Jose Manuel Matew Soto, Wendy Natalia Mora Mora, Estefany Tatiana Rodríguez Gamboa.

El presente trabajo final de graduación fue realizado con el objetivo de desarrollar una propuesta de un modelo de Control Interno en la Junta Administradora del Fondo de Ahorro y Préstamos de la Universidad de Costa Rica (JAFAP), basado en COBIT 5 para el cumplimiento de las Normas Técnicas para la gestión y control de las Tecnologías de Información de la Contraloría General de la República Capítulo I "Normas de Aplicación General" (N-2-2007-CO-DFOE), con el fin de aumentar la eficacia y eficiencia en sus actividades, mitigar los riesgos en dicho proceso y mejorar la seguridad de los procesos contables.

Para el logro del objetivo principal indicado en el párrafo anterior, se desarrollaron una serie de actividad, las mismas se detallan a continuación:

1. Identificación y descripción de las generalidades del mercado financiero, los órganos encargados de la supervisión y emisión de la normativa aplicable. Así como el análisis del entorno legal, económico y un compendio de los requerimientos teóricos relacionados con el Control Interno y riesgos asociados.
2. Descripción de la Entidad detallando la estructura interna, el perfil de JAFAP y los procedimientos del departamento contable y de tecnologías de información. A su vez, se presenta la relación entre los procesos contables y de TI, y la forma en la que el uso de las tecnologías ha contribuido con la generación de valor en las organizaciones.
3. Evaluación de la situación actual de la JAFAP, mediante un análisis de los procesos contables mediados por TI con base en un estudio de COBIT 5 y la normativa vigente aplicable de la Contraloría General de la República. Por otra parte, se realizó un análisis FOCAR a través del cual se identificaron las fortalezas, oportunidades, carencias, amenazas y riesgos de la Entidad.

4. Desarrollo de la propuesta de un modelo de Control Interno de tecnologías de información en los procesos contables basados en los resultados obtenidos en las evaluaciones realizadas y fundamentadas en las mejores prácticas tanto nacionales como internacionales para la gestión de las TI.
5. Presentación de conclusiones y recomendaciones obtenidas a partir de la elaboración de este proyecto con el propósito final de agregar valor a la Entidad.

Introducción

La Junta Administradora del Fondo de Ahorro y Préstamo (JAFAP) se encuentra ubicada en la Universidad de Costa Rica sede Rodrigo Facio en San Pedro de Montes de Oca, tiene como principal objetivo recaudar y administrar los fondos tanto del personal docente como administrativo de dicho centro de enseñanza, mediante los aportes realizados por sus asociados y el patrono. La Misión de la JAFAP es "contribuir con el mejoramiento del bienestar integral y la calidad de vida de las personas afiliadas" y su Visión es "ser el principal aliado financiero de las personas afiliadas" (Junta de Ahorro y Préstamo de la Universidad de Costa Rica, 2019).

Actualmente la JAFAP entre sus servicios cuenta con cuatro diferentes tipos de captación de recursos para sus asociados, así como un programa de incentivos. Así mismo, brinda ocho tipos de préstamos adecuados a las diferentes necesidades de cada uno de sus asociados. Mediante las inversiones realizadas por la JAFAP en otras instituciones, pretende que los fondos de los asociados aumenten su valor, generen mayor rentabilidad financiera y se fomente la cultura de ahorro (Junta de Ahorro y Préstamo de la Universidad de Costa Rica, 2019).

El organigrama de la JAFAP está compuesto por cinco departamentos los cuales son: Tecnologías de Información, Crédito y Cobro, Contabilidad, Auditoría Interna, Tesorería y la Administración. El presente trabajo será desarrollado en el Departamento Contable en conjunto con el de Tecnologías de Información (Junta de Ahorro y Préstamo de la Universidad de Costa Rica, 2019).

Hoy en día, las tecnologías de información constituyen un elemento estratégico para apoyar a las organizaciones en la consecución de las metas del negocio (Álvarez, 2004), razón por la cual representan uno de los procesos más importantes dentro de las organizaciones para generar valor.

La adecuada gestión de los procesos de tecnologías de información permite, no solo el aseguramiento y aprovechamiento de los diferentes recursos que posee, sino también, se logra una mejor prestación de los servicios hacia las áreas usuarias (Ortiz, 2017).

Por lo tanto, el beneficio obtenido por las organizaciones de las tecnologías de información no radica únicamente en la inclusión de estas en sus procesos, sino en la forma en que se gestionan las mismas, al respecto ISACA (2012) afirma:

"Empresas de éxito han reconocido que el comité y los ejecutivos deben aceptar las TI como cualquier otra parte importante de hacer negocios. Los comités y la dirección – tanto en funciones de negocio como de TI – deben colaborar y trabajar juntos, de modo que se incluya la TI en el enfoque del gobierno y la gestión".

Dado lo anterior, se pretende con este trabajo de investigación crear una propuesta de un modelo de Control Interno para el proceso contable mediante las tecnologías de información, con base en un estudio de COBIT 5 para el cumplimiento de las Normas Técnicas para la gestión y control de las Tecnologías de Información de la Contraloría General de la República Capítulo I "Normas de Aplicación General" (N-2-2007-CO-DFOE), con el objetivo de optimizar su gestión y mitigar los riesgos asociados, permitiendo así el que los procesos de tecnologías de información contribuyan al logro de las metas de la JAFAP.

Así mismo, se realiza un trabajo de investigación el cual genere valor económico y social para la JAFAP y, a la vez, sea una guía de mejora, debido al giro de negocio la Junta mantiene gran cantidad de operaciones y procesos internos fundamentales para la continuidad del negocio, lo que representará un beneficio a nivel interno y externo.

Justificación

En la actualidad existen muchas organizaciones dedicadas a la administración y recaudación de los fondos recibidos de sus asociados con la finalidad de mejorar el bienestar integral de los mismos, a través de procesos de intermediación financiera. Por lo tanto, estas organizaciones deben garantizar una estructura de control adecuado disminuyendo el impacto de factores que afecten la finalidad de la Entidad, principalmente a través de la evaluación de riesgos, entendiéndose como la identificación y análisis de todos los factores internos y externos que afectan las operaciones de la empresa, por medio de un proceso que debe ser continuo, enfocado a riesgos futuros y que, a su vez, sea más preventivo que correctivo (Hernández, 2016).

El proceso contable es vital para las organizaciones en cuanto al procesamiento y generación de información sobre su rentabilidad, además cumple con obligaciones legales y facilita el proceso de toma de decisiones de la administración. Palepu, Healy & Bernard (2002) afirman que la información contable de una empresa captura su realidad económica y, por tanto permite identificar la calidad de la información, las posibles señales de riesgo y las distintas posibilidades de crecimiento; es por esto que el proceso contable requiere una estructura de Control Interno el cual brinde seguridad razonable a su operación.

Dado lo anterior, se considera relevante la utilización de una metodología de control que aumente la seguridad en los procesos contables y, consecuentemente, minimice los riesgos asociados. Con este proyecto se propone un modelo de mejora de Control Interno a los procesos existentes de tecnologías de información, con base en el marco de referencia de COBIT 5 y las Normas técnicas para la gestión y el control de las Tecnologías de Información de la Contraloría General de la República (N-2-2007-CO-DFOE). También se utilizan dichos marcos de referencia como modelos reconocidos para la adecuada gestión de los procesos de tecnologías de información; al respecto Hernández (2015) afirma: “las buenas prácticas deben ser aplicadas para todas las empresas u organizaciones sin importar el tamaño y magnitud del Gobierno corporativo, el seguimiento a los estándares globales es de gran importancia para la administración del negocio” (p.4)

Este proyecto se aplicará en la Junta Administradora del Fondo de Ahorro y Préstamo de la Universidad de Costa Rica (JAFAP), por lo tanto, brindará un modelo de Control Interno basado en las mejores prácticas reconocidas a nivel mundial y nacional, desde una perspectiva del control de tecnologías de información, permitiendo adoptar la propuesta de un modelo de Control Interno en otros procesos de la Organización.

Para la elaboración de este trabajo de investigación es necesario realizar un análisis y diagnóstico de los marcos de referencia vigentes, con el fin realizar una adaptación a los procesos de Control Interno en Tecnología de Información utilizados por la Junta.

Alcance

El presente trabajo se realizará en la Junta Administradora del Fondo de Ahorro y Préstamos de la Universidad de Costa Rica, ubicada en San Pedro de Montes de Oca, Ciudad Universitaria Rodrigo Facio.

Se pretende crear una propuesta de un modelo de Control Interno de tecnologías de información en los procesos contables de la JAFAP, mediante un análisis de COBIT 5 para el cumplimiento de las Normas Técnicas para la gestión y control de las Tecnologías de Información de la Contraloría General de la República Capítulo I "Normas de Aplicación General" (N-2-2007-CO-DFOE), con el fin de minimizar los riesgos los cuales afectan los objetivos de la Organización.

Para la elaboración de la propuesta del modelo de Control Interno se requiere el estudio de los procesos contables actuales de la JAFAP relacionados con tecnologías de información y su comparación con los marcos de referencia indicados.

Por lo tanto, se pretende que este trabajo se convierta en una guía la cual contribuya al fortalecimiento de los controles internos de los procesos relacionados con tecnologías de información, a través de criterios que permitan medir, evaluar y controlar la gestión de los procesos.

El alcance del proyecto será únicamente la realización y no la ejecución de la metodología, la decisión de su aplicación quedará en manos de la JAFAP.

Limitaciones

Durante la realización del proyecto de investigación, en caso de presentarse limitaciones que pueden afectar el alcance de los objetivos y generar implicaciones en los resultados del trabajo, se buscarán soluciones para mitigar dichas situaciones.

Una de las limitaciones es la confidencialidad de la información por disposiciones internas de la JAFAP para la entrega a terceros, debido a la vulnerabilidad de esta, por tanto, no debe ser divulgada. Para mitigar esta limitante se realizarán cuestionarios, entrevistas y otro tipo de trabajo de campo que no involucre la obtención de dicho material.

Por último, otra limitante es la atención de consultas y reuniones con el personal a cargo. Los procesos de captación a los que está enfocado el proyecto de investigación se encuentran segregados en varios funcionarios y la disponibilidad de horarios de atención al público y cantidad de responsabilidades pueden variar, esto provoca mayor dificultad para la coordinación de reuniones y realización de entrevistas. Para solucionar tal limitante, se realizará, con anticipación, un cronograma de trabajo con los requerimientos específicos necesarios para el avance del proyecto, con fin de que tanto los colaboradores de la Junta como el equipo de trabajo de investigación estén en mutuo acuerdo.

Objetivo General

Desarrollar una propuesta de un modelo de Control Interno basado en COBIT 5 para el cumplimiento de las Normas Técnicas para la gestión y control de las Tecnologías de Información de la Contraloría General de la República Capítulo I "Normas de Aplicación General" (N-2-2007-CO-DFOE), con el fin de aumentar la eficacia y eficiencia en sus actividades y mitigar los riesgos en dicho proceso.

Objetivos Específicos

1. Identificar y describir el entorno legal y económico de la JAFAP, así como establecer los requerimientos teóricos en relación con el Control Interno y riesgos asociados, necesarios para formular la propuesta del proyecto.

2. Describir la estructura general, Organización y procedimientos de tecnologías de información del proceso contable de la JAFAP, así como sus mecanismos de control e indicadores, con el fin de formular la propuesta del presente proyecto.

3. Realizar un diagnóstico de la situación actual de la JAFAP, aplicando los conceptos teóricos de COBIT 5 para el cumplimiento de la normativa de la Contraloría General de la República a fin de identificar las oportunidades de mejora en el proceso contable.

4. Desarrollar una propuesta de un modelo de Control Interno de tecnologías de información en los procesos contables de la JAFAP, mediante un análisis basado en COBIT 5 para el cumplimiento de las Normas Técnicas para la gestión y control de las Tecnologías de Información de la Contraloría General de la República Capítulo I "Normas de Aplicación General" (N-2-2007-CO-DFOE), con el fin de optimizar la gestión y mitigar los riesgos.

5. Formular y exponer las conclusiones y recomendaciones obtenidas a partir del desarrollo del proyecto con el propósito de agregar valor a la Organización.

Perspectivas teóricas

La propuesta del modelo de Control Interno para el proceso contable de la JAFAP será realizada a través de un análisis de COBIT 5, así como la normativa aplicable referente a tecnologías de información de la Contraloría General de la República, esto brindará un marco de trabajo que contribuye a las empresas a alcanzar los objetivos para el Gobierno y gestión de las tecnologías de información corporativas (ISACA, 2012).

Inicialmente es importante definir el concepto de Control Interno el cual según el *Committee of Sponsoring Organizations of the Treadway Commision, COSO* (2013) corresponde a un proceso, efectuado por la junta directiva de una Entidad, administración y otro personal, diseñado para proporcionar una seguridad razonable con respecto al logro de los objetivos relacionados con las operaciones, informes y cumplimiento.

Así mismo, se define Control Interno como: "conjunto de métodos y procedimientos que aseguren que los activos están debidamente protegidos, que los registros contables son fidedignos y que la actividad de la Entidad se desarrolla eficazmente según las directrices marcadas por la administración" (Estupiñán, 2006, pág.19)

Por otra parte, ISACA (2012) define sistema de Control Interno como las políticas, estándares, planes y procedimientos y las estructuras organizativas diseñadas para proveer una garantía razonable de que los objetivos de la empresa van a conseguirse, además los eventos no deseados serán evitados, detectados y subsanados.

El Control Interno permite a las organizaciones obtener una serie de beneficios en su operación, por ejemplo brinda mayor confianza a la Gerencia y las Juntas Directivas con respecto al logro de los objetivos, además de brindar retroalimentación sobre el funcionamiento del negocio y contribuye a reducir las sorpresas (COSO, 2013).

Una forma de lograr los objetivos empresariales es mediante el Control Interno con ayuda de las tecnologías de información (en adelante TI), según el Reglamento General de la Gestión y Tecnología de la Información (2017) de la SUPEN se definen como el conjunto de técnicas para la captura, almacenamiento, transformación, transmisión y presentación de la información generada o recibida a partir de procesos de negocios, de tal manera pueda ser organizada y utilizada en forma consistente y comprensible por los usuarios relacionados con ella. Incluye

elementos de *hardware*, *software*, telecomunicaciones y conectividad, entre otros.

Sobre este tema, Gabriela & Garrido (Citado por Mora, 2017) afirman que, "Las TIC conforman el conjunto de recursos necesarios para manipular la información: los ordenadores, los programas informáticos y las redes necesarias para convertirla, almacenarla, administrarla, transmitirla y encontrarla." (pág. 17)

El uso de las TI en las organizaciones aumenta la productividad, competitividad, seguridad de la información, aplicación de controles, disponibilidad de la información, disminución de costos y tiempos de los procesos, lo cual genera mayor eficiencia y eficacia en las operaciones. El cumplimiento de objetivos empresariales provoca en las compañías riesgos generales del negocio, según el *Committee of Sponsoring Organizations of the Treadway Commission* (2013) riesgo se define como la posibilidad de que ocurra un evento y afecte adversamente el logro de objetivos. Las organizaciones se enfrentan a riesgos externos e internos, algunos de estos son económicos, políticos, ambientales, tecnológicos, contables, operacionales, de personal, entre otros. La afectación de cada uno dependerá del tipo de negocio en el que se desenvuelve la compañía.

Aunado a lo anterior, el cumplimiento de los objetivos organizacionales mediante la utilización de TI provoca la exposición a riesgos específicos de TI, los cuales según la SUGEF (2017) se definen como la posibilidad de pérdidas económicas derivadas de un evento relacionado con el acceso o uso de la tecnología, que afecta la capacidad de la Entidad para funcionar de manera efectiva y la adecuada gestión de riesgos, al atentar contra la confidencialidad, integridad, disponibilidad, eficiencia, confiabilidad y oportunidad de la información.

Para mitigar los riesgos generados en el giro normal del negocio y mejorar continuamente las labores empresariales, cada Organización necesita trabajar de la mano de los sistemas de información contables y procesos contables para cumplir con los objetivos, de acuerdo con Horngren, C. (Citado por Mora, 2017) los "Sistemas de información contable son quizás una de las bases de las actividades empresariales, por no decir que es la más importante dentro del campo de los negocios, dada su naturaleza de informar acerca del incremento de la riqueza, la productividad y el posicionamiento de las empresas en los ambientes competitivos, por lo que es imperioso que vaya al ritmo de las exigencias de los distintos usuarios dentro y fuera de la entidad". (pág. 9)

Al respecto Williams, Haka, & Bether (Citado por Mora, 2017) “Afirman que un sistema de información contable consta del personal, los procedimientos, los mecanismos y los registros utilizados, para una Organización, primero para desarrollar la información contable y segundo para transmitir esta información a quienes toman decisiones.” Por consiguiente, el propósito está en “satisfacer en la forma más eficiente posible las necesidades de información contable de la Organización.” (pág. 9)

Actualmente para el adecuado funcionamiento de los procesos contables es necesario la utilización de sistemas de información, pues las organizaciones se desempeñan en entornos económicos altamente competitivos, esto las obliga a mejorar sus procesos internos en búsqueda de una mejora continua para maximizar su rentabilidad. Por procesos se entiende una colección de prácticas influenciadas por las políticas y procedimientos de la empresa que toma entradas de una serie de fuentes (incluyendo otros procesos), manipula esas entradas y genera salidas (por ejemplo, productos, servicios), (ISACA, 2012).

Por lo tanto, son de particular interés para este estudio los procesos de contabilidad, así como los de tecnologías de información relacionados con dichos procesos contables y cómo estos influyen en la Organización. Medina & Morocho (2015) definen los procesos contables o ciclo contable como una serie de pasos o la secuencia que sigue la información contable desde que se origina el registro de los hechos económicos (comprobantes o documentos fuentes) hasta la presentación en los estados financieros.

Estos procesos contables, a su vez, suelen tener relación e impacto con otros sistemas institucionales, como por ejemplo el sistema de Control Interno; Posso (2014) define el Control Interno contable como los controles y métodos establecidos para garantizar la protección de los activos y la fiabilidad y validez de los registros y sistemas contables. Es decir, la relación de los procesos contables con el Control Interno tiene como objetivo final el logro de los objetivos de la Organización a través de la integridad de sus registros e información financiera.

Debido al impacto presente en la información contable y cómo esta influye en el logro de los objetivos de la Organización, es importante que la alta gerencia y la administración, según sus competencias, emprendan las medidas pertinentes para asegurar que se establezcan y se mantengan actualizados los registros contables y presupuestarios, que brinden un conocimiento razonable y confiable de las disponibilidades de recursos, las obligaciones adquiridas por la

institución, las transacciones y eventos realizados (Contraloría General de la República, 2009).

Como se mencionó anteriormente, el uso de las TI en los procesos contables permite una adecuada gestión empresarial y cumplir con los requisitos mínimos de Control Interno, así como la minimización de riesgos asociados y generación de valor a través de un uso eficaz de las TI, al generar así una relación entre las TI y los procesos contables tomados como "Conjunto de elementos o componentes interrelacionados para recolectar, manipular y diseminar datos en información y para proveer un mecanismo de retroalimentación en pro del cumplimiento de un objetivo (…) en la práctica se utiliza como sinónimo de sistema de información computarizado". López (Citado por Mora, 2017 pág. 7)

Para una optimización en el uso de las TI es importante que las compañías se guíen con herramientas o buenas prácticas de seguridad y control para establecer procedimientos a seguir y permitan gestionar sus recursos.

Para el desarrollo de este trabajo se realizará un análisis de las mejores prácticas Control *Objectives for Information and related Technology*, *COBIT* por sus siglas en inglés, emitidas por el *Information Systems Audit and Control Association* (ISACA), así como las Normas Técnicas para la gestión y el control de las Tecnologías de Información de la Contraloría General de la República (N-2-2007-CO-DFOE).

COBIT 5

COBIT 5, corresponde a un marco de negocio para el Gobierno y la gestión de las tecnologías de información de las empresas, el cual pretende que las organizaciones generen valor desde las TI, disminuyan la exposición a los riesgos y lleven a cabo un adecuado uso de los recursos.

Este marco de referencia está basado en cinco principios claves para el Gobierno y la gestión de las tecnologías de información, estos principios son:

1. Satisfacer las necesidades de las partes interesadas
2. Cubrir la empresa extrema a extremo
3. Aplicar un marco de referencia único integrado
4. Hacer posible un enfoque holístico.

5. Separar al Gobierno de la gestión.

Estos cinco principios planteados por COBIT permiten que las organizaciones desarrollen un marco para el Gobierno y administración de TI de una manera holística, tomando en consideración el negocio, así como todas las áreas funcionales, enfocándose, principalmente, en todas las partes interesadas de la Organización, ya sean internas o externas.

Además de estos principios, COBIT 5 plantea siete catalizadores o habilitadores, define catalizadores como factores que, individual y colectivamente, influyen sobre si algo funcionará, para este caso, el Gobierno y la gestión de la empresa en TI (ISACA, 2012). Los catalizadores son:

1. Principios, políticas y marcos de trabajo.
2. Procesos.
3. Estructuras organizativas.
4. Cultura, ética y comportamiento.
5. Información.
6. Servicios, infraestructuras y aplicaciones.
7. Personas, habilidades y competencias.

Principios de COBIT 5

Tal y como se mencionó anteriormente, COBIT 5 consta de cinco principios claves para el Gobierno y gestión de TI, dichos principios son genéricos y útiles para cualquier tipo y tamaño de Organización, es decir, grandes o pequeñas empresas, sector público o privado. Cada uno de estos principios brinda una guía de buenas prácticas y estándares para aplicar en las organizaciones, según se detalla a continuación:

Principio 1. Satisfacer las necesidades de las partes interesadas: La razón principal de las empresas es la creación de valor para sus partes interesadas (accionistas, clientes, proveedores), a través de un equilibrio entre la realización de beneficios, optimización de riesgos y el uso de los recursos. Por lo tanto, COBIT brinda los procesos necesarios y los catalizadores

para la generación de valor a través del uso de las TI.

Principio 2. Cubrir la empresa extremo a extremo: se cubren todos los procesos y funciones dentro de la empresa, no solo lo relacionado con TI, trata de toda la información y tecnologías relacionadas como activos manejados como cualquier otro activo, por todos en la Organización. A manera de resumen COBIT integra el Gobierno de TI al Gobierno corporativo.

Principio 3. Aplicar un marco de referencia único integrado: COBIT 5 se alinea con otros estándares y marcos de trabajo relevantes para la gestión de tecnologías de información. Como ejemplos tenemos COSO, COSO ERM, ISO 9000, ISO 38500, ISO, 2700, ITIL, entre otros.

Principio 4. Hacer posible un enfoque holístico: para un Gobierno y gestión de TI efectivo y eficiente, las organizaciones requieren de un enfoque holístico el cual considere diferentes componentes interactivos. Para esto, COBIT define un conjunto de catalizadores mencionados anteriormente, los mismos permiten apoyar la implementación de un sistema de Gobierno y gestión de TI para las empresas.

Principio 5. Separar el Gobierno de la gestión: en este particular, COBIT 5 plantea una clara diferencia entre Gobierno y gestión a saber:

- Gobierno: el Gobierno asegura la evaluación de las necesidades, condiciones y opciones de las partes interesadas para alcanzar las metas corporativas equilibradas y acordadas, establece la dirección a través de la priorización, la toma de decisiones también mide el rendimiento y el cumplimiento respecto a la dirección y metas acordadas.

- Gestión: la gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de Gobierno para alcanzar las metas empresariales (ISACA, 2012, p14).

Según lo anterior, el Gobierno y la gestión comprenden diversos tipos de actividades, requieren diferentes estructuras organizacionales y cumplen múltiples propósitos. Por lo tanto, otro marco de referencia importante son las Normas técnicas para la gestión y el control de las Tecnologías de Información de la Contraloría General de la República, en otras palabras corresponden a la normativa la cual establece los criterios básicos de control que deben observarse

en la gestión de esas tecnologías y que tiene como propósito coadyuvar en su gestión, en virtud de que dichas tecnologías se han convertido en un instrumento esencial en la prestación de los servicios públicos (Contraloría General de la República, 2007).

Estas normas técnicas brindan a las instituciones una serie de pasos a seguir para el eficiente cumplimiento de sus objetivos, pues las grandes empresas manejan gran cantidad de información, por tanto es necesario aumentar los controles y la forma de su aplicación, en suma se hace referencia a los siguientes lineamientos:

1. Planificación y Organización.
2. Implementación de tecnologías de Información.
3. Prestación de servicios y mantenimiento.
4. Seguimiento.

La búsqueda de los objetivos empresariales mediante la planificación y Organización se deben estar en congruencia tanto con la capacidad presupuestaria como con las tecnologías de información y su cumplimiento del Control Interno. Según la Contraloría General de la República, (2007) se establece la Organización debe optimizar la integración, uso y estandarización de sus sistemas de información de manera que se identifique, capture y comunique, en forma completa, exacta y oportuna.

Es importante mencionar que la función de las tecnologías de información debe ser independiente a las labores de los demás departamentos dentro de la Organización, sin embargo, debe existir comunicación directa entre estos, ahora bien esta forma información y los resultados deber ser los esperados por la administración.

Según la Contraloría General de la República, (2007) dentro de la implementación de TI se establecen los siguientes pasos a seguir para el cumplimiento de los objetivos empresariales:

1. Adoptar políticas sobre la justificación, autorización y documentación de solicitudes de implementación o mantenimiento de TI.
2. Establecer el respaldo claro y explícito para los proyectos de TI tanto del jerarca como de las áreas usuarias.
3. Garantizar la participación activa de las unidades o áreas usuarias, las cuales deben

tener una asignación clara de responsabilidades y aprobar formalmente las implementaciones realizadas.

4. Instaurar líderes de proyecto con una asignación clara, detallada y documentada de su autoridad y responsabilidad.
5. Analizar alternativas de solución de acuerdo con criterios técnicos, económicos, operativos y jurídicos, además los lineamientos previamente establecidos.
6. Contar con una definición clara, completa y oportuna de los requerimientos, como parte de los cuales debe incorporar aspectos de control, seguridad y auditoría bajo un contexto de costo – beneficio.
7. Tomar las previsiones correspondientes para garantizar la disponibilidad de los recursos económicos, técnicos y humanos requeridos.
8. Formular y ejecutar estrategias de implementación que incluyan todas las medidas para minimizar el riesgo de que los proyectos no logren sus objetivos, no satisfagan los requerimientos o no cumplan con los términos de tiempo y costo preestablecidos.
9. Promover su independencia de proveedores de *hardware*, *software*, instalaciones y servicios.

Dentro de la prestación de servicios y mantenimiento la Contraloría General de la República, (2007) establece que la Organización debe asegurarse de que los datos procesados mediante TI correspondan a transacciones válidas y debidamente autorizadas, también procesados en forma completa, exacta, oportuna, transmitidos, almacenados y desechados en forma íntegra y segura.

La información contable es esencial para el cumplimiento de los objetivos empresariales y es manejada a través de TI, la misma debe ir de la mano con lo suministrado por los demás departamentos, debe ser real y congruente. Por lo anterior, se considera necesario que la administración cuente con un adecuado Control Interno para identificar los posibles riesgos en los procesos y establecer procedimientos para minimizar dichos riesgos, lo cual cumple con el punto del seguimiento establecido en la norma.

Otro concepto importante es *mejora*, según el Instituto de Normas Técnicas de Costa Rica

(INTE/ISO 9000:2015) es esencial para que una Organización mantenga los niveles actuales de desempeño, reaccione a los cambios en sus condiciones internas, externas y cree nuevas oportunidades.

La mejora se encuentra relacionada de manera directa con lo mencionado anteriormente, las compañías una vez que planifican, aplican y evalúan los procedimientos realizados a nivel interno buscan identificar puntos de mejora que contribuyan al cumplimiento efectivo de los propósitos planteados.

Metodología de la investigación

Para el desarrollo de este proyecto de investigación se utilizarán diferentes métodos para la recolección de la información según las necesidades, los cuales pueden ser fuentes primarias o secundarias. Estas se determinarán conforme con el desarrollo de cada uno de los objetivos planteados para dicho trabajo.

A continuación, se definen las fuentes por utilizar en cada uno de los objetivos:

- Objetivo uno: se utilizarán fuentes de información secundaria para obtener la información requerida, a través de consultas en leyes, reglamentos, normativas aplicables, consultas bibliográficas, así como consultas en *sitios web*. Estas fuentes de información permitirán determinar las generalidades de la industria financiera costarricense, así como también los conceptos generales referentes a Control Interno, procesos contables y tecnologías de información requeridos para la investigación.

- Objetivo dos: la información será recolectada mediante fuentes secundarias a través de material proporcionado por la JAFAP, por ejemplo: reglamentos, políticas, normativas, esquemas de trabajos, entre otros, así mismo la consulta de libros, Trabajos Finales de Graduación (TFG), normativas vigentes y material electrónico para argumentar el objetivo sobre lo referente al Control Interno, las tecnologías de información, el funcionamiento y estructura de la JAFAP. Por otra parte, se recolectará información primaria mediante entrevistas a colaboradores y encargados con el objetivo de cubrir temas que la Organización no mantenga documentada y desarrollar mejor los temas mencionados.

- Objetivo tres: se obtendrá la información a través de material proporcionado por JAFAP, ya sea por medio de los procesos documentados, así como también en entrevistas que permitan identificar y evaluar su operación y controles en sus procesos contables y de tecnologías de información. Adicionalmente se consultarán los marcos de referencia establecidos con el fin de realizar el análisis y comparación de los procesos actuales respecto a las buenas prácticas, de acuerdo con lo establecido para este objetivo. Se pretende, identificar las oportunidades de mejora para la Organización para optimizar su gestión y minimizar sus riesgos.

- Objetivo cuatro: se reunirá la información de fuente primaria, así como la información obtenida en los capítulos anteriores, realizando la comparación de la situación actual respecto a los criterios y normativas aplicables, al determinar así las brechas y oportunidades de mejora, con el propósito de generar la propuesta de un modelo de Control Interno de tecnologías de información en los procesos contables.

- Objetivo cinco: se recopilará y analizará la información obtenida en los cuatro objetivos anteriores y, a partir de esto, se plantean los resultados obtenidos en el trabajo, luego los resultados y son generadas las recomendaciones para una propuesta de mejora de Control Interno de tecnologías de información aplicable a los procesos contables y otros procesos de la Organización.

Capítulo I. Generalidades del mercado financiero costarricense, contextualización sobre el Control Interno aplicable en procesos contables y de tecnologías de información.

En el presente capítulo se desarrollan las generalidades del mercado financiero abordando detalles desde su nacimiento, así como los órganos encargados de la supervisión y emisión de normativa aplicable. Adicionalmente, se realiza una descripción del entorno legal, económico y un compendio de los principales conceptos utilizados en el desarrollo del trabajo.

1.1. Generalidades de la Industria Financiera Costarricense.

A continuación, se presenta una descripción de la industria financiera, los órganos reguladores del mercado, los principales elementos legales y económicos que influyen en el sector.

1.1.1. Naturaleza de la Industria

La industria financiera en Costa Rica se originó entre los años 1847 y 1849, bajo la administración del entonces presidente del país José María Castro Madriz, en la cual se realizaron esfuerzos para la creación de un banco, sin embargo, hasta el año de 1858 se fundó el Banco Internacional de Costa Rica también conocido como Banco de Medina (Escoto, 2007).

Posteriormente, en el año de 1863 es fundado el Banco Anglo Costarricense siendo el primer banco en establecer el cheque como medio de pago, además, efectuó operaciones de crédito y venta de propiedades o inmuebles sumado a que estableció agencias en Puntarenas, Panamá y Guatemala (Escoto, 2007).

Entre los años1867 y 1877 se crearon nuevos bancos en el país tanto privados como del Estado, sin embargo, los bancos tenían la dificultad de reunir el capital necesario que permitiera la operación y, por lo tanto, se produjo el cierre de algunos de estos. Como parte de este proceso de creación de nuevos bancos en el país, se fundó el Banco de la Unión en 1877, establecido como un banco privado, cambiando su nombre en el año 1890 a Banco de Costa Rica tal y cómo se conoce actualmente.

Por otra parte, en 1914 fue creado el Banco Central de Costa Rica bajo el nombre de Banco Internacional de Costa Rica, teniendo como objetivo darle un préstamo al Gobierno para cumplir

con las obligaciones fiscales y cumplir las erogaciones del presupuesto nacional.

En un inicio se conocía por Banco Central el ente que tenía el monopolio de la emisión de billetes y el manejo de las operaciones bancarias del Estado. Al paso del tiempo sus funciones se ampliaron, saber mantener la convertibilidad de la moneda a oro, plata o monedas extranjeras. Luego fue adquiriendo otras funciones como la de banco de reserva reguladora del crédito y la moneda. (Escoto, 2007, p.12).

Producto de la revolución de 1948 se produce una serie de cambios por parte de la Junta Fundadora de la Segunda República, dentro de los cuales se encuentra el Decreto de Ley de Nacionalización Bancaria, el cual pretendía que los depósitos de cuenta corriente y ahorro del público estuvieran en manos de los bancos del Estado.

> *"Con la nacionalización bancaria se buscaba establecer un monopolio a favor de las instituciones bancarias del Estado para captar recursos del público, y bajo el principio de que las funciones de manejo de los depósitos del público y concesión de crédito son de carácter público.* (Escoto, 2007).

Adicionalmente, como parte de los cambios impulsados por la Junta Fundadora de la Segunda República, se emitió la Ley de naturaleza transitoria No. 1130 para la creación del Banco Central de Costa Rica y se independizó el Departamento Emisor el cual estaba a cargo del Banco Nacional de Costa Rica. Es en el año de 1953 cuando se crea la Ley Orgánica del Banco Central de Costa Rica que, posteriormente, fue modificada mediante la Ley No. 7558 del año 1995.

Dicha Ley Orgánica establece como objetivo principal del Banco Central de Costa mantener la estabilidad interna y externa de la moneda nacional y asegurar su conversión a otras monedas, así mismo los siguientes objetivos subsidiarios:

> a) Promover el ordenado desarrollo de la economía costarricense, para lograr la ocupación plena de los recursos productivos de la Nación, además evitar o moderar las tendencias inflacionistas o deflacionistas que puedan surgir en el mercado monetario y crediticio.
>
> b) Velar por el buen uso de las reservas monetarias internacionales de la Nación para el logro de la estabilidad económica general.

c) Promover la eficiencia del sistema de pagos internos y externos y mantener su normal funcionamiento.

d) Promover un sistema de intermediación financiera estable, eficiente y competitivo.[1]

Como parte de la evolución de la industria financiera costarricense, en la década de 1980, con la reforma a Ley de la Moneda, hubo un mayor ámbito de acción a la banca privada, sobre este particular Rodríguez (2012) afirma: "El proceso de apertura de la banca costarricense hacia una mayor competencia y participación de intermediarios de capital privado, empieza a darse con fuerza a mediados de la década de 1980. (p.10).

Esta situación es fortalecida en el año de 1995 con la reforma a Ley Orgánica del Banco Central, mediante la cual se eliminó el monopolio de las cuentas corrientes y de ahorro en manos de los bancos del Estado establecido mediante la nacionalización bancaria, por lo tanto permitió así a los bancos privados la captación de recursos limitada hasta ese momento a certificados de depósito a plazo.

Otras de las consecuencias de la reforma a Ley Orgánica del Banco Central del 1995 es la modificación de Auditoría General de Entidades Financieras creada mediante la Ley de Modernización del Sistema Financiero de la República de 1988 en la Superintendencia General de Entidades Financieras (SUGEF), al respecto Loría (2013) indica: "Se establece y fortalece entonces un ámbito de acción reguladora más amplio, orientado a garantizar la transparencia, promover el fortalecimiento y fomentar el desarrollo del sistema financiero" (p.81).

Dentro de este proceso de evolución de la industria financiera en Costa Rica, se promulgó en el año de 1997 la Ley Orgánica del Sistema Bancario Nacional y la Ley Reguladora del Mercado de Valores, las cuales ampliaron el marco regulatorio más allá de la competencia de la SUGEF con el fin de incluir las actividades bursátiles, de esta forma estableció así supervisiones específicas para cada mercado y creando un ente coordinador, el Consejo Nacional de Supervisión del Sistema

[1] Recuperado el 9 de mayo 2020 de: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=40928

Financiero (CONASSIF).

La Ley Orgánica del Sistema Bancario Nacional y en la Ley Reguladora del Mercado de Valores (7732) de 1997 amplían el marco regulatorio más allá de los bancos y otros intermediarios financieros para incluir a la actividad bursátil y la de carteras mancomunadas. Con ello, se reconoce la necesidad de establecer una supervisión específica para cada uno de esos mercados, al tiempo es necesario también crear un ente coordinador, el Consejo Nacional de Supervisión del Sistema Financiero (CONASSIF), el cual se compone de la SUGEF, la Superintendencia de Pensiones (SUPEN), Superintendencia General de Valores (SUGEVAL) y la Superintendencia General de Seguros (SUGESE); esta última creada en el 2008 con la Ley Reguladora del Mercado de Seguros.

1.1.1.1. Junta Administradora del Fondo de Ahorro y Préstamo de la Universidad de Costa Rica (JAFAP) y organizaciones similares en instituciones de educación superior en Costa Rica.

Dentro de las instituciones de educación superior principales en este país, a saber Universidad Nacional, Instituto Tecnológico de Costa Rica y Universidad Estatal a Distancia, se encuentran fondos o asociaciones que brindan servicios y beneficios similares a los brindados por la JAFAP. A continuación, se presenta un resumen de estos:

- **Universidad de Costa Rica - Junta Administradora del Fondo de Ahorro y Préstamo de la Universidad de Costa Rica (JAFAP)**

La Junta Administradora del Fondo de Ahorro y Préstamo de la Universidad de Costa Rica (JAFAP), fue creada con la promulgación de la Ley Orgánica de la Universidad de Costa Rica, el 26 de agosto de 1940 y por la necesidad de que sus funcionarios tuvieran acceso a un régimen de seguros al momento de jubilarse.

Esta Ley estableció que los funcionarios de la Universidad tendrían derecho a una jubilación voluntaria cuando alcanzaran los sesenta años y, forzosa, a los setenta años. Con ese propósito, se contrató un seguro para cada empleado con el Instituto Nacional de Seguros. Las primas, aportes y beneficios se basaron en las disposiciones de la Ley de Seguros de Vejez y Retiro de Empleados y Obreros de la Imprenta Nacional, por lo tanto la Universidad asumió las obligaciones que esa ley indicaba para el Estado.2

[2] Recuperado el 7 de junio 2020 de: http://jafapucr.com/Inicio/Rese%C3%B1aHist%C3%B3rica/DetalledelaHistoria.aspx

Brinda servicios de ahorro, crédito entre otros. En el capítulo II se desarrolla a profundidad el perfil de la Organización.

- **Universidad Nacional - Fondo de Beneficio Social (FBS)**

El FBS surgió en el año de 1981 como parte de la Segunda Convención Colectiva pactada entre la Universidad Nacional y el Sindicato de Trabajadores de la UNA. Creada bajo principios solidarios y la búsqueda de formas creativas para la redistribución de la riqueza social, una Entidad sólida, segura y con un amplio respaldo[3].

Dentro de los servicios que brinda FBS se encuentran los planes de ahorro tanto a la vista como a plazo, así como los planes de crédito dentro de los cuales se mencionan los créditos de consumo, hipotecarios, vivienda, entre otros. Adicionalmente, cuentan con convenios con distintas empresas que brindan ofertas y descuentos a los miembros del FBS.

- **Instituto Tecnológico de Costa Rica - Asociación Solidarista de Empleados del TEC (ASETEC)**

ASETEC fue fundada en el año de 1981 bajo el amparo la de Ley de Asociaciones, posteriormente, en el año 1967 al promulgarse la Ley de Asociaciones Solidaristas se reinscribe como Asociación Solidarista de Empleados del TEC (ASETEC)[4].

Actualmente, ASETEC brinda a sus asociados los servicios de planes de ahorro, líneas de crédito, servicio de soda, cafetería, gimnasio, servicios de salud para asociados y familiares, así como también convenios con empresas privadas para obtención de descuentos.

- **Universidad Estatal a Distancia - Asociación Solidarista de Empleados de la UNED (ASEUNED).**

ASEUNED fue fundada en el año de 1981 basada en los principios del solidarismo, fraternidad, respeto armonía, libertad y justicia en las relaciones entre trabajadores y empresas[5].

Planes de ahorro, crédito, pólizas, ferias, servicios de salud, fondo de mutualidad en caso de fallecimiento o enfermedad y otras actividades se encuentran dentro de los servicios y beneficios de ASEUNED a sus asociados.

1.1.2. Entorno Legal

Dentro del marco normativo costarricense que rige el sistema financiero existe una serie de

[3] Recuperado el 11 de mayo 2020 de: https://fobeso.com/fbs-sobre-nosotros/
[4] Recuperado el 11 de mayo 2020 de: https://aseteccr.com/Informaci%C3%B3n/Rese%C3%B1a-Hist%C3%B3rica
[5] Recuperado el 11 de mayo 2020 de: http://aseuned.com/newsite/quienes-somos/

leyes, reglamentos y otras normativas emitidas por los entes reguladores. A continuación, se detallan las de mayor relevancia:

1. Ley No. 7558: Ley Orgánica del Banco Central

La ley vigente fue emitida el 3 de noviembre de 1995 sustituyendo la ley 1552 del 23 de abril de 1955. Dicha ley establece al Banco Central de Costa Rica (BCCR) como un órgano independiente y le designa la rectoría de la política económica, monetaria y crediticia del país.

El Banco Central tiene como objetivo principal controlar la inflación, labor realizada de manera conjunta con Consejo Nacional de Supervisión del Sistema Financiero, adicionalmente, se encarga de promover la eficiencia del sistema de pagos internos y externos y mantener su normal funcionamiento. [6]

Adicionalmente, se encarga de la custodia del Encaje Mínimo Legal correspondiente a una reserva proporcional al monto total de los depósitos y captaciones de las instituciones financieras supervisadas. El límite de esta reserva será definido por la Junta Directiva del BCCR.

2. Ley No. 1644: Ley Orgánica del Sistema Bancario Nacional

Esta ley fue emitida el 27 de setiembre de 1953, es la ley que define la integración del Sistema Bancario Nacional, las funciones que competen a los bancos, la obligatoriedad de los bancos a presentar a la SUGEF la información que esta defina.

Además, regula la dirección y administración de los bancos del Estado, las operaciones de los bancos comerciales, las operaciones de fomento de cooperativas y de los bancos hipotecarios.

3. Ley No. 4179: Ley de asociaciones cooperativas y creación del Instituto de Fomento Cooperativo

Ley emitida el 22 de agosto del 1968 mediante la cual se declara de conveniencia y utilidad pública, y de interés social, la constitución y funcionamiento de asociaciones cooperativas, por ser uno de los medios más eficaces para el desarrollo económico, social, cultural y democrático de los habitantes del país.[7]

---

[6] Recuperado el 13 de mayo 2020 de: https://www.bccr.fi.cr/seccion-sobre-bccr/sobre-bccr

[7] Recuperado el 13 de mayo 2020 de: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=2435&nValor3=0&strTipM=TC

Esta ley determina los privilegios y prohibiciones que tienen las asociaciones cooperativas, la clasificación de acuerdo con su funcionamiento, así como la constitución, administración y funcionamiento de estas.

4. **Ley No. 5044: Ley reguladora de empresas financieras no bancarias**

Se decretó el 22 de setiembre de 1972, en la cual se define el concepto de empresa financiera no bancaria y se establece al BCCR como el responsable de la aplicación de la ley y a la SUGEF como el responsable de la supervisión de las actividades de estas empresas.

Se definen las condiciones para funcionar, las prohibiciones, obligaciones, así como también la liquidez y solvencia requerida para operar y las sanciones junto con los recursos presentados ante un eventual incumplimiento a lo definido en esta ley.

5. **Ley No. 8204: Reforma integral Ley sobre estupefacientes, sustancias psicotrópicas, drogas de uso no autorizado, actividades conexas, legitimación de capitales y financiamiento al terrorismo**.

Se emitió el 11 de enero del 2002 y tiene como fin regular la prevención, el suministro, la prescripción, la administración, la manipulación, el uso, la tenencia, el tráfico y la comercialización de estupefacientes, psicotrópicos, sustancias inhalables y demás drogas y fármacos susceptibles de producir dependencias físicas o psíquicas. Dentro de la Ley, se definen las entidades sujetas a la ley reguladas, supervisadas y fiscalizadas por la SUGEF, SUGEVAL, SUPEN y SUGESE.

Cabe resaltar, que la JAFAP no se encuentra dentro de las instituciones reguladas por la SUGEF, sin embargo, aplica los lineamientos emitidos por esta como mejores prácticas para su operación.

1.1.3. Entorno Económico

En el siguiente apartado se realizará un análisis de principales factores influyentes en el entorno económico del mercado financiero costarricense.

1.1.3.1. Actividad Económica

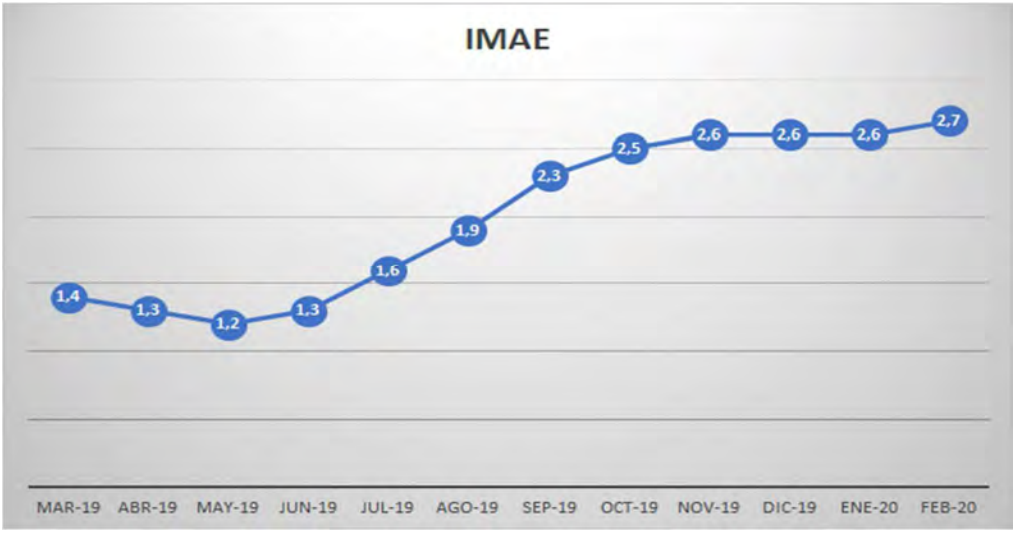
Desde aproximadamente el año 2016, la actividad económica de Costa Rica ha venido perdiendo el dinamismo con el que contaba años atrás, indica el BCCR (2020) “Un factor determinante en este proceso de desaceleración fue el rumbo insostenible de las finanzas públicas, que presionó al alza las tasas de interés y generó incertidumbre, con lo que desplazó la inversión

privada y el consumo". (p.1).

A partir de la aprobación de la reforma fiscal en el año 2018, los mercados financieros y cambiarios volvieron a la calma, sin embargo, se generó una incertidumbre sobre la sostenibilidad fiscal del país y el impacto que dicha reforma tendría en los hogares, empresas e industrias. Según estas reformas fiscales fueron asimiladas por consumidores y empresarios, se empezó a reflejar un repunte en la actividad económica del país.

Este repunte es reflejado en el Índice Mensual de Actividad Económica (IMAE), calculado por el BCCR el cual muestra el crecimiento de la actividad económica según se detalla a continuación:

Figura 1 Detalle de Índice Mensual de Actividad Económica



Fuente: elaboración propia con datos del Banco Central de Costa Rica.

1.1.3.2. Política Monetaria

Desde el mes de marzo 2019 el Banco Central de Costa Rica ha mantenido una postura monetaria expansiva, es decir, ha tratado de estimular el tamaño de la oferta monetaria del país, con el propósito de contribuir con el proceso de mejora de recuperación económica del país.

Como parte de esta postura del BCCR y producto de los bajos niveles de inflación que ha tenido el país en los últimos años, se han impulsado una serie de medidas dentro de las cuales se encuentran la reducción acumulada de la tasa de política monetaria, según se determina en el siguiente gráfico:

Figura 2 Detalle de Política Monetaria BCCR

Fuente: elaboración propia con datos del Banco Central de Costa Rica.

Otra de las medidas tomadas por el BCCR, consistió en la reducción del Encaje Mínimo Legal que las entidades financieras deben mantener en custodia en el BCCR pasando de un 15 % hasta un 12 %.

Esta flexibilización de la política monetaria indica el BCCR tiene como objetivo: "continuar con el mejoramiento de las condiciones para nuevos créditos y brindar alivio a deudores con préstamos a tasa variable y sin tasas piso" (p.5).

1.1.3.3. Inflación

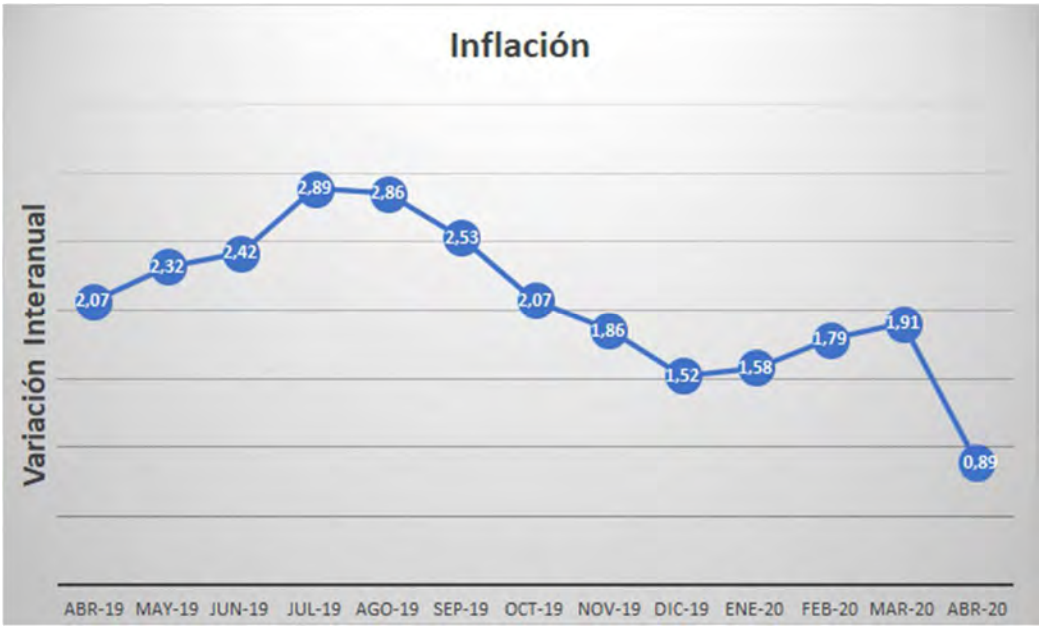
Durante el año 2019 la inflación la cual es medida por la variación interanual del Índice de Precios al Consumidor estuvo dentro del rango meta establecido por el BCCR en Programa Macroeconómico 2019-2020 al ubicarse dentro del rango meta definido (2,0% a 4,0%). Para el período 2020 la Junta Directiva del BCCR mantuvo la meta de inflación en 3 % ± 1 punto porcentual.

El comportamiento de la inflación durante el año 2020 se ha mantenido dentro de las metas establecidas por el BCCR, el cual afirma que: "Este comportamiento es coherente con la persistencia de condiciones macroeconómicas (entre otras, brecha negativa y creciente del producto

y alta tasa de desempleo) que presionan la inflación a la baja". (p. 2)

En el siguiente gráfico se observa el comportamiento de la inflación en el último año:

Figura 3 Detalle de Inflación



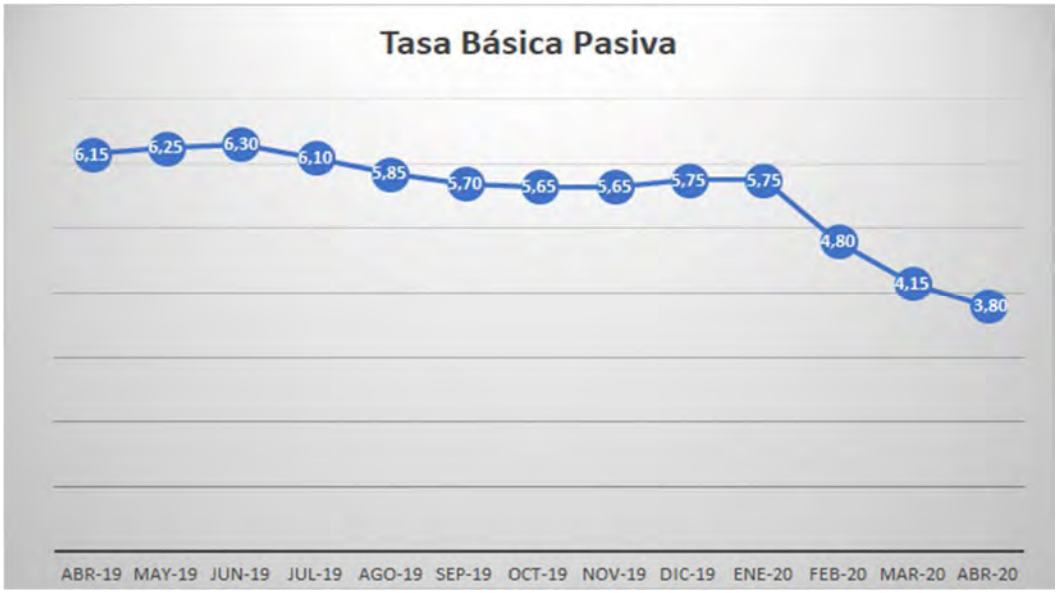
Fuente: elaboración propia con datos del Banco Central de Costa Rica.

1.1.3.4. Tasas de interés

Parte de las medidas tomadas por el BCCR indicadas anteriormente en el apartado de política monetaria, han contribuido en una mejora de las tasas de interés ofrecidas en el sistema bancario nacional, lo cual genera un beneficio en los deudores, así como en mejores condiciones para la oferta de créditos disponibles en el mercado.

A continuación, se presenta el comportamiento de la tasa básica pasiva en el último año.

Figura 4 Detalle de Tasa Básica Pasiva



Fuente: elaboración propia con datos del Banco Central de Costa Rica.

1.1.3.5. Desempleo

En los últimos años, se ha dado un incremento en las tasas de desempleo en Costa Rica, a saber, uno de los mayores problemas de relevancia en la economía costarricense que genera profundas implicaciones socioeconómicas y, que a su vez, tiene otros efectos macroeconómicos como por ejemplo los niveles de inflación.

Dentro de las principales causas del desempleo el incremento en los últimos años afirma el BCCR (2020): "Una causa del elevado desempleo estructural en la última década es el dualismo de la estructura productiva. Esto es, la bifurcación de la producción en actividades dinámicas relacionadas con las exportaciones de bienes y servicios, especialmente de zona franca, y otras orientadas a la economía interna que se han estancado y en las que las condiciones laborales (empleo y salarios reales) han empeorado, especialmente a partir del 2018, con la pérdida de dinamismo de la actividad económica. (p. 20)

A continuación, se presenta el comportamiento trimestral de las tasas de desempleo durante los dos últimos años:

Figura 5 Detalle de Tasa de Desempleo

Fuente: elaboración propia con datos del Banco Central de Costa Rica.

1.2. Conceptos teóricos sobre Control Interno aplicable en procesos contables y tecnologías de información

1.2.1. Conceptos generales de Control Interno

Para el desarrollo de este trabajo es importante definir Control Interno y diversos conceptos relacionados utilizados para la propuesta del modelo de Control Interno en el proceso contable de la JAFAP, con el objetivo de dar un entendimiento a nivel general.

Según ISACA (2012) se define control como: "Los medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras organizativas, que pueden

tener una naturaleza administrativa, técnica, de gestión, o legal. También usada como sinónimo de salvaguarda o contramedida".

Por otra parte, se define control como: "Cualquier medida que tome la administración, el consejo y otras partes para administrar los riesgos e incrementar la posibilidad de alcanzar las metas y objetivos establecidos. La administración planea, organiza y dirige la realización de acciones suficientes para proporcionar seguridad razonable de que se alcanzarán los objetivos y las metas" (Santillana, 2013).

Para un mayor alcance de los objetivos empresariales de una compañía es importante que la misma cuente con controles internos adecuados, por lo tanto se define Control Interno según el C*ommittee of Sponsoring Organizations of the Treadway Commision, COSO* (2013) como un proceso, efectuado por la junta directiva de una entidad, administración y otro personal, diseñado para proporcionar una seguridad razonable con respecto al logro de los objetivos relacionados con las operaciones, informes y cumplimiento.

También, se define Control Interno como: "conjunto de métodos y procedimientos que aseguren que los activos están debidamente protegidos, que los registros contables son fidedignos y que la actividad de la Entidad se desarrolla eficazmente según las directrices marcadas por la administración" (Estupiñán, 2006, pág.19).

El Control Interno permite a las organizaciones obtener una serie de beneficios en su operación, por ejemplo, brinda mayor confianza a la gerencia y las juntas directivas con respecto al logro de los objetivos, además de brindar retroalimentación sobre el funcionamiento del negocio y contribuye a la reducción de las sorpresas (COSO, 2013).

Es importante definir Procesos de control, ya que estos son el medio para lograr los objetivos del Control Interno, según Santillana (2013) se definen como: Políticas, procedimientos (tanto manuales como automatizados) y actividades que forman parte del marco de control, diseñados y operados para asegurar que los riesgos estén contemplados dentro de los límites de tolerancia que una Organización está dispuesta a aceptar.

Por otra parte, ISACA (2012) define sistema de Control Interno como las políticas, estándares, planes, procedimientos y las estructuras organizativas diseñadas para proveer una garantía razonable de que los objetivos de la empresa van a conseguirse y los eventos no deseados

serán evitados o detectados y subsanados.

Según la Ley No. 8292 Ley General de Control Interno se define sistema de Control Interno como: una serie de acciones ejecutadas por la administración activa, diseñadas para proporcionar seguridad en la consecución de los siguientes objetivos:[8]

a) Proteger y conservar el patrimonio público contra cualquier pérdida, despilfarro, uso indebido, irregularidad o acto ilegal.

b) Exigir confiabilidad y oportunidad de la información.

c) Garantizar eficiencia y eficacia de las operaciones.

d) Cumplir con el ordenamiento jurídico y técnico.

El cumplimiento de objetivos empresariales provoca que las compañías se encuentren expuestas a riesgos generales del negocio, según el *Committee of Sponsoring Organizations of the Treadway Commission* (2013) riesgo se define como la posibilidad de que ocurra un evento y afecte adversamente el logro de objetivos.

Por otra parte, se define riesgo como: la posibilidad de que ocurra un evento adverso que influya en el logro de los objetivos. El riesgo se mide en términos de probabilidad e impacto (Santillana, 2013).

Las organizaciones se pueden enfrentar a riesgos externos e internos, algunos de estos son económicos, políticos, ambientales, tecnológicos, contables, operacionales, de personal, entre otros. La afectación de cada uno dependerá del tipo de negocio en el cual se desenvuelve la compañía.

Debido a que un riesgo puede impactar de manera significativa los objetivos de una compañía es de vital importancia gestionar los riesgos, por lo tanto se define como: Reconocer un riesgo; evaluar su impacto y probabilidad; y desarrollar estrategias, como, por ejemplo, evitar el riesgo, reduciendo el efecto negativo de riesgo o transfiriendo el riesgo, para gestionarlo en el

[8] Recuperado el 18 de abril 2020 de: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=49185&nValor3=52569&strTipM=TC

contexto del apetito de riesgo de una empresa (ISACA, 2012).

Así mismo se define gestión de riesgos como el: proceso sistemático de identificar, medir, evaluar, controlar, dar seguimiento e informar, los distintos tipos de riesgos que podrían afectar la consecución de los objetivos de la Entidad y los fondos administrados. La gestión de riesgos permite seleccionar entre las posibles alternativas de respuesta a ellos, es decir evitarlos, reducirlos, compartirlos o aceptarlos (SUPEN, 2017).

1.2.2. Tecnologías de información en procesos contables

El uso de las Tecnologías de Información (en adelante TI) actualmente han proporcionado a las organizaciones un nuevo enfoque de trabajo, ya que las mismas han permitido a las empresas aumentar la productividad, competitividad, seguridad de la información, aplicación de controles, disponibilidad de la información, disminución de costos y tiempos de los procesos, lo cual genera mayor eficiencia y eficacia en las operaciones.

Las empresas, como parte de su negocio, generan una gran cantidad de información utilizada para evaluar su funcionamiento, aumentar capacidades, transformar su manera de trabajar, entre otras, por lo cual las TI permiten tomar esa información y convertirla en un producto más amigable en cuanto a su utilización, dicha información puede ser más confiable, consistente y estar accesible para cuando se requiera analizar tanto a nivel interno como de usuarios externos.

Aunado a lo anterior, el cumplimiento de los objetivos organizacionales mediante la utilización de TI provoca la exposición a riesgos específicos de TI, los cuales según la SUGEF (2017) se definen como la posibilidad de pérdidas económicas derivadas de un evento relacionado con el acceso o uso de la tecnología, que afecta la capacidad de la Entidad para funcionar de manera efectiva y la adecuada gestión de riesgos, al atentar contra la confidencialidad, integridad, disponibilidad, eficiencia, confiabilidad y oportunidad de la información.

Los riesgos en general y específicamente de TI van a estar presentes en las empresas tanto de manera inherente como por situaciones provocadas por decisiones tomadas por la administración. Las empresas no pueden eliminar por completo estos riesgos, aun cuando algunos de estos no son controlables, sin embargo, es posible intervenir y mitigar los riesgos para no afectar la rentabilidad y el objetivo del negocio, así mismo estar preparados para eventuales situaciones que pueden traer impactos a nivel económico y funcional.

Para mitigar los riesgos generados en el giro normal del negocio y mejorar continuamente las labores empresariales, cada Organización necesita trabajar de la mano de los sistemas de información contables y procesos contables, de acuerdo con Horngren, C. (Citado por Mora, 2017) los "Sistemas de información contable son quizás una de las bases de las actividades empresariales, por no decir que es la más importante dentro del campo de los negocios, dada su naturaleza de informar acerca del incremento de la riqueza, la productividad y el posicionamiento de las empresas en los ambientes competitivos, por lo que es imperioso que vaya al ritmo de las exigencias de los distintos usuarios dentro y fuera de la entidad". (pág. 9)

Actualmente para el adecuado funcionamiento de los procesos contables es necesario la utilización de sistemas de información, las organizaciones se desempeñan en entornos económicos altamente competitivos que las obliga a mejorar sus procesos internos en búsqueda de una mejora continua para maximizar su rentabilidad. Para que los sistemas de información contables tengan una mayor eficiencia deben contar con personal capacitado a cargo de funciones específicas que en conjunto con las TI permitan generar información valiosa para la toma de decisiones empresariales, mitigar riesgos y satisfacer las necesidades de información contable de la Organización.

El uso de las TI en los procesos contables permite una adecuada gestión empresarial y el cumplimiento de los requisitos mínimos de Control Interno, así como la minimización de riesgos asociados y generación de valor a través de un uso eficaz de las TI, por lo tanto, produce así una relación entre las TI y los procesos contables.

Son de particular interés para este objetivo de estudio los procesos de contabilidad, así como también los de tecnologías de información relacionados con dichos procesos contables y cómo estos influyen en la Organización. Tales procesos contables, a su vez, suelen tener relación e impacto con otros sistemas institucionales, a saber, el sistema de Control Interno; Posso (2014) define el Control Interno contable como los controles y métodos establecidos para garantizar la protección de los activos y la fiabilidad y validez de los registros y sistemas contables. Es decir, la relación de los procesos contables con el Control Interno tiene como objetivo final el logro de los objetivos de la Organización a través de la integridad de sus registros e información financiera.

Debido al impacto presente en la información contable y cómo esta influye en el logro de los objetivos de la Organización, es importante que la alta gerencia y la administración, según sus

competencias, emprendan las medidas pertinentes para asegurar que se establezcan y se mantengan actualizados registros contables y presupuestarios los cuales brinden un conocimiento razonable y confiable de las disponibilidades de recursos, las obligaciones adquiridas por la institución, las transacciones y eventos realizados (Contraloría General de la República, 2009).

Debido a lo anterior es fundamental una relación directa entre el Control Interno contable y el control de tecnologías de información los cuales corresponden a controles que soportan la gestión de negocios, de Gobierno y proporcionan controles generales y técnicos sobre la infraestructura de tecnología de la información, tales como aplicaciones, información, infraestructura y personal (Santillana, 2013).

Los controles internos deben abarcar todas las áreas de la empresa, trabajan de manera individual y conjunta, pues ha sido fundamental que dichos controles abarquen todas las deficiencias enfrentadas por las compañías. El uso de las TI busca maximizar resultados y lograr objetivos, por ende, se deben aplicar controles internos para que la administración obtenga los beneficios esperados para los cuales fue implementado TI en conjunto con los procesos contables.

Dado lo anterior la administración debe ser, a su vez, un Gobierno de tecnologías de información el cual consiste en el liderazgo, las estructuras de Organización y los procesos que aseguran que la tecnología de la información de la empresa mantiene, soporta las estrategias y objetivos de la Organización (Santillana, 2013).

1.2.3. Teorías aplicables al Control Interno enfocado en tecnologías de información.

A nivel internacional existen diversas teorías de Control Interno aplicables a tecnologías de información las cuales sustentan la creación de modelos o ser utilizados como soporte por las compañías. En el presente trabajo de investigación se tomarán en consideración la ISO 31000:2011, COBIT 5, ITIL y COSO como base teórica en el desarrollo de la propuesta, por lo cual se describen los aspectos más importantes de cada una de las teorías.

ISO 31000:2011. Gestión del riesgo. Principios y directrices

Todas las compañías están expuestas a situaciones de riesgo por el giro normal de negocio, por lo tanto esta norma pretende que pueda ser aplicada por cualquier tipo de industria y sector, ya sea empresa pública o privada, sin distinción de tamaño. Así mismo, la norma específica que “Esta

norma se puede aplicar a cualquier tipo de riesgo, cualquiera que sea su naturaleza, y tanto si sus consecuencias son positivas o negativas" (ISO 31000:2011 Gestión del riesgo. Principios y directrices). Por lo anterior, esta norma permite su aplicación en riesgos específicos de TI y, por ende se utilizará como fundamento teórico en el desarrollo del trabajo de investigación.

El objetivo fundamental de la norma es que sea utilizada para armonizar los procesos de gestión del riesgo establecidos en las normas existentes o futuras. Proporciona un enfoque común en el apoyo de las normas que tratan riesgos o sectores específicos y no sustituye a dichas normas (ISO 31000: 2011.Gestión del riesgo. Principios y directrices).

La norma ISO 31000:2011 Gestión del riesgo. Principios y directrices proporciona los siguientes principios sobre la gestión del riesgo:

a) La gestión del riesgo crea y protege el valor: la gestión del riesgo contribuye de manera tangible al logro de los objetivos y a la mejora del desempeño, por ejemplo, en lo referente a la salud y seguridad de las personas, a la conformidad con los requisitos legales y reglamentarios, a la aceptación por el público, protección ambiental, calidad del producto, gestión del proyecto, eficacia en las operaciones y a su gobernanza y reputación.

b) La gestión del riesgo es una parte integral de todos los procesos de la Organización: la gestión del riesgo no es una actividad independiente separada de las actividades y procesos principales de la Organización. La gestión del riesgo es parte de las responsabilidades de gestión y una parte integral de todos los procesos de la Organización, incluida la planificación estratégica y todos los procesos de la gestión de proyectos y de cambios.

c) La gestión del riesgo es parte de la toma de decisiones: la gestión del riesgo ayuda a las personas quienes toman decisiones a realizar elecciones informadas, a definir las prioridades de las acciones y a distinguir entre planes de acción alternativos.

d) La gestión del riesgo trata explícitamente la incertidumbre: la gestión del riesgo tiene en cuenta explícitamente la incertidumbre, la naturaleza de esa incertidumbre y la manera en que se puede tratar.

e) La gestión del riesgo es sistemática, estructurada y oportuna: un enfoque sistemático, oportuno y estructurado de la gestión del riesgo contribuye a la eficacia y a resultados coherentes, comparables y fiables.

f) La gestión del riesgo se basa en la mejor información disponible: los elementos de entrada del proceso de gestión del riesgo se basan en fuentes de información, tales como datos históricos, experiencia, retroalimentación de las partes interesadas, observación, previsiones y juicios de expertos. No obstante, las personas quienes toman decisiones deberían informarse y tener en cuenta todas las limitaciones de los datos o modelos utilizados, así como las posibles divergencias entre expertos.

g) La gestión del riesgo es a la medida: la gestión del riesgo se alinea con el contexto externo e interno de la Organización y con el perfil del riesgo.

h) La gestión del riesgo integra los factores humanos y culturales: la gestión del riesgo permite identificar las aptitudes, las percepciones y las intenciones de las personas externas e internas quienes facilitan u obstruyen el logro de los objetivos de la Organización.

i) La gestión del riesgo es transparente y participativa: la implicación apropiada y oportuna de las partes interesadas y, en particular, de las personas que toman decisiones a todos los niveles de la Organización, asegura que la gestión del riesgo se mantenga pertinente y actualizada. El involucramiento también permite a las partes interesadas estar correctamente representadas y que sus opiniones se tomen en cuenta en la determinación de los criterios de riesgo.

j) La gestión del riesgo es dinámica, iterativa, y responde a los cambios: la gestión del riesgo es sensible de manera continuada a los cambios y responde a ellos. Cómo se producen eventos externos e internos, el contexto y los conocimientos cambian, se realiza el seguimiento y la revisión de riesgos, surgen nuevos riesgos, algunos cambian y otros desaparecen.

k) La gestión del riesgo facilita la mejora continua de la Organización: las organizaciones deberían desarrollar e implementar estrategias para mejorar su madurez en la gestión del riesgo en todos los demás aspectos de la Organización.

Esta norma pretende ser adaptada a cada empresa según las necesidades y al sector que pertenezca, algunos de los beneficios aportados por la aplicación a las compañías son los siguientes, según lo establecido en la Norma ISO 31000:2011 Gestión del riesgo. Principios y directrices:

- Aumentar la posibilidad de alcanzar los objetivos;
- Estimular una gestión proactiva;

- Ser consciente de la necesidad de identificar y tratar el riesgo en toda la Organización;
- Mejorar la identificación de oportunidades y de amenazas;
- Cumplir los requisitos legales y reglamentarios pertinentes y las normas internacionales;
- Mejorar los informes obligatorios y voluntarios;
- Mejorar la gobernanza;
- Mejorar la seguridad y la confianza de las partes interesadas;
- Establecer una base fiable para la toma de decisiones y la planificación;
- Mejorar los controles;
- Asignar y utilizar de manera eficaz los recursos para el tratamiento del riesgo;
- Mejorar la eficacia y la eficiencia operacional;
- Aumentar las prestaciones en materia de salud y seguridad,
- Así como la protección ambiental;
- Mejorar la prevención de pérdidas y la gestión de incidentes;
- Minimizar las pérdidas;
- Mejorar el aprendizaje de la Organización; y
- Mejorar la resiliencia de la Organización.

COBIT

COBIT 5, corresponde a un marco de negocio para el Gobierno y la gestión de las tecnologías de información de las empresas, el cual pretende que las organizaciones generen valor desde las TI, al disminuir la exposición a los riesgos y con un adecuado uso de los recursos.

Este marco de referencia está basado en cinco principios claves para el Gobierno y la gestión de las tecnologías de información, estos principios son:

1. Satisfacer las necesidades de las partes interesadas
2. Cubrir la empresa extremo a extremo
3. Aplicar un marco de referencia único integrado
4. Hacer posible un enfoque holístico.
5. Separar al Gobierno de la gestión.

Estos cinco principios planteados por COBIT permiten que las organizaciones desarrollen un marco para el Gobierno y administración de TI de una manera holística, consideran el negocio, así como todas las áreas funcionales, enfocándose así en todas las partes interesadas de la Organización, ya sean internas o externas.

Además de estos principios, COBIT 5 plantea siete catalizadores o habilitadores, define catalizadores como factores que, individual y colectivamente, influyen sobre si algo funcionará, para este caso, el Gobierno y la gestión de la empresa en TI (ISACA, 2012). Los catalizadores son:

1. Principios, políticas y marcos de trabajo.
2. Procesos.
3. Estructuras organizativas.
4. Cultura, ética y comportamiento.
5. Información.
6. Servicios, infraestructuras y aplicaciones.
7. Personas, habilidades y competencias.

Tal y como se mencionó anteriormente, COBIT 5 consta de cinco principios claves para el Gobierno y gestión de TI, dichos principios son genéricos y útiles para cualquier tipo y tamaño de Organización, es decir, grandes o pequeñas empresas, sector público o privado. Cada uno de estos principios brinda una guía de buenas prácticas y estándares para aplicar en las organizaciones, según detalla ISACA (2012) estos principios son:

Principio 1. Satisfacer las Necesidades de las Partes Interesadas: las empresas existen para crear valor para sus partes interesadas manteniendo el equilibrio entre la realización de beneficios y la optimización de los riesgos y el uso de recursos. COBIT 5 provee todos los procesos necesarios y otros catalizadores para permitir la creación de valor del negocio mediante el uso de TI. Dado que toda empresa tiene objetivos diferentes, una empresa puede personalizar COBIT 5 para adaptarlo a su propio contexto mediante la cascada de metas, traduce metas corporativas de alto nivel en otras metas más manejables, específicas, relacionadas con TI y mapeándolas con procesos y prácticas específicos.

Principio 2: Cubrir la Empresa Extremo-a-Extremo: COBIT 5 integra el Gobierno y la gestión de TI en el Gobierno corporativo:

1. Cubre todas las funciones y procesos dentro de la empresa; COBIT 5 no se enfoca solo en la "función de TI", sino que trata la información y las tecnologías relacionadas como activos que deben ser tratados como cualquier otro activo por todos en la empresa.

2. Considera que los catalizadores relacionados con TI para el Gobierno y la gestión deben ser a nivel de toda la empresa y de principio a fin, es decir, incluye a todo y todos – internos y externos – relevantes para el Gobierno y la gestión de la información de la empresa y TI relacionadas.

Principio 3: Aplicar un Marco de Referencia único integrado: hay muchos estándares y buenas prácticas relativos a TI, ofrece cada uno ayuda para un subgrupo de actividades de TI. COBIT 5 se alinea a alto nivel con otros estándares y marcos de trabajo relevantes y, de este modo, cumple la función de marco de trabajo principal para el Gobierno y la gestión de las TI de la empresa.

Principio 4: Hacer Posible un Enfoque Holístico: un Gobierno y gestión de las TI de la empresa efectivo y eficiente requiere de un enfoque holístico que tenga en cuenta varios componentes interactivos. COBIT 5 define un conjunto de catalizadores (*enablers*) para apoyar la implementación de un sistema de Gobierno y gestión global para las TI de la empresa. Los catalizadores se definen en líneas generales como cualquier recurso para conseguir las metas de la empresa. El marco de trabajo COBIT 5 define siete categorías de catalizadores:

– Principios, Políticas y Marcos de Trabajo

– Procesos

– Estructuras Organizativas

– Cultura, Ética y Comportamiento

– Información

– Servicios, Infraestructuras y Aplicaciones

– Personas, Habilidades y Competencias

Principio 5: Separar el Gobierno de la Gestión: el marco de trabajo COBIT 5 establece una clara distinción entre Gobierno y gestión. Estas dos disciplinas engloban diferentes tipos de actividades, requieren diferentes estructuras organizativas y sirven a diferentes propósitos. La visión de COBIT 5 en esta distinción clave entre Gobierno y gestión es:

Gobierno: el Gobierno asegura la evaluación de las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas, establece la dirección a través de la priorización, la toma de decisiones y mide el rendimiento, el cumplimiento respecto a la dirección y metas acordadas.

En muchas corporaciones, el Gobierno global es responsabilidad del comité de dirección bajo el liderazgo del presidente. Algunas responsabilidades de Gobierno específicas se pueden delegar en estructuras organizativas especiales al nivel apropiado, particularmente en las corporaciones más grandes y complejas.

Gestión: la gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de Gobierno para alcanzar las metas empresariales. En muchas empresas, la gestión es responsabilidad de la dirección ejecutiva bajo el liderazgo del Director General Ejecutivo (CEO).

Dados los conceptos, tanto el Gobierno como la gestión comprenden diversos tipos de actividades, requieren diferentes estructuras organizacionales y cumplen múltiples propósitos.

ITIL

Information Technology Infraestructure Library (ITIL) corresponde a una serie de libros que brindan recursos para mejorar la Gestión de los Servicios de Tecnologías de Información mediante estándares y mejores prácticas. El ITIL puede ser implementado por cualquier compañía que desee aumentar la eficiencia en el diseño y administración de infraestructura de datos.

Según Ramírez y Donoso (2006) el principal objetivo de ITIL es diseminar las mejores prácticas en la gestión de servicios de Tecnologías de Información de forma sistemática y coherentemente. El planteo principal se basa en la calidad de servicio y el desarrollo eficaz y eficiente de los procesos. La idea subyacente es que, sin importar el rubro, la tecnología es cada vez más crítica para el negocio de cualquier empresa. En otras palabras, si la tecnología no es

administrada eficientemente, el negocio no funciona, esto se vuelve más cierto al ser más dependiente de la infraestructura tecnológica. En este sentido, los estándares ITIL exigen un replanteamiento del área tecnológica, la definición de los elementos y procesos "críticos" dentro de la empresa.

Los principales beneficios generados por la implementación de ITIL en las compañías según Ramírez y Donoso (2006) son los siguientes:

a) Para el negocio:

- Incremento en la productividad del negocio: Mayor disponibilidad y fiabilidad de las Tecnologías de Información.
- Mejora continua en la calidad de la prestación del servicio de las Tecnologías de Información, ya que tiene en cuenta tanto las necesidades de la compañía como sus objetivos. Existe una mejora en el alineamiento Tecnología – Negocio.
- La reducción del riesgo de no cumplir los objetivos de negocio gracias a la capacidad de recuperación y a la consistencia de los servicios.
- Mayor flexibilidad y en consecuencia un mejor alcance de las acciones de la Organización frente a cambios del entorno y el mercado. Posicionándose así en un soporte fiable para el negocio.
- Soporte para los procesos de negocios y las tareas de toma de decisiones de TI. Mediante la puesta en marcha de servicios basados en principios metodológicos y de calidad acordes con los requerimientos presentes y futuros de la compañía.
- Mejora en la satisfacción de los clientes, ya que se les asegura una mejora en la calidad del servicio entregado.
- El servicio puede ser representativamente medido, evaluado y gestionado.
- Definición de funciones, papeles y responsabilidades en el sector de los servicios.
- La posibilidad de auditar el cumplimiento de las mejores prácticas.
- Mejora en la satisfacción de los empleados y reducción de fluctuaciones de nivel de personal.
- Incremento cualitativo en la salud, la seguridad, la disponibilidad y el rendimiento de los servicios de ITIL.

b) Económicos:

- Diseño de la infraestructura y servicios de las Tecnologías de Información a costos argumentados.
- Reducción de los costos operativos de desarrollo, procedimientos e instrucciones de trabajo, al disponer, de un marco de trabajo definido.
- Además, mejora el ROI y reduce el TCO a través de la mejora de los procesos.

c) Comunidad de usuarios de TI: ITIL es comprensible e integral. ITIL crea un vocabulario común.

En la última versión de ITIL del 2019, se desarrolla el Sistema de Valor de Servicio (SVS) que es un conjunto de componentes y actividades de la compañía que permiten la creación de valor.

El Sistema de Valor de Servicio (SVS) incluye los siguientes componentes según Hiberus tecnología (2019)[9]:

Principios básicos: recomendaciones para guiar a una Organización en todas las circunstancias, independientemente de los cambios en sus objetivos, estrategias, tipo de trabajo o estructura de gestión.

Gobernanza: los medios por los cuales una Organización es dirigida y controlada.

Cadena de valor del servicio: un conjunto de actividades interconectadas realizadas por una Organización para entregar un producto o servicio valioso a sus consumidores y facilitar la realización del valor.

Prácticas: conjuntos de recursos organizacionales diseñados para realizar tareas o lograr un objetivo.

Mejora continua: una actividad organizativa recurrente realizada en todos los niveles para garantizar que el desempeño de una Organización cumpla con las expectativas de los interesados.

COSO

El informe COSO corresponde a un modelo que fue elaborado y es actualizado por el *Committe of Sponsoring Organizations of the Treadway Commission* (COSO), el mismo contiene directivas para la implementación, gestión y control de un sistema de control que permita a la administración obtener seguridad en sus procesos para el cumplimiento de objetivos.

[9] Recuperado el 02 de mayo 2020 de: https://www.hiberus.com/crecemos-contigo/novedades-itil-v4/

Según la Organización Latinoamericana y del Caribe de Entidades Fiscalizadoras Superiores (2015) el marco COSO establece tres categorías de objetivos para tomar en consideración cuando se aplique dicho enfoque de Control Interno, los mismos son los siguientes:

De operación. Se refiere a la eficacia y la eficiencia de las operaciones de la Entidad en donde se incluyen metas de desempeño operativo y financiero, así como la protección de los activos contra pérdidas.

De informes. Se refiere a los reportes internos y externos, financieros y no financieros que deben elaborarse y presentarse en términos de fiabilidad, oportunidad, transparencia y otras condiciones establecidas por los organismos reguladores, órganos normativos o políticas internas de la Entidad.

De cumplimiento. Se refiere a la adhesión y observancia de las leyes y reglamentos a los que está sujeta la Entidad.

En el enfoque COSO se establecen cinco componentes de Control Interno que según la Organización Latinoamericana y del Caribe de Entidades Fiscalizadoras Superiores (2015) son los siguientes:

Ambiente de control: es la base del sistema de Control Interno y aporta disciplina a la estructura. En él se apoyan los restantes componentes y resulta fundamental para concretar los cimientos de un Control Interno eficaz y eficiente, pues marca la pauta del funcionamiento de la Organización e influye en la forma de actuación de sus funcionarios. Sus factores incluyen la integridad y los valores éticos, la capacidad de los funcionarios, el estilo de dirección y gestión, la asignación de autoridad, responsabilidad, la estructura organizacional, las políticas y prácticas de personal utilizadas.

Evaluación de riesgos: consiste en la identificación y el análisis de los riesgos relevantes para la consecución de los objetivos y sirve de base para determinar 20 cómo deben ser gestionados. Tiene como condición previa la identificación de los objetivos a los distintos niveles, los cuales deben estar vinculados entre sí.

Actividades de control: son las políticas, los procedimientos, las técnicas, las prácticas y los mecanismos que permiten a la Dirección administrar los riesgos identificados con base en la evaluación de riesgos y asegurar que se llevan a cabo los lineamientos establecidos. Se ejecutan en

todos los niveles de la Organización y en cada una de las etapas de la gestión.

Información y comunicación: según este componente, se debe identificar, recopilar y propagar la información pertinente en tiempo y forma para cumplir a cada funcionario con sus responsabilidades a cargo. De igual modo, debe existir una comunicación eficaz que fluya en todas direcciones a través de todos los ámbitos de la Organización, tanto de forma descendente como ascendente.

Supervisión y seguimiento: el sistema de Control Interno precisa de supervisión, es decir, un proceso que verifique la vigencia del sistema a lo largo del tiempo. Esto se logra mediante actividades de supervisión continuada, evaluaciones periódicas o una combinación de ambas.

1.2.4. Teorías aplicables al Control Interno enfocado en tecnologías de información en el mercado costarricense.

1.2.4.1. Reglamento General de Gestión de la tecnología de información, CONASSIF.

Este Reglamento tiene como objetivo establecer una serie de requerimientos para la gestión de TI, cumplidos por todas las compañías que forman parte del sistema financiero de este país y por tanto son entidades supervisadas y reguladas.

Según el Reglamento General de Gestión de la Tecnología de Información (2017), las disposiciones establecidas en el mismo son de aplicación para las siguientes entidades financieras:

a) Supervisados por SUGEF.

b) Supervisados por SUGEVAL.

c) Supervisados por SUGESE.

d) Supervisados por SUPEN.

Se exceptúan los regímenes administrados por la Dirección Nacional de Pensiones del Ministerio de Trabajo, las entidades reguladas y fondos en proceso de liquidación, los fondos creados por leyes especiales cuya gestión de TI es contratada a una operadora de pensiones, así como los fondos de pensiones cerrados a nuevas afiliaciones.

En el Reglamento General de Gestión de la tecnología de información se determinan los procesos implementados por las entidades financieras supervisadas. Cada Entidad debe establecer

cuáles son los procesos más adecuados para su Marco de Gestión de TI, los mismos deben ser implementados de manera gradual, por lo tanto, las entidades supervisadas por la SUGEF cuentan con un máximo de tres años y las demás entidades con cinco años, esto a partir de fecha en la que entró a vigencia dicho reglamento.

Según el Anexo I del Reglamento General de Gestión de la tecnología de información (2017), los procesos para el Marco de Gestión de las entidades financieras supervisadas son los siguientes:

Asegurar el establecimiento y mantenimiento del marco de referencia de Gobierno: analiza y articula los requerimientos para el Gobierno de TI de la empresa y pone en marcha y mantiene efectivas las estructuras, procesos y prácticas facilitadoras, con claridad de las responsabilidades, la autoridad para alcanzar la misión, las metas y objetivos de la empresa.

Asegurar la Entrega de Beneficios: optimizar la contribución al valor del negocio desde los procesos de negocio, de los servicios TI y activos de TI resultado de la inversión hecha por TI a unos costos aceptables.

Asegurar la Optimización del Riesgo: asegurar que el apetito y la tolerancia al riesgo de la empresa son entendidos, articulados, comunicados y que el riesgo para el valor de la empresa relacionado con el uso de las TI es identificado y gestionado.

Asegurar la Optimización de Recursos: asegurar que las adecuadas y suficientes capacidades relacionadas con las TI (personas, procesos y tecnologías) están disponibles para soportar eficazmente los objetivos de la empresa a un coste óptimo.

Asegurar la Transparencia hacia las Partes Interesadas: asegurar que la medición y la elaboración de informes en cuanto a conformidad y desempeño de TI de la empresa son transparentes, con aprobación por parte de las partes interesadas de las metas, las métricas y las acciones correctivas necesarias.

Gestionar el Marco de Gestión de TI: aclarar y mantener el Gobierno de la misión y la visión corporativa de TI. Implementar, 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.

Gestionar la Estrategia: proporcionar una visión holística del negocio actual y del entorno de TI, la dirección futura y las iniciativas necesarias para migrar al entorno deseado. Aprovechar los bloques, componentes de la estructura empresarial, incluso los servicios externalizados y las capacidades relacionadas que permitan una respuesta ágil, confiable y eficiente a los objetivos estratégicos.

Gestionar la Arquitectura Empresarial: establecer 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 describen las líneas de partida y las arquitecturas objetivo. Definir los requisitos para la taxonomía, las normas, las directrices, los procedimientos, las plantillas, las herramientas y proporcionar un vínculo para estos componentes. Mejorar la adecuación, aumentar la agilidad, mejorar la calidad de la información y generar ahorros de costos potenciales mediante iniciativas tales como la reutilización de bloques de componentes para los procesos de construcción.

Gestionar el Portafolio: ejecutar el conjunto de direcciones estratégicas para la inversión alineada con la visión de la arquitectura empresarial, las características deseadas de inversión, los portafolios de servicios relacionados, considerar las diferentes categorías de inversión y recursos y las restricciones de financiación. Evaluar, priorizar y equilibrar programas, servicios, gestionar la demanda con los recursos y restricciones de fondos, basados en su alineamiento con los objetivos estratégicos, así como en su valor y riesgo corporativo. Mover los programas seleccionados al portafolio de servicios activos listos para ser ejecutados. Supervisar el rendimiento global del portafolio de servicios y programas, propone ajustes si fuesen necesarios en respuesta al rendimiento de programas, servicios o al cambio en las prioridades corporativas.

Gestionar el Presupuesto y los Costos: gestionar las actividades financieras relacionadas con las TI tanto en el negocio como en las funciones de TI, abarca presupuesto, costo, gestión del beneficio y la priorización del gasto mediante el uso de prácticas presupuestarias formales y un sistema justo y equitativo de reparto de costos a la empresa. Consultar a las partes interesadas para identificar, controlar los costos totales, los beneficios en el contexto de los planes estratégicos, tácticos de TI e iniciar acciones correctivas cuando sea necesario.

Gestionar los Recursos Humanos: proporcionar un enfoque estructurado para garantizar una óptima estructuración, ubicación, capacidades de decisión y habilidades de los recursos humanos. Esto incluye la comunicación de las funciones, responsabilidades definidas, la formación, planes de desarrollo personal y las expectativas de desempeño con el apoyo de gente competente y motivada.

Gestionar las relaciones: gestionar las relaciones entre el negocio, TI de modo formal y transparente, enfocándose hacia el objetivo común de obtener resultados empresariales exitosos apoyando los objetivos estratégicos, dentro de las restricciones del presupuesto y los riesgos tolerables. Basar la relación en la confianza mutua, usa términos entendibles, lenguaje común y voluntad de asumir la propiedad y responsabilidad en las decisiones claves.

Gestionar los acuerdos de servicio: alinear los servicios basados en TI y los niveles de servicio con las necesidades, expectativas de la empresa, incluso identificación, especificación, diseño, publicación, acuerdo, supervisión de los servicios TI, niveles de servicio e indicadores de rendimiento.

Gestionar los Proveedores: administrar todos los servicios de TI prestados por todo tipo de proveedores para satisfacer las necesidades del negocio, incluso la selección de los proveedores, la gestión de las relaciones, la gestión de los contratos, la revisión y supervisión del desempeño, para una eficacia y cumplimiento adecuados, minimiza el riesgo que los proveedores no cumplan.

Gestionar la Calidad: definir y comunicar los requisitos de calidad en todos los procesos, procedimientos y resultados relacionados de la Organización, además los controles, vigilancia constante, el uso de prácticas probadas, estándares de mejora continua y esfuerzos de eficiencia.

Gestionar el Riesgo: Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa. Integrar la gestión de riesgos empresariales relacionados con TI con la gestión de riesgos empresarial.

Gestionar la Seguridad: definir, operar y supervisar un sistema para la gestión de la seguridad de la información. Mantener el impacto y ocurrencia de los incidentes de la seguridad de la información dentro de los niveles de apetito de riesgo de la empresa.

Gestión de Programas y Proyectos: gestionar todos los programas y proyectos del portafolio de inversiones de forma coordinada y en línea con la estrategia corporativa. Iniciar, planificar, controlar, ejecutar programas**,** proyectos y cerrarlos con una revisión post-implementación.

Gestionar la Definición de Requisitos: identificar soluciones y analizar requerimientos antes de la adquisición o creación para asegurar que estén en línea con los requerimientos estratégicos de la Organización y que cubren los procesos de negocios, aplicaciones, información/datos, infraestructura y servicios. Coordinar con las partes interesadas afectadas la revisión de las opciones viables, incluyendo costes y beneficios relacionados, análisis de riesgo y aprobación de los requerimientos y soluciones propuestas.

Gestionar la Identificación y Construcción de Soluciones: establecer y mantener soluciones identificadas en línea con los requerimientos de la empresa que abarcan el diseño, desarrollo, compras/contratación y asociación con proveedores / fabricantes. Gestionar la configuración, preparación de pruebas, realización de pruebas, gestión de requerimientos y mantenimiento de procesos de negocio, aplicaciones, datos/información, infraestructura y servicios.

Gestionar la Disponibilidad y la Capacidad: equilibrar las necesidades actuales y futuras de disponibilidad, rendimiento y capacidad con una provisión de servicio efectiva en costes. Incluye la evaluación de las capacidades actuales, la previsión de necesidades futuras basadas en los requerimientos del negocio, el análisis del impacto en el negocio y la evaluación del riesgo para planificar e implementar acciones para alcanzar los requerimientos identificados.

Gestionar los Cambios: gestione todos los cambios de una forma controlada, incluyendo cambios estándar y de mantenimiento de emergencia en relación con los procesos de negocio, aplicaciones e infraestructura. Esto incluye normas y procedimientos de cambio, análisis de impacto, priorización y autorización, cambios de emergencia, seguimiento, reporte, cierre y documentación.

Gestionar la Aceptación del Cambio y la Transición: aceptar formalmente y hacer

operativas las nuevas soluciones, incluyendo la planificación de la implementación, la conversión de los datos y los sistemas, las pruebas de aceptación, la comunicación, la preparación del lanzamiento, el paso a producción de procesos de negocio o servicios TI nuevos o modificados, el soporte temprano en producción y una revisión post-implementación.

Gestionar los Activos: gestionar los activos de TI a través de su ciclo de vida para asegurar que su uso aporta valor a un coste óptimo, mantenidos en funcionamiento (acorde a los objetivos), que están justificados y protegidos físicamente y que los activos fundamentales para apoyar la capacidad del servicio son fiables y están disponibles. Administrar las licencias de software para asegurar que se adquiere el número óptimo, se mantienen y despliegan en relación con el uso necesario para el negocio y que el *software* instalado cumple con los acuerdos de licencia.

Gestionar la Configuración: definir y mantener las definiciones y relaciones entre los principales recursos y capacidades necesarias para la prestación de los servicios proporcionados por TI, incluyendo la recopilación de información de configuración, el establecimiento de líneas de referencia, la verificación y auditoría de la información de configuración y la actualización del repositorio de configuración.

Gestionar Operaciones: coordinar y ejecutar las actividades y los procedimientos operativos requeridos para entregar servicios de TI tanto internos como externalizados, incluso la ejecución de procedimientos operativos estándar predefinidos y las actividades de monitorización requeridas.

Gestionar Peticiones e Incidentes de Servicio: proveer una respuesta oportuna y efectiva a las peticiones de usuario y la resolución de todo tipo de incidentes. Recuperar el servicio normal, por otro lado, registrar y completar las peticiones de usuario, registrar, investigar, diagnosticar, escalar y resolver incidentes.

Gestionar Problemas: identificar y clasificar problemas y sus causas raíz y proporcionar resolución en tiempo para prevenir incidentes recurrentes. Proporcionar recomendaciones de mejora.

Gestionar la Continuidad: establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos

críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa.

Gestionar Servicios de Seguridad: proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad. Minimizar el impacto en el negocio de las vulnerabilidades e incidentes operativos de seguridad en la información.

Gestionar Controles de Proceso de Negocio: definir y mantener controles apropiados de proceso de negocio para asegurar que la información relacionada y procesada dentro de la Organización o de forma externa satisface todos los requerimientos relevantes para el control de la información. Identificar los requisitos de control de la información, gestionar y operar los controles adecuados para asegurar que la información y su procesamiento satisfacen estos requerimientos.

Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad: recolectar, validar y evaluar métricas y objetivos de negocio, de TI y de procesos. Supervisar que los procesos se están realizando acorde al rendimiento acordado y conforme a los objetivos y métricas y se proporcionan informes de forma sistemática y planificada.

Supervisar, Evaluar y Valorar el Sistema de Control Interno: supervisar y evaluar de forma continua el entorno de control, incluyendo tanto autoevaluaciones como revisiones externas independientes. Facilitar a la Dirección la identificación de deficiencias e ineficiencias en el control y el inicio de acciones de mejora. Planificar, organizar y mantener normas para la evaluación del Control Interno y las actividades de aseguramiento.

Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos: evaluar el cumplimiento de requisitos regulatorios y contractuales tanto en los procesos de TI como en los procesos de negocio dependientes de las tecnologías de la información. Obtener garantías de que se han identificado, se cumple con los requisitos y se ha integrado el cumplimiento de TI en el cumplimiento de la empresa general. Asegurar que la empresa cumple con todos los requisitos externos aplicables.

1.2.4.2. Normas técnicas para la gestión y el control de las Tecnologías de Información de la Contraloría General de la República (N-2-2007-CO-DFOE).

Las Normas técnicas para la gestión y el control de las Tecnologías de Información de la Contraloría General de la República, corresponden a la normativa en donde se establecen los criterios básicos de control a observar en la gestión de esas tecnologías cuyo propósito es coadyuvar en su gestión, en virtud de que dichas tecnologías se han convertido en un instrumento esencial en la prestación de los servicios públicos (Contraloría General de la República, 2007).

Estas normas técnicas brindan a las instituciones una serie de pasos a seguir para el eficiente cumplimiento de sus objetivos, pues las grandes empresas manejan una gran cantidad de información es necesario aumentar los controles y la forma de su aplicación, se hace referencia a los siguientes lineamientos establecidos por la Contraloría General de la República (2007):

1. Normas de aplicación general: se conforma por lo siguiente:

1.1 Marco estratégico de TI.

1.2 Gestión de la calidad.

1.3 Gestión de riesgos.

1.4 Gestión de la seguridad de la información.

1.5 Gestión de proyectos.

1.6 Decisiones sobre asuntos estratégicos de TI.

1.7 Cumplimiento de obligaciones relacionadas con la gestión de TI.

2. Planificación y Organización:

2.1 Planificación de las tecnologías de información.

2.2 Modelo de arquitectura de información.

2.3 Infraestructura tecnológica.

2.4 Independencia y recurso humano de la Función de TI.

2.5 Administración de recursos financieros

3. Implementación de tecnologías de Información.

3.1 Consideraciones generales de la implementación de TI.

3.2 Implementación de software.

3.3 Implementación de infraestructura tecnológica.

3.4 Contratación de terceros para la implementación y mantenimiento de software e infraestructura.

4. Prestación de servicios y mantenimiento.

4.1 Definición y administración de acuerdos de servicio.

4.2 Administración y operación de la plataforma tecnológica.

4.3 Administración de los datos.

4.4 Atención de requerimientos de los usuarios de TI.

4.5 Manejo de incidentes.

4.6 Administración de servicios prestados por terceros.

5. Seguimiento.

5.1 Seguimiento de los procesos de TI.

5.2 Seguimiento y evaluación del Control Interno en TI.

5.3 Participación de la Auditoría Interna.

La búsqueda de los objetivos empresariales mediante la planificación y Organización se deben encontrar en congruencia tanto con la capacidad presupuestaria como con las tecnologías de información y su cumplimiento del Control Interno. Según la Contraloría General de la República, (2007) se establece que la Organización debe optimizar la integración, uso y estandarización de sus sistemas de información de tal manera se identifique, capture y comunique, en forma completa, exacta y oportuna.

Según la Contraloría General de la República, (2007) dentro de la implementación de TI se establecen los siguientes pasos a seguir para el cumplimiento de los objetivos empresariales:

1. Adoptar políticas sobre la justificación, autorización y documentación de solicitudes de implementación o mantenimiento de TI.
2. Establecer el respaldo claro y explícito para los proyectos de TI tanto del jerarca como de las áreas usuarias.

3. Garantizar la participación activa de las unidades o áreas usuarias, las cuales deben tener una asignación clara de responsabilidades y aprobar formalmente las implementaciones realizadas.
4. Instaurar líderes de proyecto con una asignación clara, detallada y documentada de su autoridad y responsabilidad.
5. Analizar alternativas de solución de acuerdo con criterios técnicos, económicos, operativos y jurídicos, y lineamientos previamente establecidos.
6. Contar con una definición clara, completa y oportuna de los requerimientos, como parte de los cuales debe incorporar aspectos de control, seguridad y auditoría bajo un contexto de costo – beneficio.
7. Tomar las previsiones correspondientes para garantizar la disponibilidad de los recursos económicos, técnicos y humanos requeridos.
8. Formular y ejecutar estrategias de implementación que incluyan todas las medidas para minimizar el riesgo de que los proyectos no logren sus objetivos, no satisfagan los requerimientos o no cumplan con los términos de tiempo y costo preestablecidos.
9. Promover su independencia de proveedores de hardware, software, instalaciones y servicios.

Dentro de la prestación de servicios y mantenimiento La Contraloría General de la República, (2007) establece que la Organización se asegure de que los datos que sean procesados mediante TI corresponden a transacciones válidas y debidamente autorizadas, procesados en forma completa, exacta y oportuna, transmitidos, almacenados desechados en forma íntegra y segura.

La información contable es esencial para el cumplimiento de los objetivos empresariales y es manejada a través de TI, la misma debe ir de la mano con lo suministrado por los demás departamentos y debe ser real y congruente. Por lo anterior, se considera necesario que la administración cuente con un adecuado Control Interno para lograr identificar los posibles riesgos en los procesos y establecer procedimientos de mejora para minimizar dichos riesgos lo cual permite cumplir con el punto del seguimiento establecido en la norma.

Capítulo II. Junta Administradora del Fondo de Ahorro y Préstamos de la Universidad de Costa Rica.

En este capítulo se busca otorgar al lector una visión general de la Organización, detallando el perfil de la Empresa, la estructura interna, la descripción del departamento financiero y de tecnologías de información, la relación de la Unidad de Contabilidad con las tecnologías de información y la evolución de las Tecnologías de Información para la gestión de los procesos de la Organización y la generación de valor.

2.1. Descripción de la JAFAP

2.1.1. Perfil de la JAFAP

Para facilitar la comprensión del perfil de la JAFAP se presenta una reseña histórica de la Organización y aspectos generales de la misma como funciones, objetivos, misión, visión, valores y un detalle de los productos ofrecidos a los afiliados.

2.1.1.1 Reseña Histórica[10]

La Junta Administradora del Fondo de Ahorro y Préstamo de la Universidad de Costa Rica (JAFAP), fue creada con la promulgación de la Ley Orgánica de la Universidad de Costa Rica, el 26 de agosto de 1940 y por la necesidad de que sus funcionarios tuvieran acceso a un régimen de seguros al momento de jubilarse.

Esta Ley estableció que los funcionarios de la Universidad tendrán derecho a una jubilación voluntaria cuando alcanzarán los sesenta años y, forzosa, a los setenta años. Con ese propósito, se contrató un seguro para cada empleado con el Instituto Nacional de Seguros. Las primas, aportes y beneficios se basaron en las disposiciones de la Ley de Seguros de Vejez y Retiro de Empleados y Obreros de la Imprenta Nacional, por lo que la Universidad asumió las obligaciones que esa ley indicaba para el Estado.

En octubre de 1942, el Consejo Universitario aprobó el Reglamento de Seguros de Vejez y

[10] Recuperado el 24 de octubre del 2020 de: http://www.jafapucr.com/Inicio.aspx

Retiro del Personal Docente y Administrativo y creó la Junta Administradora del Fondo de Seguros Universitarios. Entre sus obligaciones estaba llevar una cuenta del patrimonio acumulado para cada asegurado, constituido por una contribución de la Universidad y otra deducida del salario de los funcionarios.

En sus inicios, contaba con ciento setenta y dos socios, los cuales al cabo de dos meses habían aportado un capital de ¢8.229,10 (Ocho mil doscientos veintinueve colones con diez céntimos). A partir del 15 de diciembre de 1952, el Consejo Universitario aprobó el reglamento de préstamos para aquellos asociados que tuvieran como mínimo un año de laborar activamente en la institución.

En noviembre de 1956, cambió su nombre por el de Junta Administradora del Fondo de Patrimonios Y Jubilaciones y se le otorgó personería jurídica, para su manejo independiente de la Universidad y poder contraer derechos y obligaciones en forma autónoma.

En marzo de 1964, la Junta tomó el nombre de Sistema de Patrimonios y Jubilaciones de la Universidad de Costa Rica. En ese momento, se debió incluir algunas nuevas disposiciones, pues el entorno jurídico y otras entidades competían con el accionar del sistema.

Al entrar en vigor la Ley de Pensiones y Jubilaciones del Magisterio Nacional, aprobada el 21 de agosto de 1964, obligaba a todos los empleados de la Universidad a cotizar para este régimen. En respuesta, los funcionarios universitarios cotizaron en ambos sistemas, y se elaboró un proyecto que modificó la Ley N°2076 que dio origen al Fondo y en diciembre de 1968, por medio de la Ley N° 4273, se creó la Junta Administradora del Fondo de Ahorro y Préstamo de la Universidad de Costa Rica.

De este modo, la Universidad estaba en capacidad de contribuir con un aporte igual al 2.5% del salario mensual de cada funcionario, aportando cada empleado un porcentaje idéntico.

Desde la aprobación de la Ley Orgánica de la Universidad de Costa Rica, fueron muchas las leyes y reglamentos, así como los planes y actividades que perfilaron la actual Junta Administradora de Ahorro y Préstamo.

La JAFAP es la Entidad encargada de recaudar y administrar los fondos recibidos de sus asociados, tanto docentes como administrativos, así como lo correspondiente al aporte de la Universidad de Costa Rica como patrono.

Los fondos recaudados por la JAFAP se invierten, en primer lugar, en calidad de préstamo a bajos intereses a sus asociados para diferentes planes de inversión; también en la compra de títulos valores del Estado con la intermediación de puestos de Bolsa autorizados y respaldados por la Bolsa Nacional de Valores.

La JAFAP desarrolla un amplio y eficiente programa para el bienestar de los servidores universitarios. Sus objetivos son claros, por lo tanto, su trayectoria y espíritu de servicio han sobresalido durante sus años de existencia. La Junta cuenta con un amplio panorama de actividades, todas con una sola meta: constituirse en un Ente de ayuda financiera para los funcionarios de la Universidad de Costa Rica.

La cartera crediticia se administra actualmente por medio del reglamento, siendo el mecanismo para la toma de decisiones.

La JAFAP fue creada por la Ley N° 4273 Ley Junta Administradora del Fondo de Ahorro y Préstamo de la Universidad de Costa Rica mediante decreto de la Asamblea Legislativa de la República Costarricense. Dentro de las funciones específicas otorgadas por esta Ley se encuentran las siguientes:

- Dirigir y administrar el fondo de ahorro y préstamo conforme con la reglamentación establecida por el Consejo Universitario.
- Constituir depósitos bancarios.
- Realizar inversiones con bonos del Estado y sus instituciones.
- Realizar operaciones de préstamo y descuentos a favor de los profesores y empleados administrativos de la Universidad, con la simple garantía de su fondo patrimonial acumulado, conforme a la reglamentación establecida por el Consejo Universitario; y hacer préstamos a la Universidad de Costa Rica hasta por una suma no mayor al veinticinco por ciento de su patrimonio total acumulado, por plazos no mayores a diez años, y a un tipo de interés no menor del ocho por ciento anual. Aceptar las donaciones, herencias o legados hechos a su favor.
- Realizar todas aquellas otras funciones y actividades para el buen cumplimiento de los fines estipulados, encomendados por el Consejo Universitario.

Los principales ordenamientos jurídicos de la JAFAP (2020) son:

- Ley N.° 4273 de la Junta Administradora del Fondo de Ahorro y Préstamo de la Universidad de Costa Rica.
- Reglamento de la Junta Administradora del Fondo de Ahorro y Préstamo de la Universidad de Costa Rica.
- Acuerdos del Consejo Universitario.
- Acuerdos de la Junta Directiva de la JAFAP UCR.
- Según el Artículo 4 de la Ley 4273, todo funcionario de la Universidad de Costa Rica debe ser afiliado de la JAFAP para contribuir al fondo creado por esta ley

2.1.1.2 Reseña Histórica[11]

La misión de la Institución es “Contribuir con el mejoramiento del bienestar integral y la calidad de vida de las personas afiliadas”.

La visión de la Entidades "Ser el principal aliado financiero de las personas afiliadas."

2.1.1.3 Objetivos

Adicional a los objetivos establecidos en la Ley de Creación de la Junta Administradora del Fondo de Ahorro y Préstamo, los objetivos de la Institución según la Reforma Integral de la JAFAP de la Universidad de Costa Rica (2020) son los siguientes:

- Estimular el ahorro entre las personas afiliadas para su mayor bienestar.
- Facilitar el otorgamiento de distintos tipos de préstamos a las personas afiliadas, especialmente destinados a solucionar problemas habitacionales.
- Promover y orientar sobre el buen uso de los ahorros y los préstamos a las personas afiliadas.

[11] Recuperado el 24 de octubre del 2020 de: http://www.jafapucr.com/Inicio/Con%C3%B3zcanos.aspx

- Procurar un equilibrio entre el fortalecimiento del Fondo y el beneficio integral de las personas afiliadas.
- Otorgar apoyo financiero para actividades las cuales beneficien la calidad de vida de las personas afiliadas.
- Llevar a cabo acciones de ayuda solidaria dirigidas a personas afiliadas con situaciones calificadas o especiales.

2.1.1.4 Valores

La JAFAP tiene como valores los siguientes:

Servicio: Satisfacer las necesidades y expectativas de las personas afiliadas y de todas aquellas relacionadas con la JAFAP UCR.

Innovación: Proponer de manera continua y sistemática, mejoras en todos los ámbitos de acción de la JAFAP UCR y mantener una actitud de apertura a los cambios que le permitan a la Institución mejorar su gestión.

Responsabilidad: Desempeñar las funciones con conocimiento de sus derechos y obligaciones, y, por ende, con plena consideración de las consecuencias de sus actos, decisiones y omisiones.

Compromiso: Cumplir con las obligaciones contraídas en la JAFAP UCR, mantener una buena disposición permanentemente y utilizar al máximo sus capacidades.

Honestidad: Desarrollar las funciones con respeto y en miras a la verdad y la justicia.

Solidaridad: Contribuir con sus labores a propiciar el bienestar común para las personas afiliadas y de todas aquellas relacionadas con la JAFAP UCR.

2.1.1.5 Productos[12]

La JAFAP cuenta con una amplia variedad de productos ofrecidos a sus afiliados, los mismos se dividen en ahorros y préstamos, los cuales se detallan a continuación:

Productos de Ahorro:

- Ahorro Flor de un día: corresponde a un ahorro voluntario en donde el asociado puede retirar su dinero en el momento requerido. Algunas de las ventajas ofrecidas por este tipo de ahorro son las siguientes:
    - Atractiva tasa de interés.
    - Cuota mínima de afiliación ¢500.
    - Deducción automática de cuota por planilla UCR.
    - Aportes extraordinarios por ventanilla (efectivo y cheque) o transferencia bancaria.
    - Depósito automático de salario UCR.
    - Acreditación de préstamos en forma automática en su cuenta de ahorros.
    - Los retiros se pueden efectuar en efectivo, cheques o transferencias electrónicas.
    - Nombrar autorizados de manera permanente o parcial para retiros.
    - Pago de servicios públicos mediante el sistema PAR (Pago Automático de Recibos).

- Ahorro Voluntario Vista: corresponde a un ahorro voluntario en donde el asociado puede retirar su dinero en el momento requerido, para este ahorro es necesario una cuota mensual fija que va a ser deducida de la planilla del afiliado (puede modificarse en el transcurso del tiempo). Algunas de las ventajas son las siguientes:
    - Forma de cálculo de los intereses: sobre el saldo diario, no son capitalizables y se pagan al momento del retiro.
    - Si conserva el ahorro por un año (365 días) se le pagará una tasa de 9,5 % anual.
    - Retiro total: Puede retirar su Ahorro Voluntario a la Vista en cualquier momento, para lo cual se aplicará la tasa de interés de los días de tenencia al momento del retiro.

[12] [12] Recuperado el 24 de octubre del 2020 de: http://www.jafapucr.com/Inicio.aspx

En caso de retiros parciales:

- Se desembolsará el monto solicitado más los intereses acumulados sobre el total del ahorro, aplicando la tasa de interés según los días de tenencia.
- La tasa de interés que aplicará para el saldo restante del Ahorro Voluntario a la Vista se ajustará a los nuevos días de tenencia de acuerdo con las tasas definidas en la tabla pactada.
- Al vencimiento del periodo de tenencia del Ahorro Voluntario a la Vista, el plan se renueva automáticamente con las condiciones vigentes en la fecha de renovación, excepto que la persona afiliada indique lo contrario.
- No se permiten depósitos extraordinarios.
- El monto máximo autorizado por persona afiliada a trasladar a este ahorro es de ¢150.000.000; provenientes del ahorro a la vista o de otros productos disponibles.

Productos de Préstamo

- Sobre Aportes: la JAFAP ofrece dos tipos de préstamos sobre los aportes de sus afiliados, los mismos son los siguientes:
    - Corriente: los afiliados tienen derecho a solicitar el cien por ciento de su aporte disponible en préstamos corrientes para dedicarlo a asuntos de carácter personal.
    - No Fiduciario: se otorgan siempre que haya aporte disponible, cada noventa días se ofrecerá un préstamo no fiduciario por el monto del aporte disponible, sin fiadores y por una suma no mayor al cincuenta por ciento (50%) del aporte total, que se amortiza por aparte, para el cual rigen los plazos y montos establecidos según Reglamento.

- Especiales: tienen la función de resolver necesidades urgentes comprobadas por los afiliados, se otorgan cuando el afiliado tiene agotadas las posibilidades del préstamo corriente. El tope aprobado y monto a otorgar serán definidos por la Junta, con base en la documentación aportada por el afiliado, de acuerdo con las posibilidades financieras del Fondo y otros criterios establecidos por la Junta.

- Vivienda: ofrece financiar planes de inversión como compra de lote o vivienda, construcción, cancelación de hipotecas, mejoras y ampliación. Las condiciones del crédito van a variar de acuerdo con la necesidad del asociado.
- Vehículo: ofrece préstamos para la compra de vehículos nuevos, usados o de tecnología limpia. Las tasas de interés dependen del tipo de vehículo que el afiliado va a adquirir.
- Pólizas Autoexpedibles: estos préstamos por concepto de pólizas por enfermedades graves incluye al afiliado y sus familiares. Las enfermedades atendidas por dichas pólizas son el cáncer, accidente cerebro vascular, insuficiencia renal e infarto al miocardio. Asimismo, cubre la indemnización por el primer diagnóstico de enfermedad grave, renta diaria por hospitalización y muerte.
- Póliza de Incendio, vehículos y vida: La JAFAP tiene convenios con el INS para que los asociados puedan acceder a estos servicios, las condiciones van a depender de los requerimientos del asociado y el porcentaje de cobertura.

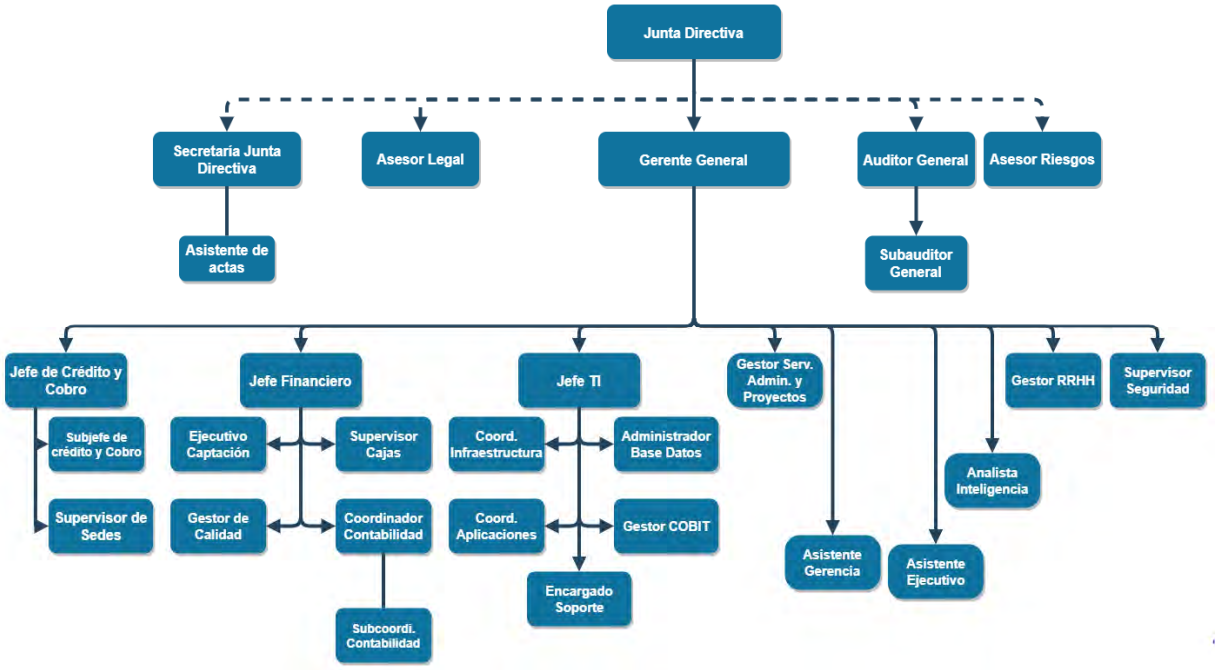
2.1.2. Descripción de la Estructura interna de JAFAP. (Manual de Organización y organigrama)

La JAFAP cuenta con una estructura orgánica aprobada por su Junta Directiva mediante el documento denominado Manual de Organización, el cual se refiere a la descripción ordenada jerárquicamente de las unidades administrativas con las que cuenta la Organización.

- Organigrama

Mediante el organigrama las organizaciones presentan una descripción gráfica y ordenada jerárquicamente de las unidades administrativas de la Organización. A continuación, se presenta el organigrama de la Junta de Ahorro

Figura 6 Organigrama JAFAP



Fuente: elaboración propia, con base en el organigrama de la Empresa.

Como parte del Manual de Organización de la JAFAP aprobado por su Junta Directiva el 19 de febrero 2020, se definen las dependencias jerárquicas de la Organización, así como el objetivo, las funciones principales, responsabilidad, relación de supervisión y relación de coordinación interna de cada una de estas.

La estructura orgánica de la JAFAP está compuesta por las siguientes dependencias:

1. **Junta Directiva**
    1. Auditoría Interna
    2. Asesoría Legal
    3. Asesoría de Riesgos
    4. Secretaría de Junta Directiva
    5. Comités

2. **Gerencia General**
    1. Departamento Financiero
        1. Unidad de Contabilidad
        2. Unidad de Tesorería
        3. Unidad de Presupuesto
    2. Departamento de Operaciones
        1. Plataforma de Servicio
        2. Información
        3. Call Center
    3. Departamento de Ahorro y Crédito
        1. Ahorro
        2. Crédito
    4. Departamento de Mercadeo
        1. Investigación de Mercadeo
        2. Comunicación
        3. Promoción de Bienestar y Calidad de Vida
    5. Departamento Administrativo
        1. Recursos Humanos
        2. Seguridad
        3. Archivo
        4. Compras, Bienes y Servicios
    6. Departamento de Tecnología de la Información
        1. Infraestructura
        2. Desarrollo
        3. Administración de Base de Datos
        4. Seguridad de la Información
        5. Gestión de Servicios

Como se determina en el detalle de la estructura orgánica de la JAFAP, es la Junta Directiva el órgano superior administrativo de la Organización, cuya composición es la siguiente:

La Junta Directiva estará integrada por cinco miembros; el rector o la rectora de la

> Universidad, en su calidad de presidente, y cuatro miembros más, que serán nombrados por el Consejo Universitario y podrán ser removidos por éste, por mayoría absoluta del total de los miembros. Dos de ellos serán representantes del sector docente, y los otros dos del sector administrativo de la Universidad. (Consejo Universitario, 2020, p.2)

La Reforma integral al Reglamento de la Junta Administradora del Fondo de Ahorro y Préstamo de la Universidad de Costa Rica en su artículo 8 establece las funciones de la Junta Directiva, dentro de las cuales podemos mencionar, la definición de políticas y estrategias de operación, tomar las medidas y acuerdos necesarios para la adecuada aplicación de las disposiciones de este reglamento y otra normativa que regula el funcionamiento de la JAFAP para garantizar la sana administración del Fondo.

Aunado a lo anterior, presentar al Consejo Universitario las propuestas de reformas reglamentarias, de estructura y de gestión de la JAFAP que considere pertinentes o se le soliciten, fiscalizar la administración de las finanzas del Fondo, mediante el análisis de los informes que la Gerencia presente o los solicitados a otras instancias competentes, elaborar el plan anual operativo y el proyecto de presupuesto de la JAFAP, evaluar la gestión gerencial anualmente, de conformidad con el plan operativo, las políticas y las metas definidas, y comunicarlo al Consejo Universitario.

Y finalmente, aprobar por solicitud de la Gerencia o la jefatura de la Auditoría Interna, la creación de nuevas plazas, sus perfiles y el salario base de contratación en la JAFAP, de acuerdo con el plan operativo aprobado por el Consejo Universitario, nombrar y remover a quien ocupe la jefatura del Departamento de Auditoría Interna y a quién ocupe el cargo de asesor legal, establecer los parámetros y criterios que se aplicarán para definir la política salarial del personal de la JAFAP y remitir un informe al Consejo Universitario, contratar una auditoría externa anualmente, entre otros.

Adicionalmente, la JAFAP cuenta con un Gerente General el cual es nombrado por la Junta Directiva por un período de cuatro años, renovable según una evaluación positiva de los resultados de la gestión. Según el Manual de Organización de la JAFAP la gerencia general tiene como objetivo "*Planificar, organizar, dirigir, coordinar y controlar todas las áreas funcionales de la JAFAP, de tal forma que se logren alcanzar los objetivos de acuerdo con las disposiciones de la Junta Directiva*". (p.29, 2020)

Por otra parte, de acuerdo con el artículo 16 de la Reforma integral al Reglamento de la JAFAP, las funciones de la Gerencia son, actuar como superior jerárquico del personal de la JAFAP, excepto del Departamento de Auditoría Interna y de la Asesoría Legal, aprobar el nombramiento y la remoción de las personas quienes ocupen jefaturas de área y comunicarlo a la Junta Directiva, contratar y remover al personal de la JAFAP, excepto el que sea nombrado por la Junta Directiva, presentar los informes solicitados por la Junta Directiva y el Consejo Universitario. Además, presentar un informe anual a la comunidad universitaria, brindar criterio a la Junta Directiva en aquellos aspectos solicitados, proponer a la Junta Directiva el plan de inversiones, previo estudio de riesgos, asistir a las reuniones de la Junta Directiva, con voz pero sin voto, y ejecutar sus acuerdos, implementar y mantener un estricto control financiero y un sistema de manejo de los riesgos institucionales, presentar anualmente a la Junta Directiva, dos meses después del cierre contable anual, un informe de labores, que incluirá los estados financieros y el grado de cumplimiento de los objetivos, de acuerdo con el plan de trabajo y presupuesto establecidos.

El superior jerárquico de la Gerencia General es la Junta Directiva, además, mantiene relación de coordinación interna con la Auditoría Interna, Asesoría Legal, Asesoría de Riesgos y Secretaría de Junta Directiva. A su vez, es el área encargada de la supervisión del Departamento Financiero, Departamento de Operaciones, Departamento de Ahorro y Crédito, Departamento de Mercadeo, Departamento Administrativo y Departamento de Tecnologías de Información.

2.1.3 Descripción del Departamento Financiero y de Tecnologías de Información.

La JAFAP cuenta dentro de su estructura orgánica con un Departamento Financiero y un Departamento de Tecnologías de Información, los cuales tienen dependencia jerárquica de la Gerencia General. Ambos departamentos mantienen relación de coordinación con el resto de los departamentos de la Organización.

A continuación, se describe la composición y funciones de estos departamentos.

2.1.3.1 Departamento Financiero

El Departamento Financiero de la JAFAP está compuesto por las unidades de Contabilidad,

Tesorería y Presupuesto, con un total de 12 colaboradores. Dicho departamento responde a la Gerencia General y cuenta con un jefe financiero a cargo de las unidades. Además, mantiene relación de coordinación interna con el Departamento de Operaciones, Departamento de Ahorro y Crédito, Departamento de Mercadeo, Departamento Administrativo y Departamento de Tecnologías de Información.

El objetivo del departamento es *"Planificar, coordinar y administrar los recursos, registros y operaciones financieras de la JAFAP, con el fin de garantizar la continuidad y sustentabilidad financiera." (*p. 35, 2020*).*

Las principales funciones del departamento son, definir la estrategia y el proceso de planeación financiera de la Organización, administrar el ahorro obligatorio de las personas afiliadas y el aporte obrero de la Universidad de Costa Rica, administrar la liquidez de la JAFAP mediante el control del flujo de efectivo, establecer propuestas de inversión de los recursos financieros y controlar las inversiones en títulos valores, dirigir la formulación y control del presupuesto ordinario y extraordinario con base en las disposiciones establecidas, dirigir, supervisar el proceso de registro y cierre contable, con el propósito de reflejar, en forma confiable y oportuna, la gestión financiera en apego a las normativas, dirigir el adecuado cumplimiento de las obligaciones en materia fiscal, dirigir la estrategia para la mitigación de riesgos financieros, analizar información financiera y brindar informes a la gerencia para la toma de decisiones, elaborar, ejecutar y controlar las actividades del PAO y presupuesto del departamento, así como determinar, actualizar políticas y normativas competentes al departamento.

2.1.3.1.1 Unidad de Contabilidad

Esta unidad tiene como objetivo *"Generar y proporcionar información contable razonable, de acuerdo con las Normas Internacionales de Contabilidad (NIC) y las Normas Internacionales de Información Financiera (NIIF), con la finalidad de mostrar la situación real de la JAFAP para la toma de decisiones.".*

Las principales funciones del departamento son, revisar las partidas contables del balance y sus auxiliares, con el fin de identificar inconsistencias en los registros automáticos o manuales y

proceder con la corrección de los mismos de una manera ágil y eficiente, consolidar la información contable en estados financieros que aporten información necesaria y oportuna para la toma de decisiones, atender los requerimientos y oportunidades de mejora señalados en los informes y cartas de gerencia elaborados por la auditoría interna y externa, para que los mismos en sus opiniones expresen la razonabilidad en los estados financieros de acuerdo con las Normas Internacionales de Contabilidad (NIC) y las Normas Internacionales de Información Financiera (NIIF).

Sus funciones son controlar el flujo de efectivo mediante previsiones de ingresos y desembolsos, ejecutar el desembolso de recursos por pago a proveedores, gestiones bancarias y operativas, a través de los diferentes medios: transferencias, cheques y efectivo, desarrollar informes de los saldos disponibles para la toma de decisiones de inversión, dirigir y controlar el servicio de autogestión, garantizando su cumplimiento para satisfacción de las necesidades de los afiliados, de acuerdo con los productos financieros de la JAFAP, coordinar y tramitar el aprovisionamiento a las caja y establecer contacto permanente con los ejecutivos de cuenta de los diferentes bancos.

2.1.3.1.2 Unidad de Tesorería

El objetivo de esta unidad es "D*irigir y controlar en forma eficiente las actividades de custodia, control, manejo, entrada y salida de valores de la JAFAP, con la finalidad de atender las necesidades de la Organización, su operativa y maximizar los rendimientos".*

Sus funciones son, controlar el flujo de efectivo mediante previsiones de ingresos, desembolsos, ejecutar el desembolso de recursos por pago a proveedores, gestiones bancarias y operativas, a través de los diferentes medios: transferencias, cheques y efectivo, desarrollar informes de los saldos disponibles para la toma de decisiones de inversión, dirigir y controlar el servicio de autogestión, por otro lado garantiza su cumplimiento para satisfacción de las necesidades de los afiliados, de acuerdo con los productos financieros de la JAFAP, coordinar y tramitar el aprovisionamiento a las caja y establecer contacto permanente con los ejecutivos de cuenta de los diferentes bancos.

2.1.3.1.3 Unidad de Presupuesto

El propósito de la Unidad de presupuesto es "*Programar, controlar y evaluar la gestión presupuestaria de la JAFAP, manteniendo la razonabilidad en el uso de los recursos humanos, físicos y financieros de la Organización".*

La Unidad de presupuesto es responsable de definir las políticas y normas presupuestarias de corto y mediano plazo que optimicen los recursos humanos, físicos y financieros, dictar lineamientos y procedimientos a los departamentos ejecutores para la elaboración de los presupuestos anuales, elaborar el presupuesto anual de acuerdo con el Plan Anual Operativo y controlar las partidas presupuestarias, elaborar informes sobre el avance de la ejecución del presupuesto en general, recomendando las medidas necesarias para el cumplimiento oportuno de las metas establecidas y presentar información presupuestaria consistente, clara y oportuna sobre los distintos planes, programas y proyectos que la JAFAP desarrolla anualmente.

2.1.3.2 Departamento de Tecnologías de Información

El Departamento de Tecnologías de Información de la JAFAP está compuesto por 12 colaboradores y cuenta con las áreas de Infraestructura, Desarrollo, Administración de Base de Datos, Seguridad de la Información y Gestión de Servicios. Este departamento tiene dependencia jerárquica de la Gerencia General y mantiene una relación de coordinación con el Departamento Financiero, Departamento de Operaciones, Departamento de Ahorro y Crédito, Departamento de Mercadeo y Departamento Administrativo.

De acuerdo con el Manual de la Organización el objetivo del departamento es "*Planificar, organizar y controlar los recursos tecnológicos que permitan la mejora e innovación de los procesos y servicios que brinda la JAFAP.*"

De acuerdo con el Manual de Organización, las funciones más relevantes del Departamento de TI son, definir la estrategia de desarrollo de sistemas de información y demás servicios informáticos, de acuerdo con sus objetivos y planes estratégicos, proveer herramientas de cómputo,

sistemas y telecomunicaciones según los requerimientos de los distintos departamentos, diseñar planes de contingencia, seguridad y control de la operación, con el fin de garantizar la disponibilidad de la información, supervisar, mantener la operatividad y disponibilidad de los sistemas de información, servicios basados en tecnologías de información y comunicaciones así como coordinar la mesa de servicios para centralizar y controlar las solicitudes de requerimientos tecnológicos, formular los términos de referencia para la adquisición de los equipos, así como la como la contratación de servicios externos.

2.1.3.2.1 Área de Infraestructura

Esta área tiene como objetivo "*Coordinar, ejecutar y supervisar la administración de la infraestructura informática, que permita mantener la seguridad y alta disponibilidad de los servicios de TI y garantizar la continuidad del negocio.*"

Las principales funciones del área son proponer e implementar metodologías, técnicas, estándares, procedimientos, tecnologías y buenas prácticas, orientadas a mejorar los servicios de TI, supervisar la instalación, configuración y administración de servidores de red, aplicaciones y sistemas operativos con el fin de garantizar alta disponibilidad de los servicios de TI, supervisar y monitorear los respaldos de la información con el propósito de garantizar la recuperación de esta cuando se necesite, supervisar, dar seguimiento a los incidentes y requerimientos de TI con el fin de brindar soluciones oportunas, monitorear y ajustar la plataforma tecnológica, así como hacer recomendaciones pertinentes encaminadas al óptimo desempeño de los recursos y crear indicadores, métricas de desempeño y funcionamiento de los componentes de la plataforma tecnológica.

2.1.3.2.2 Área de Desarrollo

El objetivo del área es *"Planear, coordinar, supervisar y controlar las tareas involucradas en el desarrollo y mantenimiento de los proyectos y sistemas de la Organización."*

Como parte de las funciones del Área de Desarrollo se encuentran participar en el

establecimiento de estrategias y criterios metodológicos para el diseño y desarrollo de sistemas, validar los prototipos, formatos y sistemas funcionales como las soluciones viables a las necesidades informáticas de la Organización, coordinar, desarrollar los proyectos y sistemas en proceso que consideren las necesidades de información de los departamentos, actualizar los sistemas y proyectos en producción, participar en la definición de infraestructura e insumos informáticos necesarios para satisfacer las necesidades de Sistemas (Plataforma, equipo, comunicaciones, teleproceso, herramientas de desarrollo, etc.), generar la documentación técnica y manuales de cada sistema, entre otras.

2.1.3.2.3 Área de Administración de Base de Datos

El propósito del área es *"Administrar, mantener y brindar de manera segura la administración de todas las bases de datos de la Organización, así como la mejora y diseño de nuevos modelos de estas"*.

Las principales funciones de esta área son la administración de la estructura de la base de datos, la actividad de los datos y el sistema manejador de base de datos, establecer el Diccionario de Datos, asegurar la confiabilidad y confirmar la seguridad de la base de datos, establecer un rol de respaldos para garantizar la recuperación de la información, definir y proponer modelos de extracción y presentación de los datos, apoyar las iniciativas de las áreas de negocio en la implementación de reportería y utilización de herramientas de inteligencia de negocio, definir y establecer indicadores y métricas de desempeño para monitorear la base de datos.

2.1.3.2.4 Área de Seguridad de la Información

El objetivo del área es *"Definir y establecer las medidas y controles que aseguran la confidencialidad, integridad y disponibilidad de los activos de los sistemas de información, incluyendo hardware, software, firmware y aquella información que se procesa, almacena y se comunica"*.

Dentro de sus funciones del área se encuentran: Mantener las reglas de acceso a los datos y otros recursos de TI, mantener la seguridad y la confidencialidad sobre la emisión y mantenimiento

de la identificación de usuarios, contraseñas, preparar y monitorear el programa de concientización en seguridad., probar la arquitectura de seguridad para evaluar la fortaleza de la seguridad y para detectar las posibles amenazas, mantener actualizadas las políticas, estándares, procedimientos y toda la documentación necesaria para el cumplimiento de la política de seguridad de la información e implementar un proceso de administración de incidentes de seguridad que permita prevenir y limitar el impacto de estos.

2.1.3.2.5 Área de Gestión de Servicios

El objetivo de Gestión de Servicios es *"Alinear y soportar los procesos de negocio con la infraestructura de tecnologías de información, con el fin de brindar una adecuada gestión de la calidad de los servicios que se brindan."*

En sus funciones destacan, aumentar la eficiencia en la prestación de los servicios brindados, reducir los riesgos asociados a los servicios de TI, apoyar de manera operativa los procesos de negocio, proporcionar un marco de gobernanza de tecnologías de información, estimar la capacidad y recursos necesarios para la prestación del servicio, establecer los niveles de calidad del servicio así como los mecanismos de mejora, evolución de este, además definir y establecer indicadores y métricas de desempeño para monitorear la Base de Datos.

2.2. Relación del departamento contable con las tecnologías de información.

La información contable es imprescindible para las empresas, pues sin ella sería imposible conocer la situación y evolución de los negocios, así mismo, les permite tomar decisiones adecuadas con base a una información consistente, objetiva y relevante.

Actualmente para el adecuado funcionamiento de los procesos contables es necesario la utilización de sistemas de información, las organizaciones se desempeñan en entornos económicos altamente competitivos, que las obliga a mejorar sus procesos internos en búsqueda de una mejora continua que permita maximizar su rentabilidad.

Para la JAFAP es fundamental la utilización de TI en sus procesos contables debido a la gran cantidad de información procesada diariamente, esto les exige disponer de sistemas de información automatizados, cada vez más específicos y complejos que agrupen y sinteticen esta información y generar productos. La JAFAP utiliza el sistema contable llamado Sibú, el mismo fue desarrollado por un proveedor desde cero, de acuerdo con las necesidades de la Organización, este sistema se encuentra dividido por módulos que fueron creados específicamente para cada área.

El sistema Sibú cuenta con tres módulos más importante, los mismos son de crédito, ahorros y contabilidad. Se detallan a continuación:

- Crédito: este módulo se utiliza para la creación de nuevas líneas de crédito, mantenimiento de los préstamos que los afiliados tengan activos o la anulación de los estos.
- Ahorros: este módulo se utiliza para la creación de nuevos planes de ahorros del asociado, permite la modificación de las cuotas y de los tipos de movimiento propios de los diferentes planes de ahorro.
- Contabilidad: este módulo se utiliza para el control y registros de los gastos e ingresos, además permite la elaboración de nuevas cuentas contables y edición de asientos.

Para cada uno de los módulos encontrados en el sistema Sibú, la JAFAP cuenta con manuales de uso para sus colaboradores, los mismos fueron desarrollados por el proveedor del sistema.

Las funcionalidades del sistema Sibú son las siguientes:

- Elaboración de recibos
- Registros contables (asientos de diario)
- Reportería
- Conciliaciones de cuentas
- Estados Financieros

Como parte de las funciones, cada departamento realiza los registros contables en cada uno de los módulos del sistema Sibú, por ejemplo: pago de créditos, captación de ahorros, pagos de servicios públicos, entre otros, automáticamente la información está a disposición del departamento de contabilidad para la generación de reportes, estados financieros, toma de decisiones y demás.

Mediante el sistema Sibú se generan dos tipos de asientos contables, manuales (depreciación y amortización de activos, ajustes y reclasificaciones) y automáticos, por lo cual se requiere que el departamento de TI realice un adecuado mantenimiento y control para evitar que se generen errores los cuales alteran los datos.

El sistema contable tiene la capacidad de identificar movimientos erróneos ingresados por los encargados de cada departamento, en caso de que ocurran dichas situaciones el sistema genera una alerta de error la cual permite la corrección y detección a tiempo. Es importante recalcar, no todo el personal cuenta con acceso total a la información contable.

Aunado al sistema Sibú, el departamento contable utiliza el paquete de Office (especialmente la herramienta Excel) para realizar bases de datos, tablas dinámicas, aplicación de fórmulas y demás que complementan la información contable generada por el sistema.

El departamento contable está directamente relacionado con áreas de cobros, ahorro y crédito, sin embargo, debemos recalcar que la relación con TI es fundamental, pues mediante el sistema se consolida toda la información requerida para cumplir con los objetivos institucionales.

2.3. Evolución de las Tecnologías de Información para la gestión de los procesos de la Organización y la generación de valor.

Existe una relación directa entre la evolución de la tecnología y el cambio en las organizaciones, producto del surgimiento de nuevas tecnologías de información y comunicación con el objetivo de afrontar nuevas realidades del entorno empresarial, esto produjo posteriormente cambios en el diseño estructural, cultural y en el clima organizacional.

Así mismo, los sistemas de información aportan relevancia para las empresas no sólo en la toma de decisiones, sino también en sus capacidades, sus colaboradores y alta gerencia en cuanto a los valores organizacionales, habilidades y experiencia.

A través del tiempo, las TI han tenido una evolución considerable para lograr la gestión de todos los procesos en las organizaciones. Según Córdoba et al. (2019):

"los dirigentes logran implantar estrategias adecuadas y ordenar sus objetivos con el de

> la Organización, gracias a las posibilidades que ofrecen las tecnologías de información, tales como los métodos para procesamiento de datos de la información y Big Data para toma de decisiones. La computación en la nube y el aprendizaje en línea para mejorar el uso de recursos".

Desde tal perspectiva, (Mujica, 2000, como se citó en De Vita, 2008), considera que "el avance tecnológico de la informática, la computación, y las telecomunicaciones, incorporaron en las organizaciones un enfoque diferente al habitual para acceder al conocimiento, flexibilidad, interactividad, economía, rapidez, independencia, comunicación y desarrollo".

Algunos de los beneficios aportados por las TI a las organizaciones son:

- Acceso a la información rápida, completa, confiable y comprensible.
- Procesos rápidos y simplificados, esto genera un ahorro de tiempo considerable.
- Obtención de la información ordenada y en tiempo real.
- Comunicación asertiva entre los diferentes departamentos.
- Alto grado de almacenamiento.
- Procesos automáticos.
- Mejor aprovechamiento del espacio físico.

Según (Cano y García, 2018) se describe lo siguiente:

> "Las TI son capaces de proporcionar sistemas de control y de planificación más integral, que favorecen un análisis global de los datos por parte de una persona en particular o la mayoría de actores que conforman la Organización, en definitiva, se trata de proveer la herramienta necesaria para promover la toma de decisiones a cualquier área de la Organización. Son esenciales para mejorar la productividad de las empresas, la calidad, el control y facilitar la comunicación, entre otros beneficios, aunque su aplicación debe llevarse a cabo de forma inteligente. El hecho de introducir tecnología en los procesos empresariales no es garantía de gozar de estas ventajas. Para que la

> implantación de nueva tecnología produzca efectos positivos, se debe cumplir varios requisitos: tener un conocimiento profundo de los procesos de la Empresa, planificar detalladamente las necesidades de tecnología de la información e incorporar los sistemas tecnológicos paulatinamente, empezando por los más básicos".

Sumado a los beneficios, es importante hacer énfasis en la generación de valor que representan las TI dentro de las entidades. Algunos ejemplos son los siguientes:

- Capacidad de análisis de gran cantidad de información.
- Toma de decisiones asertivas.
- Posicionamiento de la empresa con respecto al mercado local e internacional.
- Establecimiento de planes de acción para mejoras internas.

En el caso específico de la JAFAP, las TI tienen gran importancia para la gestión de los procesos, pues detectan y corrigen errores al momento de generar información relevante. Algunos de los beneficios y generación de valor de las TI dentro de la JAFAP son:

- Generar información conciliada.
- Adaptaciones y actualizaciones según requerimientos de la contabilidad.
- Mejora continua en los procesos contables mediados por las tecnologías de información.
- Evita el trabajo manual y errores humanos.
- Facilidad de crear productos, por ejemplo: integrar nuevos tipos de créditos.
- Cálculos automáticos: intereses, análisis para otorgar nuevos créditos, liquidaciones de ahorros, entre otros.
- Eficiencia y eficacia en los procesos.

Debido a la gran competitividad existente en la actualidad, las organizaciones requieren la optimización y la generación de recursos para la generación de valor. Las TI forman parte de las herramientas para la mejora continua y la utilización de la información de manera oportuna.

Las TI han cambiado la manera de trabajar y la forma de generar resultados en las

organizaciones, son clave para que el trabajo sea más productivo mediante mayor fluidez en las comunicaciones, aumento del trabajo en equipo y realizando análisis financieros. La tecnología siempre está presente en las diferentes etapas de desarrollo de las empresas, por lo cual existe una relación muy estrecha entre evolución, tecnología y sistemas contables.

Capítulo III. Análisis y comparación de la situación actual de la gestión de los procesos contables vinculados con tecnologías de información.

En este capítulo se realiza un análisis comparativo de la gestión de los procesos contables mediados por tecnologías de información que actualmente tiene la JAFAP para el logro de sus objetivos, con base en un estudio de COBIT 5 y la normativa vigente aplicada por la Contraloría General de la República con el fin de identificar oportunidades de mejora.

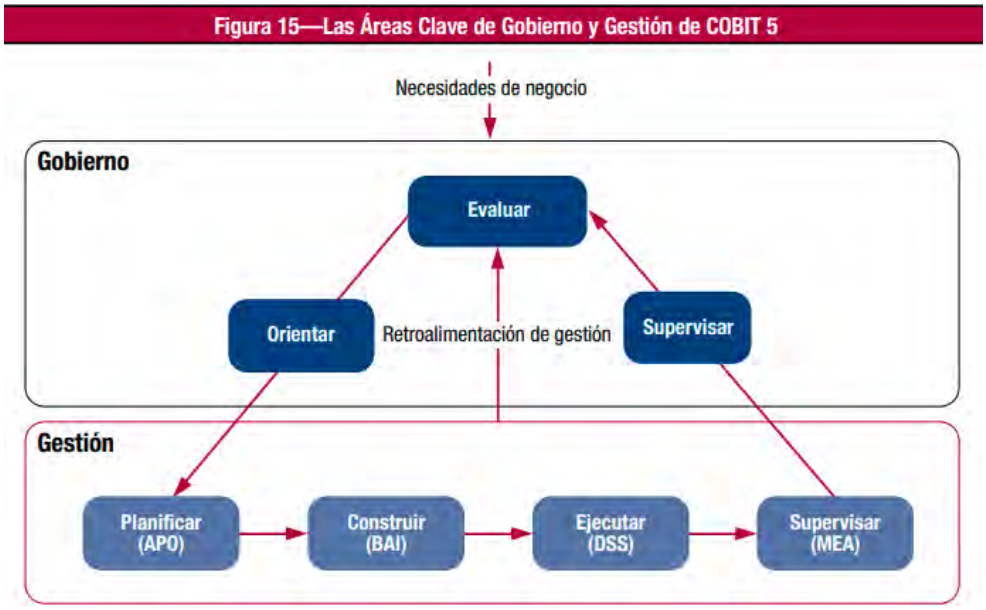
3.1 Identificación y evaluación de las políticas, normas y procedimientos vigentes para los procesos contables.

3.1.1 Análisis de las políticas, normas y procedimientos utilizados por la JAFAP.

La JAFAP al ser una Organización autónoma, no se encuentra sujeta a regulación, ni a la aplicación obligatoria de políticas, normas y procedimientos, sin embargo, para realizar de forma segura sus funciones y cumplir con las buenas prácticas utilizan la ISO 27001 y algunos procesos de COBIT 5 e ITIL. Según la información brindada por la JAFAP y el Departamento de TI, a continuación, se desarrollarán los puntos específicos utilizados por la Entidad.

De los dominios de COBIT 5, la JAFAP utiliza el dominio Entregar, Dar Servicio y Soporte (*Deliver, Service and Support*, DSS) relacionado con la entrega de los servicios requeridos, prestación del servicio, administración de la seguridad y continuidad, soporte a usuarios del servicio, administración de datos e instalaciones operativas. Su objetivo es identificar las prioridades de negocio y con esto entregar los servicios de TI, mejorar los costos, utilización de los sistemas de forma productiva y segura, confidencialidad, integridad y disponibilidad.

Ilustración 1 Área clave de Gobierno y Gestión de COBIT 5



Fuente: COBIT 5, Un Marco de Negocio para el Gobierno y la Gestión de TI de la Empresa

Cada uno de los dominios de COBIT 5 se encuentran integrados por una serie de procesos, como se detallan a continuación:

Ilustración 2 Modelo de Referencia de Procesos de Cobit 5

Fuente: COBIT 5, Un Marco de Negocio para el Gobierno y la Gestión de TI de la Empresa

Del dominio Entregar, Dar Servicio y Soporte (*Deliver, Service and Support*, DSS), la JAFAP utiliza únicamente los siguientes procesos:

Gestor de Servicios: para cumplir con este aspecto, la JAFAP utiliza los siguientes procesos:

Dominio DSS - Proceso DSS01 - COBIT 5: Gestionar Operaciones

Coordinar y ejecutar las actividades y los procedimientos operativos requeridos para entregar servicios de TI tanto internos como externalizados, incluso la ejecución de procedimientos operativos estándar predefinidos y las actividades de monitorización requeridas. El propósito del proceso es entregar los resultados del servicio operativo de TI, según lo planificado (ISACA, 2012).

Dominio DSS - Proceso DSS02 - COBIT 5: Gestionar Peticiones e Incidentes de Servicio

Proveer una respuesta oportuna y efectiva a las peticiones de usuario y la resolución de todo tipo de incidentes. Recuperar el servicio normal, registrar, completar las peticiones de usuario, registrar, investigar, diagnosticar, escalar y resolver incidentes. El propósito del proceso es lograr una mayor productividad y minimizar las interrupciones mediante la rápida resolución de consultas de usuario e incidentes (ISACA, 2012).

Continuidad: para cumplir con este aspecto, la JAFAP utiliza los siguientes procesos:

Dominio DSS - Proceso DSS04 - COBIT 5: Gestionar la Continuidad

Establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa. El propósito del proceso es continuar las operaciones críticas para el negocio y mantener la disponibilidad de la información a un nivel aceptable para la empresa ante el evento de una interrupción significativa (ISACA, 2012).

Riesgos y seguridad: para cumplir con este aspecto, la JAFAP utiliza los siguientes procesos:

Dominio DSS - Proceso DSS05 - COBIT 5: Gestionar Servicios de Seguridad

Proteger la información de la empresa para mantener aceptable el nivel de riesgos de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener las funciones de seguridad y privilegios de acceso de la información, también realizar la supervisión de la seguridad. El propósito del proceso consiste en la minimización del impacto en el negocio de las vulnerabilidades e incidentes operativos de seguridad en la información (ISACA, 2012).

Seguridad de la información

En lo referente a seguridad de la información, la JAFAP utiliza como marco de referencia y modelo de buenas prácticas la norma ISO 27001 *Tecnología de la información —Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos.* A través de esta norma, se busca preservar la confidencialidad, integridad y disponibilidad de la información a través de la gestión de riesgos.

Esta norma tiene como objetivos establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información en el contexto de la Organización, a través de la evaluación de los riesgos que afectan la información y posterior a esto, establece medidas para evitar que estos riesgos se materialicen en la Organización.

El sistema de gestión de seguridad de la información de la norma ISO 27001 se resume en la siguiente figura:

Ilustración 3 Sistema de Gestión de Seguridad ISO 27001

Fuente: ISO 27001, Sistema de Gestión de Seguridad

ITIL

La JAFAP como parte del uso de buenas prácticas en sus operaciones de tecnologías de información ha implementado el uso del proceso Operaciones del Servicio de ITIL (*Information Technology Infraestructure Librar*y), que corresponde a un conjunto de publicaciones de buenas prácticas para la gestión de servicios de TI.

La operación del servicio según ITIL consiste en asegurar que los servicios de TI se ofrezcan efectiva y eficientemente. Esto incluye cumplir con los requerimientos de los usuarios, resolver fallos en el servicio, solución de inconvenientes y llevar a cabo operaciones rutinarias.

Este proceso ha sido implementado en la JAFAP a través de la herramienta *Aranda Service Desk,* a través del cual se realiza la gestión de eventos, gestión de incidencias, gestión de peticiones del servicio, gestión de problemas, gestión de accesos, centro de servicio al usuario, monitorización de control y operación de TI.

La utilización de estos procesos permite la gestión y el control de las solicitudes de soporte, así como la Organización y el control, el monitoreo continuo de los casos y los activos asociados, una consola *web* para seguimiento de los casos, disminución del tiempo de respuesta a usuarios, entre otros.

3.1.2. Evaluación de los procesos existentes en la JAFAP a nivel contable y de tecnologías de información.

Actualmente la Entidad cuenta con un Plan Anual Operativo y un Presupuesto, aunado a una serie de manuales de políticas, procedimientos para todas sus áreas, que describen a detalle el objetivo, alcance y procesos a cumplir por parte de la Organización para obtener un alto grado de control, de esta manera prevenir, detectar, corregir eventuales errores y mitigar los riesgos operativos y financieros a los que está expuesta.

Para la evaluación de los procesos de la JAFAP se realizaron tres cuestionarios aplicados al personal de los departamentos de Crédito y Cobro, Contabilidad y Tecnologías de Información.

A continuación, se detallan los resultados de los cuestionarios aplicados en cada departamento, los mismos fueron consolidados según los procesos de COBIT 5 y las Normas de Aplicación General" (N-2-2007-CO-DFOE) de la Contraloría General de la República.

Para más detalle de los cuestionarios véase Anexos 1, 2 y 3.

Contabilidad

Gestionar el Riesgo

De acuerdo con los resultados se determinó la falta de uniformidad en la información brindada en lo relacionado a la existencia de herramientas con las cuales cuenta el departamento para realizar las evaluaciones del riesgo correspondientes.

Gestionar las operaciones

Según la información suministrada, los Estados Financieros de la JAFAP son generados por el sistema SIBU y se afirma que dicho sistema contribuye con el logro de los objetivos del departamento.

Gestionar los recursos humanos

Los resultados indican que el personal del departamento recibe inducción del sistema SIBU, así como de los procedimientos del área contable, los cuales son claros y precisos.

Así mismo, hay concordancia en las respuestas obtenidas sobre el proceso de revisión y aprobación de los Estados Financieros por el órgano competente.

Gestionar controles de proceso del negocio

Se indicó que el departamento mantiene acceso restringido. Dichos accesos son otorgados por el Departamento de TI (seguridad lógica en los sistemas) y físicamente el área se encuentra resguardada con llaves de acceso únicamente para el personal contable.

El departamento cuenta con segregación de funciones para la realización, revisión, y aprobación de procesos contables mensuales tales como confección de registros, conciliación de cuentas bancarias y de Estados Financieros. Los encargados del proceso son el asistente contable, subcoordinador y coordinador del área de Contabilidad.

Gestionar la continuidad

Los resultados reflejan que toda la información generada por el departamento se encuentra

debidamente respaldada.

Se determinó que no existe uniformidad en la información brindada por los colaboradores en lo relacionado a la existencia de planes de continuidad de negocio, plan de contingencia en caso de alguna falla del sistema SIBU y en la utilización de información en formato físico como soporte de los procesos contables del departamento.

Gestionar las Peticiones y los Incidentes del Servicio

Se identificó que no existe relación en la información brindada, en cuanto a actualizaciones e incorporación de nuevas funciones en el sistema SIBU, las cuales deben ser solicitadas por el personal según sus necesidades.

Gestionar la identificación y construcción de soluciones

Se identificó que no existe relación en la información brindada en cuanto a las capacitaciones otorgadas al personal sobre las actualizaciones del sistema SIBU, las cuales permitan obtener soluciones puntuales y rentables capaces de soportar la estrategia del negocio y los objetivos operacionales.

Gestionar los servicios de seguridad

Mediante los resultados se afirma que el departamento cuenta con políticas de seguridad de la información, ejemplo de ello es lo siguiente:

- Para la utilización del sistema SIBU se requiere que los colaboradores cuenten con un usuario y contraseña para acceder al módulo de contabilidad en el sistema SIBU, lo cual le permite ingresar al sistema y a las funciones definidas según el papel del colaborador.

Gestionar la seguridad

Se determinó la existencia de contratos de confidencialidad con los colaboradores del departamento.

Gestionar la calidad

Se determinó que la información generada por el sistema SIBU es sometida a un proceso de revisión y validación por parte del personal a cargo, con el fin de entregar productos y servicios satisfactorios para los requerimientos de los usuarios.

Supervisar, evaluar y valorar el sistema de Control Interno

Los procesos de contabilidad son auditados por la auditoría interna y externa de la JAFAP. La auditoría externa realiza tres visitas durante el año para la revisión de los Estados Financieros anuales y la auditoría interna realiza las revisiones de forma constante, cada vez que el departamento lo considere necesario.

Crédito y Cobro

Gestionar controles de proceso del negocio

La información crediticia de los afiliados sólo puede ser utilizada por el Departamento de Crédito y Cobro y cualquier otro departamento (tesorería, inteligencia de negocios, auditoría, entre otros) que lo requiera con la debida autorización del nivel jerárquico adecuado y con los accesos correspondientes otorgados únicamente por el departamento de TI.

Se afirmó la existencia de una correcta segregación de funciones para la realización, revisión y aprobación de los créditos y los cargos involucrados en dichos procesos son Supervisor, Jefatura y Subjefatura.

Se indicó que los encargados de verificar la adecuada aplicación de ahorros y aportes a los préstamos activos es el Departamento de Crédito y Cobro. Así mismo, este Departamento es el encargado de verificar que el reporte de morosidad suministrado por sistema SIBU sea el correcto.

Gestionar la calidad

Los resultados indican que para las solicitudes de créditos se corroboran los datos del sistema de constancias salariales de la Universidad de Costa Rica y su concordancia con los datos proporcionados por el sistema SIBU, así mismo, se verifica el correcto ingreso de las solicitudes en el sistema (*Check List*).

El personal a cargo verifica el adecuado registro de las gestiones de cobro en el sistema SIBU.

Para los créditos sobre aportes se revisa el tipo (créditos corrientes o no fiduciario) y que el monto máximo del crédito suministrados por el sistema SIBU sea correcto. Así mismo, se debe revisar la información relacionada al *Cashback*, con el objetivo de verificar la integridad de la información.

Antes de realizar la entrega de las liquidaciones de la Asociación se verifica la cancelación previa de los préstamos activos.

Los datos suministrados reflejan la carencia de uniformidad en cuanto a la revisión de la planilla mensual para verificar en el sistema SIBU el estatus de los afiliados (activos e inactivos), además se determinó con los resultados que no hay concordancia con la aplicación del procedimiento de verificar la aplicación previa de los depósitos realizados por los afiliados para el pago de las cuotas de créditos.

También se comprobó un posible desconocimiento en cuanto a la aplicación del procedimiento de verificación de que los afiliados incluidos como morosos (base de datos de TI) efectivamente se encuentren con dicho estado en el sistema SIBU.

Según la información proporcionada existen respuestas diferentes en cuanto a la forma de corroborar que los rebajos de planilla y de afiliados pensionados (reporte realizado por TI) sean los correctos, esto debido a las diferentes respuestas obtenidas, las cuales se detallan a continuación:

1. El área de TI realiza el proceso validando y procesando las inconsistencias.
2. Se desconoce el procedimiento.
3. Se verifica el estado de cuenta de cada persona afiliada.

Así mismo, se determinó la incompatibilidad en las respuestas en lo referente a la verificación por parte del departamento en lo relacionado con las deducciones ejecutadas por TI en

cuanto a la correcta aplicación en el sistema SIBU a continuación se brindan las respuestas de los colaboradores:

1. Al inicio del mes se toma una muestra para validar la correcta aplicación.
2. Se desconoce el procedimiento.
3. El departamento de crédito y cobro realiza una revisión de la aplicación de planilla.

También se ha determinado la poca uniformidad en las respuestas brindadas en cuanto a la frecuencia de lo siguiente:

- Periodicidad del envío de la cartera de crédito al Departamento de Crédito y Cobro por parte del Departamento de TI, las respuestas otorgadas son las siguientes:

    1. Diario.
    2. Semanalmente.
    3. Una vez al mes.

- Regularidad de revisión en el sistema SIBU de la clasificación de morosidad de créditos (gestión de cobro y cobro judicial), las respuestas fueron las siguientes:

    1. Mensual, con los reportes de morosidad.
    2. Se desconoce.

Gestionar la continuidad

Existe respaldo de los expedientes de créditos de manera digital y se realizan de forma diaria por los encargados. Así mismo, se mantiene un historial crediticio de todos los créditos otorgados a cada uno de los afiliados y se encuentra oportunamente respaldado.

Gestionar la identificación y construcción de soluciones

Los resultados indican que los cambios solicitados y realizados al módulo de crédito y cobro son comunicados previamente al personal responsable del proceso.

Gestionar las operaciones

Los colaboradores del Departamento de Crédito y Cobro tienen conocimiento de los procedimientos a aplicar para el adecuado otorgamiento de los créditos. Así mismo, se indicó que todos los responsables reciben capacitaciones de manera regular en el uso correcto del sistema SIBU.

Tecnología de Información

Marco estratégico de Tecnologías de información

Según los resultados obtenidos, la JAFAP cuenta con plan estratégico de tecnologías de información, debidamente alineado a la estrategia institucional. Dentro del personal del departamento de tecnología de información no existe claridad sobre la existencia de procedimientos para la ejecución del plan estratégico de TI vigente.

Gestión de la calidad

Con base en los resultados obtenidos se determina que el departamento de TI es auditado tanto por la auditoría interna como por auditoría externa, esta última al menos una vez al año. Adicionalmente, la JAFAP cuenta con una política debidamente aprobada y divulgada que promueve la mejora continua de los servicios de TI.

Gestión de riesgos

En lo referente a la gestión de riesgos, según la información obtenida, se puede determinar que la JAFAP no cuenta con una metodología de análisis de riesgos, no se cuenta con una lista de amenazas para cada riesgo ni con un método para calcular el riesgo inherente y residual. Adicionalmente, no se cuenta con procedimientos relacionados con el diseño de planes de acciones de respuesta a los riesgos ni procedimientos orientados al monitoreo periódico de las vulnerabilidades, amenazas y riesgos identificados.

Gestión de la seguridad de la información

- **Implementación de un marco de seguridad**

Los resultados obtenidos indican la claridad sobre la existencia de una política debidamente aprobada y divulgada la cual defina tanto los lineamientos como los controles para un marco de

seguridad de la información, sin embargo, se cuenta con un procedimiento aprobado y comunicado, es decir, debidamente informado a los colaboradores, para la revisión periódica del marco de seguridad de la información.

- **Compromiso del personal con la seguridad de la información**

Según los resultados obtenidos, la JAFAP cuenta con un plan global de seguridad de TI debidamente aprobado y divulgado al personal, en el cual se definen las políticas y los procedimientos relacionados con la seguridad de la información.

Además, existe un procedimiento mediante el cual se establecen las responsabilidades sobre la seguridad de la información y se cuenta con acuerdos de confidencialidad, medidas de seguridad específicas, relacionadas con el manejo de la documentación y rescisión de contratos.

- **Seguridad física y ambiental**

Los resultados indican la existencia de políticas de seguridad debidamente aprobadas y divulgadas para la implementación de medidas de seguridad físicas tales como: esquema del perímetro de seguridad, zonas de seguridad, ubicación de equipos críticos, entre otros. Dentro de estas políticas se establecen las responsabilidades sobre el monitoreo, procedimientos de reporte y resolución de incidentes de seguridad física.

Por otra parte, según los resultados se determina que los cuartos de servidores cuentan con aire acondicionado, así como con extintores de CO2 para casos de emergencias, a los cuales se les da mantenimiento en las fechas de recarga respectivas.

Por último, se cuenta con bitácoras actualizadas las cuales mantienen controles sobre el ingreso y salida de los activos de TI y los demás activos de la Organización.

- **Seguridad en las operaciones y comunicaciones**

De acuerdo con los resultados, se cuenta con medidas de prevención, detección y corrección

para proteger los sistemas de información y tecnología contra *software* malicioso[13].

- **Control de acceso**

Según los resultados obtenidos, se ha determinado que los cuartos de servidores cuentan con acceso restringido, dicho acceso es para el coordinador de infraestructura y para la jefatura del departamento de TI.

Por otra parte, no existe claridad en los colaboradores del departamento de TI sobre la existencia de políticas para la propiedad, custodia y responsabilidad sobre los recursos de TI, así como tampoco sobre políticas de acceso para el manejo de información impresa o almacenada en medios físicos.

Según los resultados obtenidos, el Oficial de Seguridad de TI es quien tiene acceso al módulo de seguridad del sistema SIBU. Mediante este módulo, se verifica que quienes tengan acceso al sistema sean funcionarios de la JAFAP, además, mediante la configuración de perfiles y roles autorizados se verifica el acceso por parte de los usuarios a los módulos o transacciones relacionadas con sus puestos, sin embargo, no se tiene claro la periodicidad de revisión de accesos a dicho sistema. Además, no sé tiene conocimiento sobre las verificaciones de usuarios bloqueados o inactivos en el sistema SIBU.

- **Continuidad de los Servicios de TI**

Relacionado a la revisión de servidores no existe uniformidad en las respuestas obtenidas, algunos funcionarios de TI indican no tener conocimiento sobre dicha revisión. En lo referente a la periodicidad de la revisión, se indica que es diaria y bimensual, esto evidencia falta de claridad en este tema por parte del personal del Departamento de TI.

Sobre el respaldo de bases de datos, ha sido terminado mediante las respuestas del área de

[13] El software malicioso, conocido en inglés como “malware”, es un software diseñado específicamente para obtener acceso a un equipo o dañarlo sin que el usuario tenga conocimiento. Hay distintos tipos de software malicioso, como el spyware, los registradores de pulsaciones, los virus, los gusanos o cualquier tipo de código malicioso que se infiltre en un equipo. (Norton, 2021. Recuperado de https://mx.norton.com/internetsecurity-malware.html)

TI que hace con regularidad, específicamente a diario, bajo la responsabilidad del *Datebase Administrator* (DBA).

Los resultados indican que no hay criterios uniformes sobre la existencia de contratos *Service Level Agreement (SLA)* con el proveedor de internet de la JAFAP, una respuesta indica no tener conocimiento y las restantes respuestas señalan la existencia de dichos contratos. Por otra parte, no existe claridad sobre quien es el proveedor de internet de la JAFAP, pues las respuestas indican diferentes proveedores, a saber, ICE y UCR.

Sobre la existencia de plan de continuidad de servicios de TI, no hay claridad sobre la existencia de dicho plan debidamente aprobado y divulgado a los colaboradores, sin embargo, según los resultados obtenidos si se tienen documentadas las acciones preventivas y correctivas para mantener la continuidad razonable de los procesos.

En lo relacionado con la realización de pruebas de validación del plan de continuidad del negocio y su correcta operación, los resultados muestran la no realización de dichas pruebas, así mismo, se indica que la JAFAP no cuenta con un sitio alterno fuera de la UCR.

Decisiones sobre asuntos estratégicos

Según los resultados obtenidos, se cuenta con un Comité de Tecnología el cual defina prioridades, asigne recursos y atienda los requerimientos de la Institución.

3.1.3 Realizar análisis FOCAR.

La herramienta FOCAR permite el estudio de la situación actual de las empresas mediante el análisis de las características y condiciones tanto internas como externas. El resultado obtenido con la aplicación de esta metodología ayuda a planificar una estrategia de acuerdo con las características propias y el mercado en donde se desenvuelve. Mediante este análisis se evalúan las fortalezas, oportunidades, carencias, amenazas y riesgos.

3.1.3.1 Análisis de las fortalezas de la Entidad. (Interno)

Las fortalezas se definen como los recursos y capacidades con los que cuentan las empresas para generar una ventaja competitiva a nivel de mercado y desempeñarse de manera eficaz en sus

funciones. A continuación, se detallan las fortalezas identificadas:

- Utilización de software diseñado de acuerdo con las necesidades: actualmente la JAFAP cuenta con el sistema SIBU, el cual presenta una serie de características y funcionalidades creadas de acuerdo con las especificaciones de la Entidad y se actualiza conforme las necesidades. Este sistema trabaja mediante módulos que permite a los funcionarios realizar el trabajo de manera sistematizada casi en un cien por ciento y con ello disminuir el riesgo asociado a errores humanos.

- Recurso humano altamente calificado: el personal a cargo de las labores administrativas, servicio al cliente y control cuenta con amplios conocimientos y poseen estudios académicos relacionados con el campo laboral de su área.

- Variedad de servicios y productos: la Junta ofrece variedad de préstamos para sus afiliados por ejemplo de vivienda, vehículo, pólizas, especiales, sobre aportes, entre otros (Ver a detalle en el capítulo II). Así mismo, permite al afiliado crear y mantener ahorros con tasas de interés atractivas. Para facilitar el acceso de los afiliados a préstamos y ahorros, la JAFAP ha creado requisitos agiles y eficientes para la solicitud de estos.

- Bajo nivel de morosidad: la deducción de los aportes y cuotas de los afiliados es de forma directa mediante rebajo de salario, lo cual contribuye a mantener bajos niveles de morosidad.

3.1.3.2 Análisis de las oportunidades de la Entidad. (Externo)

Las oportunidades se definen como los factores positivos y favorables que se desarrollan en el entorno actual para obtener ventajas competitivas. La Empresa puede utilizar las oportunidades y disminuir el impacto de las amenazas de las cuales tiene poco o ningún control directo. A continuación, se detallan las oportunidades identificadas:

- Acceso a la tecnología: alto uso de las tecnologías y redes sociales para llegar a los funcionarios de nuevo ingreso a la Universidad. Al estar dentro de las instalaciones de la

Universidad de Costa Rica, todos los usuarios cuentan con acceso a internet lo cual permite una mayor comunicación e interacción de los afiliados.

- Necesidad del producto: fomento de ahorro y colocación de créditos para ayudar a las personas afiliadas con proyectos personales o crisis financieras las cuales requieren buscar entidades con experiencia y las cuales ofrezcan las mejores condiciones dentro del mercado.

- Existencia de clientes potenciales: según el Artículo 4 de la Ley 4273, todo funcionario de la Universidad de Costa Rica debe ser afiliado de la JAFAP para contribuir al fondo creado por esta ley.

- Facilidad por parte del cliente para el acceso a los productos: la JAFAP tiene presencia en cada una de las sedes y recintos de la Universidad de Costa Rica esto permite a los clientes acercarse fácilmente para solicitar los productos y servicios requeridos.

3.1.3.3 Análisis de las carencias de la Entidad. (Interno)

Las carencias se definen como factores que provocan una situación desfavorable frente a la competencia, por recursos y habilidades o falta de estos. Las carencias identificadas podrían impedir una buena dirección de la Empresa, por lo tanto, al desarrollar una adecuada estrategia pueden ser eliminadas. A continuación, se detallan las carencias identificadas:

- Ubicación de la JAFAP: esta Entidad se encuentra dentro de las instalaciones de la Universidad de Costa Rica, lo cual implica estar sujetos a la gestión y tiempos de respuesta propios de cada área o unidad de la Institución.

- Distribución inadecuada de espacio físico de las instalaciones: la JAFAP requiere mejorar aspectos como el sistema eléctrico, distribución en plataforma de servicios, hacinamiento en algunas áreas e instalación de centros de impresión. Es importante en este aspecto, verificar las condiciones y ajustarse a la nueva normalidad según medidas dictadas por el Ministerio de Salud de Costa Rica.

- Espacios inadecuados de oficinas ubicadas en sedes y recintos universitarios: la JAFAP realizó una encuesta de servicio a la persona afiliada, los resultados muestran que el 76 % de las personas afiliadas entrevistadas en sedes considera la necesidad de la remodelación de las instalaciones para mayor comodidad, dicha respuesta refleja una posible inconformidad de los clientes, los cuales eventualmente pueden buscar nuevas instituciones para adquirir productos y servicios.

3.1.3.4 Análisis de las amenazas de la Entidad. (Externo)

Las amenazas se definen como situaciones negativas externas a la Empresa las cuales no pueden ser controladas y pueden provocar efectos negativos, por lo cual en algunos casos es necesario desarrollar una estrategia adecuada para hacer frente a las mismas. A continuación, se detallan las amenazas identificadas:

- Cambios en leyes y regulaciones: actualmente en Costa Rica las leyes de impuestos son cambiantes debido a la crisis fiscal del país, por lo cual todos los mercados están expuestos a la implementación de nuevas prácticas fiscales implicando un impacto financiero sobre las empresas.

- Gran cantidad de competidores: a nivel nacional existe amplia oferta de Cooperativas y Entidades Financieras que ofrecen diferentes servicios, préstamos y ahorros a sus clientes por tanto la oferta financiera en el mercado es alta.

- Situación económica actual del país: mejores tasas y beneficios por parte de la competencia, menor cantidad de colaboradores dispuestos a adquirir los productos de la Entidad y menos ingreso de personal lo cual genera una disminución en los ingresos para la Junta y por ende los préstamos disponibles se reducen.

3.1.3.5 Análisis de los riesgos de la Entidad.

Los riesgos se definen como la posibilidad de ocurrencia de un evento que provoque efectos en la continuidad del negocio, los mismos podrían tener diferentes niveles de impacto.

Para mayor conocimiento según Canales et al. (2014) se describen los siguientes riesgos:

- Riesgos operativos: es el potencial de pérdida, debido a la falla en los procesos internos, recursos humanos y sistemas de la Entidad a consecuencia de acontecimientos externos fuera del control directo de las empresas.

- Riesgos ambientales: es la probabilidad de afectación de un espacio geográfico por consecuencias de un proceso natural que afecte los espacios físicos y actividades humanas.

- Riesgos financieros: probabilidad de la ocurrencia de un evento que genere consecuencias financieras negativas o adversas para una empresa. Pueden ser provocados por la volatilidad del mercado tanto en divisas como en los tipos de interés y en su capacidad de liquidez u operativa, al no poder afrontar sus obligaciones con el desempeño esperado en el ciclo normal de su operación.

- Riesgos psicosociales: son condiciones presentes en situaciones laborales relacionados con el trabajo, tipo de puesto, realización de las tareas y el entorno, los cuales afectan el trabajo y la salud de las personas trabajadoras.

Así mismo, el riesgo tecnológico según (Boccazzi y Negrete, 2015) se describe como la "probabilidad de sufrir daños o pérdidas económicas, ambientales y humanas como consecuencia del funcionamiento deficiente o accidente de una tecnología aplicada en una actividad humana".

A continuación, se detallan los riesgos asociados a la Entidad:

- Riesgo de captación: por el giro de negocio de la JAFAP existe probabilidad de no recuperar los préstamos otorgados en su totalidad, esto provoca una disminución significativa de los ingresos, liquidez e inversiones.

- Riesgo tecnológico: la JAFAP cuenta con sistemas tecnológicos para la operatividad de la Institución, por tanto, las fallas en los mismos pueden interrumpir el adecuado funcionamiento de las labores y comunicación con los afiliados.

3.1.4 Realizar análisis comparativo con base en el marco de referencia.

Para realizar el análisis comparativo se procedió con la elaboración de las matrices basadas en los criterios de COBIT 5 y el Capítulo I "Normas de Aplicación General" (N-2-2007-CO-DFOE) de la Contraloría General de la República.

3.1.4.1 Matriz de revisión según COBIT 5

La matriz de revisión según COBIT 5 fue elaborada con base en los resultados de los cuestionarios aplicados a los colaboradores de la JAFAP (Anexo 1, 2 y 3), así como la revisión de las políticas y procedimientos existentes, los mismos alineados con el alcance de este proyecto.

La finalidad de esta matriz es realizar un análisis comparativo entre los marcos de referencia y los procesos contables mediados por las Tecnologías de Información aplicados actualmente por la JAFAP para el logro de sus objetivos. Con los resultados arrojados en dicho análisis se obtendrá la base para la creación de nuestra propuesta de mejora.

Para la elaboración de la matriz se realizó un análisis los procesos y las metas de COBIT 5 alineados con la JAFAP para el cumplimiento de las normas de aplicación general, a continuación, se da una breve explicación de cada uno de los procesos y metas seleccionados según ISACA (2012):

Dominio: Procesos

Evaluar, Orientar y Supervisar (EDM)

EDM03: Asegurar la Optimización del Riesgo: Asegurar que el apetito y la tolerancia al riesgo de la Empresa son entendidos, articulados y comunicados y que el riesgo para el valor de la Empresa relacionado con el uso de las TI es identificado y gestionado.

Alinear, Planificar y Organizar (APO)

APO01: Gestionar el Marco de Gestión de TI: Aclarar y mantener el Gobierno de la misión y la visión corporativa de TI. Implementar y mantener mecanismos y autoridades para la gestión de la información y el uso de TI en la empresa para apoyar los objetivos de Gobierno en consonancia con las políticas y los principios rectores.

APO02: Gestionar la Estrategia: Proporcionar una visión holística del negocio actual y del entorno de TI, la dirección futura y las iniciativas necesarias para migrar al entorno deseado. Aprovechar los bloques y componentes de la estructura empresarial, incluso los servicios externalizados y las capacidades relacionadas para permitir una respuesta ágil, confiable y eficiente a los objetivos estratégicos.

APO07: Gestionar los Recursos Humanos: Proporcionar un enfoque estructurado para garantizar una óptima estructuración, ubicación, capacidades de decisión y habilidades de los recursos humanos. Esto incluye la comunicación de las funciones, responsabilidades definidas, la formación, planes de desarrollo personal y las expectativas de desempeño con el apoyo de gente competente y motivada.

APO011: Gestionar la Calidad: Definir y comunicar los requisitos de calidad en todos los procesos, procedimientos y resultados relacionados de la Organización, incluso controles, vigilancia constante, el uso de prácticas probadas, estándares de mejora continua y esfuerzos de eficiencia.
APO012: Gestionar el Riesgo: Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa.

APO013: Gestionar la Seguridad: Definir, operar y supervisar un sistema para la gestión de la seguridad de la información.

Construcción, Adquisición e Implementación (BAI)

BAI01: Gestionar los Programas y Proyectos: Gestionar todos los programas y proyectos del portafolio de inversiones de forma coordinada y en línea con la estrategia corporativa. Iniciar, planificar, controlar, ejecutar programas, proyectos y cerrarlos con una revisión post-implementación.

BAI03: Gestionar la Identificación y la Construcción de Soluciones: Establecer y mantener soluciones identificadas en línea con los requerimientos de la Empresa abarcando el diseño, desarrollo, compras/contratación y asociación con proveedores/fabricantes. Gestionar la configuración, preparación de pruebas, realización de pruebas, gestión de requerimientos y mantenimiento de procesos de negocio, aplicaciones, datos/información, infraestructura y servicios.

Entregar, dar Servicio y Soporte (DSS)

DSS01: Gestionar las Operaciones: ver en apartado 3.1.1 de este capítulo

DSS02: Gestionar las Peticiones y los Incidentes del Servicio: ver en apartado 3.1.1 de este capítulo

DSS04: Gestionar la Continuidad: ver en apartado 3.1.1 de este capítulo

DSS05: Gestionar los Servicios de Seguridad: en apartado 3.1.1 de este capítulo

DSS06: Gestionar los Controles de los Procesos del Negocio: Definir y mantener controles apropiados de proceso de negocio para asegurar que la información relacionada y procesada dentro de la Organización o de forma externa satisface todos los requerimientos relevantes para el control de la información.

Supervisión, Evaluación y Verificación (MEA)

MEA02: Supervisar, Evaluar y Valorar el Sistema de Control Interno: Facilitar a la Dirección la identificación de deficiencias e ineficiencias en el control y el inicio de acciones de mejora. Planificar, organizar, mantener normas para la evaluación del Control Interno y las actividades de aseguramiento.

MEA03: Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos: Evaluar el cumplimiento de requisitos regulatorios y contractuales tanto en los procesos de TI como en los procesos de negocio dependientes de las tecnologías de la información. Obtener garantías de que se han identificado, se cumple con los requisitos y se ha integrado el cumplimiento de TI en el cumplimiento de la empresa general.

Metas relacionadas con TI

Según COBIT 5 (ISACA, 2012), cada empresa opera en un contexto diferente determinado por factores externos y factores internos requeridos por un sistema de Gobierno y gestión personalizada. Las necesidades de las partes interesadas deben transformarse en una estrategia corporativa factible. La cascada de metas de COBIT 5 permite transformar las necesidades de las partes interesadas metas corporativas, que desencadenan en metas relacionadas con las TI para anidarse en metas catalizadoras específicas, útiles y a medida. Esto permite establecer metas específicas en todos los niveles y en todas las áreas de la empresa en apoyo de los objetivos generales y requisitos de las partes interesadas, de esta forma, soportar la alineación entre las necesidades de la empresa, las soluciones y servicios de TI.

Dentro de las metas de la JAFAP relacionadas con TI se encuentran las siguientes, divididas según el tipo de objetivo empresarial:

Financieras

1. Alineamiento de TI y la estrategia de negocio.
2. Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas.

3. Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI.
4. Riesgos de negocio relacionados con las TI gestionados.

Cliente

1. Entrega de servicios de TI de acuerdo con los requisitos del negocio.

Interna

1. Seguridad de la información, infraestructura de procesamiento y aplicaciones.
2. Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.
3. Disponibilidad de información útil y relevante para la toma de decisiones.
4. Cumplimiento de las políticas internas por parte de las TI.

Posteriormente se estableció una clasificación para cada proceso, la cual se detalla a continuación:

Ilustración 4 Clasificación Procesos COBIT 5

SIMBOLOGÍA		
CUMPLE		La entidad cumple con los requerimientos establecidos en los procesos de COBIT 5.
CUMPLE PARCIALMENTE		El cumplimiento es parcial, se identificaron debilidades en la alineación con los procesos de COBIT 5.
NO CUMPLE		No existe alineación alguna con lo que dictan los procesos de COBIT 5.

Fuente: elaboración propia

Seguidamente, se asignaron las metas de acuerdo con el grado de importancia de los procesos de COBIT 5 y el cumplimiento de los objetivos de la JAFAP, dónde Principal “P” corresponde a la existencia de una relación importante, por ejemplo el proceso de COBIT 5 proporciona un soporte imprescindible para conseguir las metas relacionadas con TI y Secundario “S” representa un vínculo fuerte pero menos importante, por ejemplo el proceso de COBIT 5 es un apoyo secundario para los procesos relativos a TI.

A continuación, se presenta la matriz de evaluación de COBIT 5 con los resultados obtenidos:

Tabla 1 Matriz de evaluación COBIT 5

			Meta relacionada con las TI				
			Entrega de servicios de TI de acuerdo a los requisitos del negocio	Seguridad de la información, infraestructura de procesamiento y aplicaciones	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	Disponibilidad de información útil y relevante para la toma de decisiones	Cumplimiento de las políticas internas por parte de las TI
Procesos de COBIT 5			Cliente	Interna			
Evaluar, Orientar y Supervisar	EDM03	Asegurar la Optimización del Riesgo	S	P	S	S	P
Alinear, Planificar y Organizar	APO01	Gestionar el Marco de Gestión de TI	S	S	S	S	S
	APO02	Gestionar la Estrategia	P	S	S	S	S
	APO07	Gestionar los Recursos Humanos	S	S	S	S	S
	APO11	Gestionar la Calidad	P	S	P	S	S
	APO12	Gestionar el Riesgo	S	P	P	S	S
	APO13	Gestionar la Seguridad	S	P	S	P	S
Construcción, Adquisición e Implementación	BAI01	Gestionar los Programas y Proyectos	S	S	P	S	S
	BAI03	Gestionar la Identificación y la Construcción de Soluciones	P	S	S	S	S
Entregar, dar Servicio y Soporte	DSS01	Gestionar las Operaciones	P	S	S	S	S
	DSS02	Gestionar las Peticiones y los Incidentes del Servicio	P	S	S	S	S
	DSS04	Gestionar la Continuidad	P	S	S	P	S
	DSS05	Gestionar los Servicios de Seguridad	S	P	S	S	S
	DSS06	Gestionar los Controles de los Procesos del Negocio	S	P	S	S	S
Supervisión, Evaluación y Verificación	MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno	S	S	S	S	P
	MEA03	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos	S	S	S	S	S

Nota aclaratoria: P: Principal y S: Secundario

Fuente: elaboración propia

			Meta relacionada con las TI			
			Alineamiento de TI y la estrategia de negocio	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	Riesgos de negocio relacionados con las TI gestionados
Procesos de COBIT 5			Financiera			
Evaluar, Orientar y Supervisar	EDM03	Asegurar la Optimización del Riesgo	S	S	S	P
Alinear, Planificar y Organizar	APO01	Gestionar el Marco de Gestión de TI	P	P	S	S
	APO02	Gestionar la Estrategia	P	S	S	S
	APO07	Gestionar los Recursos Humanos	P	S	S	S
	APO11	Gestionar la Calidad	S	S	S	S
	APO12	Gestionar el Riesgo	S	P	S	P
	APO13	Gestionar la Seguridad	S	P	S	P
Construcción, Adquisición e Implementación	BAI01	Gestionar los Programas y Proyectos	P	S	S	P
	BAI03	Gestionar la Identificación y la Construcción de Soluciones	S	S	S	S
Entregar, dar Servicio y Soporte	DSS01	Gestionar las Operaciones	S	S	S	P
	DSS02	Gestionar las Peticiones y los Incidentes del Servicio	S	S	S	P
	DSS04	Gestionar la Continuidad	S	S	S	P
	DSS05	Gestionar los Servicios de Seguridad	S	P	S	P
	DSS06	Gestionar los Controles de los Procesos del Negocio	P	P	S	S
Supervisión, Evaluación y Verificación	MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno	S	P	S	P
	MEA03	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos	S	P	S	P

Nota aclaratoria: P: Principal y S: Secundario

Fuente: elaboración propia

3.1.4.2 Matriz de revisión según las Normas técnicas para la gestión y el control de las Tecnologías de Información de la Contraloría General de la República Capítulo I "Normas de Aplicación General" (N-2-2007-CO-DFOE).

Con el propósito de evaluar el cumplimiento del capítulo "Normas de Aplicación General" de las Normas técnicas para la gestión y el control de las Tecnologías de Información de la CGR, se procedió a evaluar una matriz en donde se evalúan los diferentes criterios contenidos en dicho capítulo observados como parte de la gestión de la JAFAP, para evaluar y perfeccionar el sistema de Control Interno organizacional y facilitar el cumplimiento de la integración de la tecnología de información en sus procesos para el logro de los objetivos.

Se estableció una escala de valoración para cada uno de los apartados según el siguiente detalle:

Tabla 2 Escala de valoración - Normas de aplicación general

Valoración	Criterio
Cumple Excelente 4	La Organización cumple con los requerimientos establecidos en las Normas Técnicas de la Contraloría General de la República.
Cumple satisfactoriamente 3	La Organización mantiene un alineamiento fuerte respecto a las Normas Técnicas de la CGR, proporciona un nivel razonable de cumplimiento con las mismas
Cumple adecuadamente 2	El cumplimiento es parcial, se identificaron debilidades en la alineación con las Normas de la CGR.
Cumple débilmente 1	La Organización no alcanza un nivel de cumplimiento aceptable, pues existen muchas debilidades o deficiencias en la alineación con las Normas Técnicas de la Contraloría General de la República.
No cumple 0	La Organización no alcanza un nivel de cumplimiento aceptable, aun cuando existen muchas debilidades o deficiencias en la alineación con las Normas Técnicas de la

	Contraloría General de la República.

Fuente: elaboración propia

Según la escala de valoración anterior, el nivel óptimo para cada uno de los puntos a evaluar es un valor de 4, con base en esto se genera una puntuación para cada una de las siguientes áreas del capítulo de Normas de aplicación general, a saber:

- Marco Estratégico de TI
- Gestión de la Calidad
- Gestión de Riesgos
- Gestión de la seguridad de la información
- Gestión de Proyectos
- Decisiones sobre asuntos estratégicos de TI
- Cumplimiento de obligaciones relacionadas con la gestión de TI

Con el objetivo de evaluar estas áreas se ha establecido una serie de puntos de revisión, lo cual otorga un peso porcentual para cada área según la cantidad de los criterios a evaluar que presentan las normas técnicas, a continuación, se presenta el detalle:

Tabla 3 Distribución porcentual de criterios de evaluación por área de revisión

Áreas de revisión	Peso %	Puntos
Marco estratégico de TI	3	1
Gestión de la calidad	7	2
Gestión de riesgos	17	5
Gestión de la seguridad de la información	63	19
Gestión de proyectos	3	1
Decisiones sobre asuntos estratégicos de TI	3	1
Cumplimiento de obligaciones relacionadas con la gestión de TI	3	1
Total	**100 %**	**30**

Fuente: elaboración propia

Una vez establecidos los criterios de revisión se establecieron los componentes para evaluar cada una de las áreas indicadas anteriormente y aplicar la escala de valoración definida, con base en la información obtenida en los cuestionarios aplicados al personal de la JAFAP, así como la revisión de las políticas y procedimientos existentes. A continuación, se detallan los componentes evaluados en cada área, así como los resultados de la evaluación realizada.

.

Tabla 4 Matriz de evaluación - Normas de Aplicación General

Áreas de revisión		**Nivel óptimo**	**Evaluación**	
			Sí	**No**
Marco estratégico de TI				
Se cuenta con un procedimiento aprobado y divulgado y para ejecutar el plan estratégico de TI		4	3	
Calificación	**75 %**	4	3	0
Gestión de la Calidad				
Se cuenta con una política aprobada y divulgada que promueva la mejora continua de los servicios de TI		4	3	
Se cuenta con una política aprobada y divulgada de estándares de calidad de los servicios de TI		4	3	
Calificación	**75 %**	**8**	**6**	**0**
Gestión de riesgos				
Se cuenta con una metodología aprobada y divulgada para el análisis y gestión de riesgos		4		0
Se cuenta con una lista de amenazas para cada análisis de riesgos		4		0
Se cuenta con un método para calcular riesgo inherente y residual		4		0
Se cuenta con un procedimiento aprobado y divulgado para diseñar el plan de acción como respuesta al riesgo		4		0
Se cuenta con un procedimiento aprobado y divulgado para monitorear periódicamente las vulnerabilidades, amenazas y riesgos identificados		4		0

Calificación	**0 %**	**20**	**0**	**0**
Gestión de la seguridad de la información				
Implementación de un marco de seguridad de la información				
Se cuenta con una política aprobada y divulgada que defina los lineamientos y controles para un marco de seguridad de la información		4	3	
Se cuenta con una política aprobada y divulgada que defina las responsabilidades de los funcionarios relacionadas con el marco de seguridad de la información		4	4	
Se cuenta con un procedimiento aprobado y divulgado para la revisión periódica del marco de seguridad de la información		4	4	
Compromiso del personal con la seguridad de la información				
Se cuenta con un plan global de seguridad TI aprobado y divulgado, donde se defina la implementación de políticas y procedimientos de seguridad de la información		4	4	
Se cuenta con un procedimiento aprobado y divulgado para la vigilancia del debido cumplimiento de las responsabilidades de la seguridad de la información		4	4	
Se cuenta acuerdos vigentes de confidencialidad y medidas de seguridad específicas, relacionadas con el manejo de la documentación y rescisión de contratos		4	4	
Seguridad física y Ambiental				
Se cuenta con una política aprobada y divulgada para la implementación de medidas de seguridad físicas tales como: esquema		4	4	

del perímetro de seguridad, zonas de seguridad, ubicación de equipos críticos, entre otros			
Se cuenta con una política aprobada y divulgada que establezca las responsabilidades sobre el monitoreo, los procedimientos de reporte y resolución de incidentes de seguridad física	4	4	
Se cuenta con una bitácora para el control de ingreso y salida de activos de TI de la Organización	4	4	
Seguridad en las operaciones y telecomunicaciones			
Se cuenta con medidas de prevención, detección y corrección a lo largo de toda la Organización para proteger los sistemas de información y la tecnología contra *software* malicioso	4	4	
Control de acceso			
Se cuenta con una política aprobada y divulgada que establezca procedimientos relacionados con el acceso a la información, al *software* de base y de aplicación, a las bases de datos y a las terminales y otros recursos de comunicación	4	3	
Se cuenta con una política aprobada y divulgada que establezca controles de acceso para el manejo de información impresa, visible o almacenada en medios físicos	4	1	0
Se cuenta con una política aprobada y divulgada que defina la propiedad, custodia y responsabilidad sobre los recursos de TI	4	3	
Seguridad en la implementación y mantenimiento de *software* e infraestructura tecnológica			

Se cuenta con una política aprobada y divulgada que defina los requerimientos de seguridad sobre los ambientes de desarrollo, mantenimiento y producción		4	4	
Se cuenta con un procedimiento aprobado, divulgado y que defina el acceso a los programas fuente y a los datos de prueba		4	4	
Continuidad de los servicios de TI				
Se cuenta con un plan de continuidad de los servicios de TI aprobado, divulgado		4	3	
Se documentan las acciones preventivas y correctivas para mantener una continuidad razonable de los procesos		4	4	
Se realizan y documentan pruebas para validar que el plan de continuidad de negocio está operando satisfactoriamente		4	1	
Se cuenta con un sitio alterno de TI fuera de la UCR		4		0
Calificación	**82 %**	**76**	**62**	**0**
Gestión de proyectos				
Se cuenta con una metodología de administración de proyectos aprobada de manera que se logren sus objetivos, satisfaga los requerimientos y cumpla con los términos de calidad, tiempo y presupuesto óptimos preestablecidos		4		0
Calificación	**0 %**	**4**	**0**	**0**
Decisiones sobre asuntos estratégicos de TI				
Se ha definido un comité de tecnología que defina prioridades, que asigne recursos y que atienda los requerimientos de la institución		4	3	

Calificación	**75 %**	**4**	**3**	**0**
Cumplimiento de obligaciones relacionadas con la gestión de TI				
Se cuenta con una lista de los componentes que conforman el marco jurídico que aplica TI		4	4	
Calificación	**100 %**	**4**	**4**	**0**

Fuente: elaboración propia

Con base en la revisión de criterios y componentes establecidos en la matriz anterior, se obtuvieron las siguientes calificaciones por área de revisión:

Tabla 5 Resultados de evaluación por área

Áreas de revisión	**Calificación %**
Marco estratégico de TI	75
Gestión de la calidad	75
Gestión de riesgos	0
Gestión de la seguridad de la información	82
Gestión de proyectos	0
Decisiones sobre asuntos estratégicos de TI	75
Cumplimiento de obligaciones relacionadas con la gestión de TI	100

Fuente: elaboración propia

Según los resultados obtenidos en la evaluación de los componentes establecidos fueron consolidadas las calificaciones obtenidas (Tabla 4) según el peso porcentual de cada área (Tabla 3-2) y, de esta forma obtener el porcentaje general ponderado de cumplimento de las Norma de

Aplicación General por parte de la JAFAP, para obtener los siguientes resultados:

Tabla 6 Resultado General de Cumplimiento

Áreas de Revisión	**Peso %**	**Calificación obtenida %**	**General Ponderado %**
Marco estratégico de TI	3	75	3
Gestión de la Calidad	7	75	5
Gestión de Riesgos	17	0	0
Gestión de la Seguridad de la Información	63	82	52
Gestión de Proyectos	3	0	0
Decisiones sobre asuntos estratégicos	3	75	3
Cumplimiento de obligaciones relacionadas con la gestión de TI	3	100	3
Cumplimiento General			**65 %**

Fuente: elaboración propia

De acuerdo con la revisión y los resultados obtenidos en la tabla anterior, se ha determinado que la JAFAP presenta un cumplimiento general de las Normas de Aplicación General de 65 %. Destacan en la evaluación las áreas de gestión de riesgos y gestión de proyectos, donde la JAFAP no cumple con los criterios establecidos en las Normas Técnicas, así como la gestión de la seguridad de la información y el cumplimiento de obligaciones relacionadas con la gestión de TI en donde se presentan los porcentajes más altos de cumplimiento.

3.1.5 Resultados de evaluación comparativa.

De acuerdo con la revisión realizada en el presente capítulo, se presentan los resultados de la evaluación comparativa de acuerdo con las Normas Técnicas para la gestión y el control de las Tecnologías de Información mediante un análisis de COBIT 5.

Áreas de revisión

Marco Estratégico de TI

Según los resultados obtenidos en la revisión realizada se identificó que la JAFAP cuenta con un marco estratégico de TI constituido por políticas y procedimientos para su cumplimiento, sin embargo, las mismas no son de conocimiento general de los colaboradores.

Una adecuada gestión de la estrategia y correcta aplicación del marco de gestión por parte de la JAFAP permitiría un mejor alineamiento entre las TI y la estrategia de negocio que contribuyen al logro de los objetivos organizacionales mediante la entrega de servicios de TI.

Adicionalmente, el marco estratégico de TI contribuye a que la JAFAP cumpla con las leyes y regulaciones aplicables al negocio, por ejemplo, la protección de datos de los afiliados.

Gestión de la Calidad

La JAFAP cuenta con políticas y procedimientos que promueven un enfoque de eficiencia y mejoramiento continuo de los productos y servicios de TI, no obstante, dichas políticas y procedimientos no han sido debidamente divulgados, lo anterior se determinó que algunos colaboradores tienen desconocimiento de estos.

A su vez, se cuenta con una política de estándares de calidad de los servicios de TI debidamente aprobada, a pesar de esto, dicha política es desconocida por el personal de la JAFAP.

Como parte de la gestión de los recursos humanos y del proceso de desarrollo del personal, se considera importante la comunicación de funciones y responsabilidades a cada colaborador

dentro de las cuales se debe incluir las políticas, los procedimientos generales de la Organización y específicos a cada área de trabajo.

En caso de contar con una correcta divulgación y capacitación sobre las políticas y procedimientos relacionados con la calidad de productos y servicios de TI, la JAFAP mejoraría la entrega de servicios y programas de acuerdo con los requisitos del negocio que proporcionan beneficios a tiempo, dentro del presupuesto, satisfaciendo los requisitos y normas de calidad.

Gestión de Riesgos

De acuerdo con la información recopilada, la JAFAP no cuenta con un marco integral de gestión de riesgos aprobado, divulgado que permita la identificación, el análisis cualitativo y cuantitativo de los riesgos, la planificación de respuesta a los riesgos, el control y seguimiento de estos.

A partir de la información evaluada, se determinó que la JAFAP cuenta con una serie de controles orientados a minimizar el riesgo dentro de los cuales se mencionan la segregación de funciones, *check list*, controles de acceso, funciones de usuario, entre otros, sin embargo, estos no son parte de un marco integral de gestión de riesgos sino como parte de controles rutinarios de los procesos.

Esta situación repercute en la gestión y optimización de riesgos para mitigar amenazas que pueden afectar los objetivos organizacionales y, a su vez, afecta las metas de negocio relacionadas con TI, a saber:

- Cumplimiento y soporte de las TI al cumplimiento del negocio, de las leyes y regulaciones externas.
- Seguridad de la información, infraestructura de procesamiento y aplicaciones.
- Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.
- Cumplimiento de las políticas internas por parte de las TI.

Adicionalmente, la carencia de un marco de gestión de riesgos impacta en la supervisión, evaluación y valoración del sistema de Control Interno al ser un componente fundamental de este.

Gestión de la seguridad de la información

Con el fin de evaluar la implementación de una política de seguridad de la información y los procesos correspondientes, se presentan los resultados obtenidos por cada componente:

1. **Implementación de un marco de seguridad de la información**

La JAFAP mantiene una política aprobada la cual define los lineamientos y controles para un marco de seguridad de la información, sin embargo, no es de conocimiento de todo el personal.

Por otra parte, se cuenta con una política debidamente aprobada y divulgada que define las responsabilidades de los funcionarios, relacionadas con el marco de seguridad de la información y con un procedimiento que establece su revisión periódica.

2. **Compromiso del personal con la seguridad de la información**

La Organización tiene un plan global de seguridad de TI aprobado y divulgado en donde se define la implementación de políticas y procedimientos de seguridad de la información.

Además, se cuenta con un procedimiento para la vigilancia del cumplimiento de las responsabilidades de la seguridad de la información. Así mismo, se cuenta con acuerdos vigentes de confidencialidad para el manejo de documentación y rescisión de contratos.

3. **Seguridad física y ambiental**

De acuerdo con los resultados obtenidos, la JAFAP cuenta con una política aprobada y divulgada para la implementación de medidas de seguridad física, como, por ejemplo, zonas de seguridad, ubicación de equipos críticos, entre otros.

Adicionalmente, cuenta con una política en la que se establecen las responsabilidades sobre el monitoreo, los procedimientos de reporte y resolución de incidentes de seguridad física. Así mismo, con una bitácora para el control de ingreso y salida de activos de TI de la Organización.

4. **Seguridad en las operaciones y telecomunicaciones**

La JAFAP cuenta con medidas de prevención, detección y corrección a lo largo de toda la Organización para proteger los sistemas de información y la tecnología contra software malicioso.

5. **Control de acceso**

Mediante los resultados obtenidos, se determinó que la JAFAP cuenta con una política aprobada y divulgada la cual establece los procedimientos relacionados con el acceso a la información, al software de base y de aplicación, a las bases de datos, a las terminales y otros recursos de comunicación. A su vez, cuenta con una política aprobada y divulgada que defina la propiedad, custodia y responsabilidad sobre los recursos de TI. Sin embargo, dichas políticas no son de conocimiento general de los colaboradores de la Entidad.

No obstante, la Organización no cuenta con una política aprobada y divulgada que establezca controles de acceso para el manejo de información impresa, visible o almacenada en medios físicos.

6. **Seguridad en la implementación y mantenimiento de software de infraestructura tecnológica**

La JAFAP cuenta con una política aprobada y divulgada que define los requerimientos de seguridad sobre los ambientes de desarrollo, mantenimiento y producción, también cuenta con un procedimiento aprobado, divulgado en el cual es definido el acceso a los programas fuente y a los datos de prueba.

7. Continuidad de los servicios de TI

La Organización cuenta con un plan de continuidad de los servicios de TI aprobado, sin embargo, este no es de conocimiento de todos los colaboradores. Además, se documentan las acciones preventivas y correctivas para mantener una continuidad razonable de los procesos de la Organización.

Por otra parte, la JAFAP no realiza ni documenta pruebas para validar que el plan de continuidad de negocio vigente opere de manera satisfactoria. Tampoco se cuenta con un sitio alterno de operaciones fuera de las instalaciones de la Universidad de Costa Rica.

En el grado en que la JAFAP cumpla con cada uno de los componentes de la gestión de la seguridad de la información definidos en las Normas Técnicas puede alcanzar el logro de las metas relacionadas detalladas a continuación:

- Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas.
- Riesgos de negocio relacionados con las TI gestionados.
- Seguridad de la información, infraestructura de procesamiento y aplicaciones.
- Disponibilidad de información útil y relevante para la toma de decisiones.
- Entrega de servicios de TI de acuerdo con los requisitos del negocio

Gestión de Proyectos

La JAFAP no cuenta con una metodología de administración de proyectos aprobada de tal manera se logren sus objetivos, satisfaga los requerimientos y cumpla con los términos de calidad, tiempo y presupuesto óptimos preestablecidos.

Una apropiada gestión de proyectos permitiría a la JAFAP contar con un marco de gestión de identificación y construcción de soluciones y, a su vez, con una gestión de programas y proyectos lo que tiene impacto en el logro de las metas relacionadas de TI como:

- Alineamiento de TI y la estrategia de negocio sobre asuntos estratégicos de TI.
- Riesgos de negocio relacionados con las TI gestionados.
- Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.
- Entrega de servicios de TI de acuerdo con los requisitos del negocio.

Decisiones sobre asuntos estratégicos de TI

La Organización cuenta con un comité de tecnología que define las prioridades, asigna los recursos y atiende los requerimientos tecnológicos de la JAFAP lo cual permite mantener alineados las prioridades y proyectos de TI a la estrategia organizacional, para lograr una adecuada atención de los requerimientos y un equilibrio en la asignación de recursos. Sin embargo, la responsabilidad de este comité no es de conocimiento del personal.

Cumplimiento de obligaciones relacionadas con la gestión de TI

La Organización cuenta con un listado de marco jurídico que tiene incidencia sobre la gestión de TI con el fin de evitar incumplimientos legales y normativos que podrían ocasionar pérdidas económicas o sanciones legales a la JAFAP.

El tener identificado este marco jurídico permite a la Entidad asegurar el cumplimiento de leyes y regulaciones externas y mitigar el riesgo legal relacionados con la gestión de TI.

Capítulo IV. Propuesta de un modelo de Control Interno para la gestión del control de tecnologías de información en los procesos contables.

En el presente capítulo se realiza una propuesta de un modelo de Control Interno para el proceso contable de la JAFAP mediado por tecnologías de información, con base en un estudio de COBIT 5, la normativa vigente aplicada por la Contraloría General de la República y el análisis efectuado en el capítulo III.

4.1 Objetivo

Desarrollar una propuesta de Control Interno para la gestión del control de tecnologías de información en los procesos contables que contribuya a la administración con el cumplimiento de los objetivos de la Organización.

4.2. Justificación de la propuesta

La presente propuesta se basa en la necesidad de proporcionar a la JAFAP un modelo de Control Interno para la gestión de tecnologías de información en los procesos contables basado en las mejores prácticas aplicadas tanto a nivel nacional como internacional, lo cual le permitirá asegurar el cumplimiento de los objetivos de la Organización y consecuentemente una minimización de los riesgos asociados.

Por otra parte, según la revisión realizada en el capítulo III, se determinaron oportunidades de mejora en la Organización, las cuales contribuirán al fortalecimiento del sistema del Control Interno adaptado a las necesidades organizacionales.

Mediante la propuesta se pretende crear una guía que contribuya a la JAFAP al establecimiento de prácticas para la medición, evaluación y control de la gestión de los procesos contables relacionados con tecnología de información. de la gestión de los procesos contables relacionados con tecnología de información.

4.3. Bases normativas en que se fundamenta la propuesta

Las bases normativas en donde se fundamenta la propuesta son las Normas Técnicas para la gestión y control de las Tecnologías de Información de la Contraloría General de la República Capítulo I "Normas de Aplicación General" (N-2-2007-CO-DFOE), mediante un análisis de COBIT 5; en dichas normas se definen las diferentes características y aspectos a cumplir por las organizaciones para una adecuada gestión del Control Interno en los procesos relacionados con TI.

4.4. Metodología aplicada

Con base en los resultados obtenidos en las evaluaciones realizadas en el capítulo III se determinaron las áreas y oportunidades de mejora de la JAFAP respecto a las Normas Técnicas para la gestión y control de las Tecnologías de Información de la Contraloría General de la República Capítulo I "Normas de Aplicación General" (N-2-2007-CO-DFOE) y el COBIT 5, dado esto, se presenta la propuesta basada en las mejores prácticas nacionales e internacionales mediante herramientas para la gestión de los procesos contables gestionados mediante TI.

4.5. Propuesta de un modelo de Control Interno para el proceso contable mediado por tecnologías de información

Área: Marco Estratégico de TI

La Organización debe establecer un marco estratégico de TI mediante políticas, procedimientos, prácticas cotidianas promovidas, divulgadas a todos sus colaboradores y que sean aplicadas y comprendidas por estos.

APO01 - Gestionar el Marco de Gestión de TI

Para materializar la visión estratégica de TI a las operaciones de la Organización es necesario elaborar un plan que contemple los siguientes puntos:

APO01.01 Definir la estructura organizativa: Establecer una estructura en donde se refleje las necesidades del negocio, las prioridades de TI en el cual se defina el alcance, las funciones internas, externas, los papeles y capacidades de la estructura.

Establecer los requerimientos de las partes interesadas críticas para la toma de decisiones de TI y, a su vez, definir las reglas básicas de comunicación mediante la identificación de las

necesidades y establecer los planes basados en dichas necesidades.

Verificar periódicamente la adecuación y eficacia de la estructura organizativa con el fin de identificar posibles ajustes a la estrategia de TI.

APO01.02 Establecer funciones y responsabilidades: Determinar, comunicar funciones y responsabilidades del personal de TI y de partes interesadas con relación directa en las TI corporativas, delimitando dichas funciones y la rendición de cuentas.

Para la definición de funciones y responsabilidades se deben tomar en consideración los requisitos y giro de negocio de la Empresa, así mismo implementar prácticas de supervisión para evaluar el adecuado cumplimiento de dichas funciones y la entrega de resultados.

Establecer claramente la segregación de funciones con el objetivo de minimizar las posibilidades de que un solo papel pueda comprometer un proceso crítico.

APO01.03 Mantener los elementos catalizadores del sistema de gestión: Mantener los elementos catalizadores del sistema de gestión y del entorno de control de la TI de la Empresa, para finalmente garantizar que estén alineados con la filosofía, el estilo operativo de Gobierno y la gestión organizacional.

APO01.04 Comunicar los objetivos de la dirección de gestión: Comunicar constantemente los objetivos y dirección de TI, para garantizar que la información proporcionada a las partes interesadas sea clara y describa los objetivos, controles internos, políticas y procedimientos, responsabilidades, entre otros.

APO01.05 Optimizar la ubicación de la función de TI: Definir la ubicación de las funciones de TI en la Organización, así mismo, evaluar la estrategia empresarial y el modelo operativo de TI.

APO01.06 Definir la propiedad de la información (datos) y del sistema: Establecer políticas y procedimientos que aseguren la integridad y consistencia de la información.

Definir controles internos para garantizar la seguridad de los datos y crear un listado que detalle propietarios, custodios, clasificaciones y servicios subcontratados.

APO01.07 Gestionar la mejora continua de los procesos: Evaluar las oportunidades de mejora de cada proceso y aplicar controles que aseguren la continuidad. Así mismo, emplear los procedimientos establecidos en los manuales de la Entidad relacionados con la continuidad y

eliminar procesos desactualizados que no agregan valor.

APO01.08 Mantener el cumplimiento con las políticas y procedimientos: Garantizar el cumplimiento de políticas, procedimientos establecidos por la administración y evaluar periódicamente con el objetivo de adoptar medidas correctivas.

APO02 - Gestionar la Estrategia

La Entidad debe proporcionar una visión integral del negocio y del entorno de TI mediante una alineación de los planes estratégicos de TI con los objetivos de negocio, para considerar las siguientes actividades:

APO02.1 Comprender la dirección de la Empresa: Desarrollar y mantener conocimiento de las estrategias de la Organización y del entorno tanto interno como externo.

Identificar las partes interesadas de mayor trascendencia definir fuentes de posibles cambios en la Organización para desarrollar una estrategia basada en prioridades.

APO02.2 Evaluar el entorno, capacidades y rendimientos actuales: Desarrollar un marco de referencia (que incluya entorno de TI, servicios, capacidades, Gobierno de TI, entre otras), utilizado según las necesidades futuras y determinar los posibles riesgos de TI actuales y potenciales.

Definir problemas, fortalezas, oportunidades, amenazas del entorno actual y establecer áreas de mejora que contribuyan al objetivo del negocio.

APO02.3 Definir el objetivo de las capacidades de TI: Considerar la adopción de nuevas tecnologías e identificar el impacto de adquirirlas.

Establecer objetivos y metas de TI que agreguen valor a la Empresa y contribuyan a la gestión. Así mismo, definir las capacidades, servicios de TI, procesos, procedimientos, habilidades, competencias de TI, entre otras que permitan cubrir las necesidades y acercarse al tipo de negocio deseado.

APO02.4 Realizar un análisis de diferencias: Identificar las implicaciones tanto negativas como positivas y el impacto de aplicar cambios en la Empresa.

APO02.5 Definir un plan estratégico y la hoja de ruta: Identificar adecuadamente los

riesgos, costos y beneficios para obtener la Entidad integrando cambios como inversiones tecnológicas, variaciones normativas internas y externas, recurso humano, entre otras.

Crear presupuestos, establecer requerimientos de recursos y definir objetivos para cada una de las iniciativas presentadas por la Organización.

APO02.6 Comunicar la estrategia y la dirección de TI: Establecer un plan de comunicación que cubra las necesidades y se encuentre alineado con los objetivos de la Organización de manera eficiente y eficaz.

Obtener retroalimentación de las partes interesadas y los jerarcas.

Área: Gestión de la Calidad

La Entidad debe generar productos y servicios de TI que cumplan con los requerimientos de los usuarios, basados en un enfoque de eficiencia y mejora continua.

APO07 Gestionar los Recursos Humanos

Se debe proporcionar un enfoque estructurado orientado a garantizar las capacidades de gestión y habilidades de recurso humano para optimizar las capacidades de los colaboradores para el logro de los objetivos, con base en las siguientes actividades:

APO07.01 Mantener la dotación de personal suficiente y adecuado: Evaluar la necesidad de personal de manera constante y antes de aplicar cambios de relevancia en la Organización con el objetivo de validar que los recursos humanos sean suficientes y apoyar el logro de objetivos de TI.

Verificar que los procesos de contratación y retención de personal de TI se encuentren alineados con las políticas, los procedimientos de la Empresa y aplicar controles necesarios según las funciones del personal.

Establecer un entrenamiento cruzado para el personal de TI con el fin de asegurar que todas las funciones pueden ser ejecutadas por el personal y se reduzca la dependencia.

APO07.02 Identificar personal clave de TI: Para las funciones críticas la Organización debe documentar los datos, establecer un intercambio de información entre el personal, realizar un respaldo (*backup*) del personal a cargo y mantener entrenamientos cruzados para disminuir la

dependencia.

APO07.03 Mantener las habilidades y competencias del personal: Establecer las habilidades y competencias necesarias para el logro de los objetivos de la Entidad y la gestión de TI.

Evaluar las habilidades existentes tanto de recursos internos como externos y determinar si es necesario una contratación, redistribución y cambio de estrategias.

Dar acceso a información relevante que incremente las habilidades y conocimiento del personal y desarrollar capacitaciones.

Evaluar periódicamente (según la necesidad de la Entidad) las habilidades del personal para asegurarse que cumplan con los requisitos establecidos para el logro de objetivos y determinar si el personal a cargo posee la formación académica y experiencia para afrontar los cambios y el impacto de ciertas situaciones.

APO07.04 Evaluar el desempeño laboral de los empleados: Realizar evaluaciones de desempeño periódicamente (según la necesidad de la Entidad) y proporcionar retroalimentación oportuna sobre el cumplimiento adecuado de las metas individuales y globales. Así mismo, crear planes de mejora continúa basados en los resultados de la evaluación.

Desarrollar programas que premien el desempeño del personal y logro exitoso de objetivos mediante una aplicación coherente y en consistencia con el reglamento de la Organización.

APO07.05 Planificar y realizar un seguimiento del uso de recursos humanos de TI y del negocio: Mantener claridad de los recursos internos y externos necesarios para el logro de los objetivos de TI y ofrecer soluciones en caso de identificar debilidades y carencias en las operaciones diarias.

Establecer un calendario de actividades en donde se detalle el tiempo a dedicar a las actividades, trabajos, servicios y proyectos.

APO07.06 Gestionar el personal contratado: En caso de contratar consultores se debe establecer políticas que describen cuándo, cómo y qué tipo de trabajo se va a realizar. Obtener un contrato formal firmado por ambas partes en donde se especifiquen todos los términos, así mismo, realizar revisiones constantes para asegurarse que el trabajo realizado cumpla con las expectativas iniciales.

APO11 Gestionar la Calidad

Es necesario definir, comunicar los requisitos de calidad en los procesos, procedimientos y resultados de la JAFAP, incluyendo controles, monitoreo continuo y el uso de mejores prácticas y estándares reconocidos, para tomar en consideración las siguientes actividades:

APO11.01 Establecer un sistema de gestión de la calidad (SGC): Definir un marco de control y procesos de TI alineados con el enfoque y objetivos de la Organización, así mismo, identificar criterios de calidad (por ejemplo: requerimientos legales). Establecer funciones, tareas y responsabilidades dentro de la estructura organizativa.

Confeccionar planes de calidad específicos para trabajos, proyectos y objetivos de relevancia que se encuentren en concordancia con el sistema de calidad corporativo.

Recibir retroalimentación de las partes interesadas internas y externas para establecer criterios de calidad con base en las necesidades.

Supervisar periódicamente la eficiencia, la eficacia de los procesos de calidad aplicados y su cumplimiento, además verificar la aceptación por parte de la Organización.

APO11.02 Definir, gestionar los estándares, procesos y prácticas de calidad: Establecer procedimientos y políticas de calidad alineados con los requerimientos del marco de control de TI y tomar como referencia las mejores prácticas de la industria.

APO11.03 Enfocar la gestión de la calidad en los clientes: Establecer la gestión de la calidad con base en los requerimientos de los clientes asegurándose que se encuentren alineados a los objetivos de TI. Así mismo, comunicar los requisitos y expectativas de los clientes.

Obtener la opinión de los clientes sobre la gestión de la Empresa con el objetivo de mejorar la calidad en los procesos y servicios.

Establecer oportunidades de mejora para garantizar que las exigencias de los clientes puedan ser cumplidas.

Verificar regularmente que el sistema de gestión de calidad está de acuerdo con los requisitos mínimos de cumplimiento y tomar en consideración los comentarios de los clientes, usuarios y la dirección.

APO11.04 Supervisar y hacer controles, junto con revisiones de calidad: Establecer

revisiones de calidad periódicamente, informar los resultados y aplicar las medidas correctivas necesarias.

Supervisar la calidad de los procesos, servicios de la Organización y garantizar que se encuentren alineados con los objetivos de TI.

APO11.05 Integrar la gestión de la calidad en la implementación de soluciones y entrega de servicios: Incorporar la gestión de la calidad en el desarrollo de soluciones y la prestación de servicios. Identificar inconformidades y aplicar las correcciones oportunamente.

APO11.06 Mantener una mejora continua: Comunicar regularmente la necesidad y beneficios de la mejora continua y compartir las mejores prácticas con el fin de obtener conocimiento a partir de información relevante.

Detectar deficiencias, problemas recurrentes de calidad, determinar las causas, el impacto y establecer medidas correctivas y de mejora continua.

Proporcionar al recurso humano la formación necesaria y las herramientas de mejora continua, y a su vez, recurrir a información histórica, normas y datos similares que ayuden al logro de objetivos.

DSS06 - Gestionar los controles de los procesos del negocio

Mantener una adecuada gestión de los controles en los procesos es fundamental para cumplir con los objetivos corporativos, para esto se deben alinear las actividades de control con dichos objetivos. Con el fin de gestionar los controles de los procesos del negocio la administración debe realizar las siguientes actividades:

DSS06.01 Alinear actividades de control embebidas en los procesos de negocio con los objetivos corporativos: Contar con requerimientos de control establecidos para el logro de los objetivos de negocio, identificar y documentar todas las actividades de control de los procedimientos clave para el cumplimiento de dichos requerimientos.

Tomando como base el riesgo inherente del negocio, se deben priorizar las actividades de control e identificar los controles clave, dichas actividades serán supervisadas continuamente con el objetivo de identificar y efectuar las oportunidades de mejora continua en el diseño y ejecución de los controles de los procesos de negocio.

DSS06.02 Controlar el procesamiento de la información: Crear las transacciones de sus labores diarias según los papeles y los procedimientos establecidos considerando la segregación de funciones en cuanto a registro, revisión y aprobación (dicha información deberá encontrarse en cada una de las transacciones realizadas con el fin de verificar si los colaboradores cuentan con los permisos correspondientes).

Verificar la precisión, completitud y validez de las transacciones.as. En caso de que se deban realizar correcciones, la transacción se devolverá lo más cerca posible del punto de origen para cumplir con la integridad y validez de la información, las transacciones devueltas no deben comprometer el proceso de las válidas. En caso de presentarse fallos en los procesos de las transacciones, se debe verificar la integridad de los datos posterior a la resolución de los incidentes.

Toda salida de datos debe ser precisa, completa y aprobada por quien corresponda, el informe obtenido como resultado de la salida de los datos se envía solamente al usuario final

DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización: Cada colaborador debe tener asignados los roles y responsabilidades de su cargo, la administración otorgará los niveles de autoridad para el registro, revisión y aprobación de transacciones.

En el sistema SIBU se deben establecer los derechos de acceso a los usuarios según las responsabilidades a cargo, en caso de cambio de roles de los usuarios o cuando algún colaborador deja el área para la cual laboraba se le deben eliminar los derechos de acceso. Realizar revisiones periódicas para verificar si los accesos otorgados son válidos, pertenecen a colaboradores actuales y están alineados a sus responsabilidades, con el objetivo de mitigar posibles amenazas y riesgos y con esto, cumplir con los objetivos del negocio. Para transacciones sensibles es necesario una adecuada segregación de funciones.

Recibir capacitación constante referente a los roles y responsabilidades atinentes a cada cargo, con el fin de transmitir a los colaboradores sus responsabilidades, los controles que deben cumplir, así como la integridad, privacidad y confidencialidad de la información de la JAFAP.

DSS06.04 Gestionar errores y excepciones: Establecer procedimientos para corregir y reemplazar errores de las transacciones los cuales junto con las excepciones y desviaciones deben ser revisados. Dar seguimiento oportuno a los errores presentados, corregirlos y aprobar las transacciones modificadas, toda corrección realizada debe dejar evidencia.

En los casos donde se presenten errores en transacciones que son relevantes, se deben informar de manera oportuna con el fin de identificar las causas generadoras y ejecutar los análisis de las tendencias.

DSS06.05 Asegurar la trazabilidad de los eventos y responsabilidades y de información: Toda transacción debe contener como respaldo la documentación que la origina, así como el nombre de la persona encargada de realizar el registro de la transacción y los colaboradores a cargo de la revisión y aprobación, esto para garantizar la confiabilidad de la información y el debido procesamiento acorde con los objetivos corporativos definidos.

DSS06.06 Asegurar los activos de información: Aplicar políticas de clasificación de datos y procedimientos para la protección de los activos de información. Según la clasificación definida se procederá con la restricción para el uso, distribución y acceso físico a la información, para velar por su cumplimiento se deben crear y ejecutar procedimientos, herramientas y técnicas necesarias donde cualquier violación debe ser informada a la administración e interesados.

MEA02- Supervisar, Evaluar y Valorar el Sistema de Control Interno

La Entidad debe ofrecer transparencia a las partes interesadas respecto al funcionamiento del Control Interno y su capacidad para generar confianza en las operaciones, en el logro de los objetivos organizacionales y un entendimiento de los riesgos mediante las siguientes actividades:

MEA02.01 Supervisar el Control Interno: Realizar de forma continua la supervisión y mejora del entorno de Control Interno y su marco normativo con el fin de cumplir los objetivos organizacionales.

Considerar las evaluaciones internas y externas del sistema de Control Interno mediante auditorías.

Mantener actualizado el sistema de Control Interno, considerando los cambios en el entorno de la Organización, los procesos de negocio y los riesgos asociados.

MEA02.02 Revisar la efectividad de los controles sobre los procesos de negocio: Revisar la operación de los controles, en donde se incluya la revisión de la evidencia de supervisión y pruebas para asegurar la efectividad de los controles.

Definir los controles claves para el negocio y desarrollar una estrategia adecuada para su validación.

Identificar la información clave para identificar que los controles están operando de manera efectiva y resguardar la evidencia correspondiente.

MEA02.03 Realizar autoevaluaciones de control: Establecer programas continuos de autoevaluación con el fin de valorar la efectividad de las políticas, normas y procedimientos de control vigentes en la Organización.

Establecer planes de mejora al sistema de Control Interno basados en los resultados obtenidos en la autoevaluación.

Evaluar los resultados contra los buenos estándares y prácticas de la industria.

MEA02.04 Identificar y comunicar las deficiencias de control: Identificar las deficiencias de control y analizar e identificar las causas que las generan.

Comunicar los procedimientos implementados para identificar las deficiencias en el Control Interno a las partes interesadas y propietarios de las áreas afectadas.

Implementar acciones correctivas según las deficiencias identificadas.

MEA02.05 Garantizar que los proveedores de aseguramiento son independientes y están cualificados: Asegurar que las entidades quienes realizan el aseguramiento del Sistema de Control Interno sean independientes a la Organización.

Establecer procedimientos para la calificación de los proveedores externos de aseguramiento de calidad y Control Interno, dentro de los cuales se incluyan aspectos éticos.

MEA02.06 Planificar iniciativa de aseguramiento: Definir los usuarios finales responsables de recibir los informes de los procesos de aseguramiento de la Entidad, basado en los objetivos empresariales, prioridades estratégicas y riesgos.

MEA02.07 Estudiar las iniciativas de aseguramiento: Definir el alcance de las actividades de aseguramiento realizadas por la Entidad, mediante la identificación de los objetivos empresariales, la valoración de riesgos y los recursos disponibles.

Definir las prácticas de recolección y evaluación de la información de los diferentes procesos con el fin de identificar los controles sujetos a procesos de revisión.

MEA02.08 Ejecutar las iniciativas de aseguramiento: Supervisar las actividades de aseguramiento verificando que las labores se realizan según lo planificado, cumpliendo con los objetivos y estándares definidos.

Realizar pruebas de la efectividad de los objetivos del sistema de control, documentando los resultados obtenidos.

Proveer a la Alta Dirección un informe detallado de los resultados obtenidos, incluso las fortalezas y debilidades encontradas, así como las recomendaciones necesarias para el fortalecimiento de los sistemas de gestión de la Entidad.

Área: Gestión de Riesgos

La Organización debe responder adecuadamente a las amenazas que puedan afectar la gestión de las TI, mediante un proceso de gestión continua de riesgos integrado a la gestión institucional basado en las políticas y bases de conocimiento de la Organización.

EDM03 - Asegurar la Optimización del Riesgos

La administración debe asegurar que los riesgos relacionados con TI no excedan el nivel de tolerancia y el impacto de estos no comprometa la gestión, por lo cual se debe conocer, atender, comunicar y dar seguimiento. Tomando en consideración los siguientes aspectos:

EDM03.01 Evaluar la gestión de riesgos: Establecer el nivel de riesgo relacionado con TI que la administración está dispuesta asumir para el logro de sus objetivos, mediante la elaboración de una propuesta donde se indique claramente los niveles de aceptación del riesgo, factores a considerar relacionados al riesgo antes de tomar decisiones estratégicas y como la Empresa podría solventar situaciones de riesgos durante su operación.

EDM03.02 Orientar la gestión de riesgos: Promover una cultura consciente de los riesgos que involucra el uso de TI en la toma decisiones de la Organización, a través de la comunicación de las propuestas, planes y mecanismos confeccionados por la administración para responder rápidamente ante el riesgo.

EDM03.03 Supervisar la gestión de riesgos: Supervisar que el riesgo presente en la toma

de decisiones se encuentre dentro del nivel aceptable definido por la administración, evaluar el origen de las desviaciones respecto al plan inicial y aplicar las medidas correctivas según el plan creado por la Organización, así mismo, mantener informados a los niveles jerárquicos encargados sobre los problemas que se podrían presentar.

APO12 - Gestionar el Riesgo

Definir, evaluar, supervisar y disminuir los riesgos relacionados con TI, tomando como base los niveles establecidos por la administración. Mediante la aplicación de las siguientes actividades:

APO12.1 Recopilar datos: Identificar los riesgos tanto internos como externos que comprometen el logro de objetivos mediante una metodología para obtener información relevante. Es importante tomar como referencia información histórica relacionada al riesgo y factores que contribuyeron y afectaron de manera significativa la gestión, además analizar, periódicamente, situaciones nuevas y emergentes relacionadas al riesgo de TI.

APO12.2 Analizar el riesgo: Establecer un nivel tolerable de riesgo y determinar las respuestas mediante requerimientos, controles para reducir, mitigar y comunicar estos riesgos, así mismo, definir los coste- beneficio asociados.

Validar los resultados de los análisis realizados antes de aplicarlos a la toma de decisiones para disminuir de manera fiable el riesgo.

APO12.3 Mantener un perfil de riesgo: Contar con conocimiento claro de cada uno de los procesos que componen la gestión, con el objetivo de determinar el riesgo asociado a cada proceso, el nivel de aceptable y la respuesta para mitigar los impactos.

APO12.4 Expresar el riesgo: Informar a todos los niveles jerárquicos interesados sobre los resultados de los análisis e incluir una estimación de las posibles pérdidas y ganancias, implicaciones legales, regulaciones y otras que ayuden a la toma de decisiones.

Examinar la efectividad de los controles aplicados, tomar en consideración evaluaciones realizadas por auditoría interna, cualquier revisión relacionada al impacto del riesgo y la posibilidad

de incrementar o disminuir la tolerancia al riesgo.

APO12.5 Definir un portafolio de acciones para la gestión de riesgos: Aplicar controles relacionados al riesgo que se encuentren alineados al nivel de riesgo aceptado y conforme con lo definido en las propuestas elaboradas por la administración para cada proceso.

APO12.6 Responder al riesgo: Categorizar los riesgos y su nivel de impacto con el fin de realizar la comparación con el nivel de tolerancia al riesgo determinada por la administración y aplicar el plan de respuesta que permita minimizar los efectos. Es importante comunicar resultados y eventos pasados relacionados al riesgo con el objetivo de mejorar las acciones a futuro.

Área: Gestión de la seguridad de la información

Garantizar la integridad y disponibilidad de la información con el objetivo de que la misma se encuentre protegida contra uso, modificación no autorizada, divulgación, daño o pérdida.

Para una adecuada gestión de la seguridad de la información es necesario determinar, documentar e implementar una política y los procedimientos necesarios, así como designar los recursos idóneos para alcanzar los niveles de seguridad adecuados.

APO13 - Gestionar la seguridad

La JAFAP debe definir, operar y supervisar un sistema de gestión de seguridad de la información (SGSI) que permita mantener el impacto y ocurrencia de los incidentes de seguridad de la información dentro de los niveles de apetito de riesgo definidos por la Entidad. La administración podría aplicar las siguientes actividades:

APO13.01 Establecer y mantener un SGSI: Establecer el alcance y los límites del sistema de gestión de seguridad de la información, para esto es necesario que la administración contemple las características de la JAFAP, su localización y activos.

El SGSI debe definirse de acuerdo con la política de la Empresa y alineado a su enfoque global de la gestión de la seguridad. Una vez el SGSI haya sido aprobado por la dirección, se procede a definir y comunicar los roles y responsabilidades para finalmente comunicar el enfoque del sistema.

APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la

información: Definir y mantener un plan de tratamiento de riesgos de seguridad de la información que se encuentre alineado con los objetivos estratégicos de la Empresa para lo cual se incluirán las prácticas de gestión, soluciones de seguridad adecuadas, así como las prioridades y responsabilidades para gestionar los riesgos identificados.

Desarrollar propuestas para implementar el plan de tratamiento de riesgos definido. A su vez, la administración definirá la forma de medición de la efectividad de dichas prácticas para posteriormente integrar la planificación, el diseño, la puesta en marcha y supervisión de los procedimientos de seguridad de la información, también es fundamental considerar los controles establecidos para la prevención y detección de incidentes.

APO13.03 Supervisar y revisar el SGSI: Someter el SGSI a revisiones periódicas mediante auditorías internas y revisiones realizadas por la Dirección, con el fin de identificar si el alcance del sistema continúa siendo el adecuado y cuáles mejoras se pueden implementar en el proceso del SGSI para que la efectividad y el desempeño sea el planificado.

DSS01 - Gestionar operaciones

Para realizar una adecuada gestión de operaciones, es necesario establecer y ejecutar actividades y procedimientos operativos fundamentales para que la Empresa entregue servicios de TI adecuados, asimismo, se deben realizar actividades de monitoreo para cumplir con lo planificado. Para gestionar las operaciones es necesario realizar las siguientes actividades:

DSS01.01 Ejecutar procedimientos operativos: Desarrollar procedimientos y actividades operativas confiables, las cuales deben ser programadas y realizadas de forma constante, por lo cual es importante el cumplimiento de los estándares de seguridad alineados con la política de seguridad, objetivos y requerimientos regulatorios empresariales en los procesos de recepción, procesamiento, almacenamiento y salida de datos.

Verificar que los datos esperados sean recibidos y procesados de forma completa, precisa y oportuna esto para poder entregar a los usuarios finales los resultados acordes con los requisitos de la JAFAP.

Realizar la programación para el registro de copias de respaldo para cumplir con las políticas y procedimientos definidos.

DSS01.02 Gestionar servicios externalizados de TI: Los procesos de información deben estar alineados con los requerimientos de seguridad de la JAFAP conforme con los contratos firmados con proveedores externos de servicios de TI. Así mismo, las prioridades en la entrega de servicios, los requerimientos operativos y de procesamiento de TI también deben estar acorde con los contratos mencionados anteriormente.

Los procesos críticos de gestión interna de TI se deben integrar con los procesos de los proveedores de servicios externos. Para corroborar que los requerimientos acordados en los contratos con proveedores externos están siendo tratados de forma oportuna y adecuada, se debe realizar la planeación y ejecución de auditorías de los entornos en los donde operan dichos proveedores.

DSS01.03 Supervisar la infraestructura de TI: Identificar y registrar todos los eventos relacionados con la infraestructura de TI, al considerar el riesgo presentado.

Realizar y mantener actualizada una lista de activos de infraestructura que requieren de monitoreo constante, los mismos se ordenarán acorde al grado crítico de los servicios dependientes de estos.

Definir y ejecutar reglas de identificación, registro de eventos falsos, menores y significativos para encontrar un equilibrio en su generación, dichos registros podrán ser retenidos por un período determinado para futuras investigaciones. A su vez, se deberán crear procedimientos para las revisiones periódicas, así como para la supervisión de dichos registros.

DSS01.04 Gestionar el entorno: El área de las instalaciones de TI pueden verse afectadas por desastres naturales o incidentes causados por el ser humano, estos deben ser identificados para posteriormente evaluar el efecto que podrían ocasionar en dichas instalaciones.

Todo el equipo de TI (incluyendo equipo móvil y el que se encuentra fuera de las instalaciones) debe estar protegido contra posibles afectaciones originadas por amenazas del entorno. La administración deberá contar con políticas relacionadas con la prohibición de fumar, beber, comer y utilizar suministros de oficina los cuales ocasionan incendios en las áreas de TI que se definan como sensibles.

Las instalaciones de TI deben estar construidas en entornos para mitigar la susceptibilidad

ante amenazas, es importante realizar revisiones periódicas para la supervisión y mantenimiento de los dispositivos de detección de amenazas del entorno.

Documentar y probar los procedimientos establecidos para activación de alarmas a causa de incidentes, los mismos deberán incluir la priorización de alarmas y el contacto determinado para dar aviso de la emergencia a las entidades locales, todo el personal deberá ser entrenado para estar preparado ante cualquier eventualidad.

Comparar los requerimientos de las pólizas de seguros con las medidas y planes de contingencia y posteriormente comunicar los resultados para la resolución de inconformidades de manera oportuna. Todos los sitios de TI deben ser diseñados y construidos considerando los riesgos del entorno, esto para mitigar el impacto de los incidentes que se presenten, ejemplo de esto son las celdas a prueba de incendio ubicadas en los servidores.

Por último, las áreas de TI y las zonas donde se encuentren los servidores deben mantenerse limpias y en condiciones seguras para evitar incidentes.

DSS01.05 Gestionar las instalaciones: Ante fluctuaciones y corte de energía eléctrica es necesario el análisis de los requerimientos de las instalaciones de TI y contar con el equipo adecuado de alimentación eléctrica ininterrumpida con el objetivo de dar soporte al plan de continuidad.

El sistema de alimentación ininterrumpida (SAI) debe ser probado periódicamente para asegurar la transmisión de electricidad al sistema sin afectar significativamente las operaciones del negocio.

El sitio alterno de TI debe tener un cableado bajo tierra o con una adecuada protección alternativa y debe estar contenido en conductos asegurados. Los armarios de cableado deben ser de acceso restringido y solamente puede ingresar personal autorizado. Todo el cableado y el *patching* físico (datos y telefonía) deben estar adecuadamente estructurados y organizados, de forma tal que dichas estructuras de cableado y conductos deberán estar documentados.

Todos los sitios e instalaciones de TI deben cumplir de manera estricta con las regulaciones y directrices establecidas para la salud y seguridad en el trabajo, las mismas deben ser estipuladas en informes divulgados a todos los colaboradores. El personal deberá ser capacitado continuamente para conocer las acciones apropiadas a realizar ante situaciones de incendio o incidentes similares.

El personal autorizado debe realizar el mantenimiento de los sitios y equipos de TI acorde con lo recomendado por el proveedor. Por último, es importante realizar análisis constantes de las alteraciones físicas en los sitios o localizaciones de TI con el objetivo de reevaluar el riesgo del entorno, los resultados de los análisis efectuados deben ser comunicados a la directiva de continuidad del negocio y gestión de edificios.

DSS05 - Gestionar servicios de seguridad

Para mitigar el impacto ocasionado por las deficiencias e incidentes de seguridad en la información es importante una adecuada y oportuna gestión de los servicios y con esto proteger la información sensible de la JAFAP y mantener aceptable el nivel de riesgo relacionado, de acuerdo con la política de seguridad definida. Para gestionar la seguridad de la información es necesario que la administración defina y conserve los roles de seguridad y los privilegios de acceso a la información otorgados, también se deben realizar revisiones y supervisiones constantes de la seguridad de la información, lo anterior se detalla a continuación:

DSS05.01 Proteger contra *software* malicioso (*malware*): Creación e implementación de procedimientos y responsabilidades para prevenir, detectar y corregir el software malicioso. Todas las instalaciones deben tener instaladas y activadas las herramientas de protección contra software malicioso.

Periódicamente se deben realizar revisiones y evaluaciones de posibles nuevas amenazas, así mismo, todo el personal debe recibir capacitaciones constantes sobre *software* malicioso, por ejemplo, uso de correo electrónico, descargas, uso de internet e instalaciones de software.

DSS05.02 Gestionar la seguridad de la red y las conexiones: Ejecutar procedimientos de gestión y medidas de seguridad para el uso de la red y conexiones de internet alineadas con el análisis de riesgos de la Organización y los requerimientos del negocio.

Solamente dispositivos autorizados podrán tener acceso a la información y red de internet de la JAFAP. Es importante que el Departamento de TI realice procedimientos de filtrado de red con el objetivo de mantener un adecuado control del tráfico entrante y saliente, ejemplo de esto es la implementación de mecanismos como los cortafuegos y *software* de detección de intrusiones.

La información en tránsito debe ser cifrada según su clasificación. Para las conexiones de red es fundamental la aplicación de los protocolos de seguridad aprobados y se configuren de forma segura los equipamientos de red.

Realizar frecuentemente pruebas de intrusión y de seguridad del sistema para verificar el adecuado funcionamiento de la protección de la red y del sistema.

DSS05.03 Gestionar la seguridad de los puestos de usuario final: Asegurar los puestos de usuario final para lograr que la información procesada, almacenada y transmitida se encuentre resguardada, para esto lo primero es configurar de forma segura los sistemas operativos, implementar el bloqueo a los dispositivos e incluir cifrado a la información.

Gestionar de forma adecuada y segura el acceso y control remoto mediante la configuración de la red y una correcta ejecución del filtrado de tráfico de la red en los dispositivos. Es importante proteger la integridad del sistema, así como la protección física a los dispositivos de usuario final.

DSS05.04 Gestionar la identidad del usuario y el acceso lógico: Asegurar que los derechos de acceso a la información de todos los usuarios sean acordes con los permisos otorgados, esto según las funciones y responsabilidades del cargo.

Coordinar con las unidades de negocio para asegurar que los roles de los usuarios se encuentren definidos y alineados con los accesos a la diferente información. Las aplicaciones deben contar con autenticador para su acceso esto según su clasificación de seguridad, garantizando una adecuada administración de los controles de autenticación.

Realizar revisiones periódicas de todas las cuentas de usuario y de los privilegios otorgados para detectar, prevenir y corregir errores. Todos los usuarios, tanto internos, externos y temporales, y las actividades de proceso de información a realizar deben ser identificables.

DSS05.05 Gestionar el acceso físico a los activos de TI: Definir e implementar los procedimientos para otorgar, limitar y eliminar el acceso físico a los activos de TI de la JAFAP (locales, edificio y áreas), para esto es necesario que la dirección de TI complete, autorice y guarde las peticiones formales de acceso físico a las diferentes instalaciones de TI debidamente aprobadas tomando como fundamento las funciones y responsabilidades del solicitante, dichos formularios deben indicar claramente los activos físicos a los cuales puede acceder cada colaborador, cliente, visitante y terceras personas.

Asegurar que todos los perfiles de acceso a las instalaciones físicas se encuentren actualizados. Cada uno de los puntos de entrada a las ubicaciones de TI deben ser supervisados y registrar todos los visitantes, para esto es importante instruir a todo el personal a mantener visible su tarjeta o placa de identificación y para los visitantes será necesario el acompañamiento por parte del personal de seguridad mientras se encuentren dentro de las instalaciones.

Verificar que el acceso a las ubicaciones de TI definidas como sensibles se encuentre restringido mediante placas o tarjetas de llave, vallas, muros y dispositivos de seguridad en puertas inferiores y exteriores, además de contar con alarmas para la identificación de cualquier acceso no autorizado.

DSS05.06 Gestionar documentos sensibles y dispositivos de salida: Establecer medidas de seguridad para la recepción, utilización, eliminación y destrucción de activos de TI sensibles como lo son formularios especiales mediante el uso de dispositivos de salida (por ejemplo, trituradores, papeles y más), para esto primeramente deben asignar los privilegios de acceso, posteriormente se debe realizar un inventario de documentos sensibles y dispositivos de salida que debe ser conciliado regularmente y finalmente se deben definir las medidas físicas de salvaguardia.

DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad: Las herramientas de monitoreo de la seguridad de la infraestructura deben estar programadas para registrar todos los eventos relacionados a la seguridad que han sido reportados, dichos registros deben ser guardados por un tiempo adecuado y apropiado para ser soporte de futuras investigaciones.

Todos los incidentes importantes relacionados con seguridad deben ser definidos y se deberá dejar registro de sus características y naturaleza para que los mismos y sus impactos sean reconocidos de forma fácil para darles una respuesta adecuada. Es importante realizar revisiones periódicas para detectar incidentes potenciales.

Todos los colaboradores deben conocer los requerimientos solicitados por el departamento de TI para recopilar la evidencia de los incidentes que se les presentan para los cuales deben crear de forma oportuna la solicitud correspondiente. Cuando en el proceso de monitoreo se identifiquen incidentes de seguridad potenciales es importante crear inmediatamente las solicitudes de incidentes para atenderlos y guardar el soporte.

Subárea: Gestión de la seguridad de la Información - Continuidad de los servicios de TI

La administración debe realizar una adecuada gestión de la seguridad de la información y de la continuidad del negocio para lograr sus objetivos empresariales. En incidentes de servicios, es necesario que la Organización realice procedimientos oportunos y efectivos para la adecuada recuperación de los servicios normales y con esto alcanzar la continuidad del negocio.

DSS02 - Gestionar Peticiones e Incidentes de Servicio

Mediante una adecuada, oportuna, rápida respuesta y solución de los incidentes reportados por los usuarios, así como de las consultas realizadas por estos, es posible mitigar las interrupciones y de esta forma lograr una mayor productividad. Para gestionar las peticiones e incidentes de servicio es necesario realizar las siguientes actividades:

DSS02.01 Definir esquemas de clasificación de incidentes y peticiones de servicio: Establecer esquemas en los cuales se realice la clasificación de las peticiones e incidentes de los servicios de los usuarios, así mismo, se debe realizar una priorización de estos y definir los criterios para su registro con el fin de dar un tratamiento adecuado.

Es importante determinarlos modelos de incidentes recurrentes y peticiones de servicio para dar una solución rápida, efectiva a los usuarios y con esto lograr la continuidad del negocio. Para incidentes importantes y de seguridad, es fundamental definir los procedimientos para escalar los incidentes y las reglas por cumplir.

DSS02.02 Registrar, clasificar y priorizar peticiones e incidentes: Los incidentes y las peticiones de servicio se deben registrar por completo incluyendo toda la información importante para realizar la clasificación de estos según el tipo y la categoría y darle prioridad a los clasificados como urgentes y a los que impacten de manera significativa el negocio, esto según los acuerdos de servicios de la Empresa.

DSS02.03 Verificar, aprobar y resolver peticiones de servicio: En casos en los que para resolver peticiones de usuarios se deban realizar cambios estándar acordados es necesario solicitar las aprobaciones y firmas correspondientes para su realización.

DSS02.04 Investigar, diagnosticar y localizar incidentes: Identificar y definir las causas de los incidentes con el fin de establecer las soluciones temporales y permanentes. Cuando se presente un incidente se debe registrar si el mismo cumple los criterios definidos por la administración para su correspondiente registro, para problemas complejos es necesario transferirlos a los expertos y

se gestione adecuadamente.

DSS02.05 Resolver y recuperarse ante incidentes: para resolver los incidentes se deben aplicar las soluciones temporales (deben quedar registradas) o permanentes adecuadas y en caso de requerir se deben aplicar acciones de recuperación del incidente. Es importante que todas las soluciones de incidentes queden documentadas y analizar si las mismas pueden ser utilizadas para la resolución de futuros problemas.

DSS02.06 Cerrar peticiones de servicio e incidentes: Junto con los usuarios que reportaron, se debe verificar que el incidente o la petición del servicio haya sido resuelta satisfactoriamente para cerrar los casos.

DSS02.07 Seguir el estado y emitir informes: Dar seguimiento al escalado de los incidentes y a los procedimientos ejecutados para darles solución. También, es fundamental que se entreguen informes a las partes interesadas.

Las peticiones de servicio y los incidentes presentados deben ser clasificados por categoría y tipo con el objetivo de identificar las causas de la frecuencia de estos y las infracciones cometidas por los usuarios de los servicios, la información resultante de los análisis realizados se debe utilizar en el plan de mejora continua de la JAFAP.

DSS04 - Gestionar la Continuidad

Ante un evento de interrupción significativa de servicios es importante poder continuar realizando las operaciones críticas fundamentales para el negocio y mantener disponible la información. Para gestionar la continuidad es necesario que se cumplan las siguientes actividades:

DSS04.01 Definir la política de continuidad de negocio, objetivos y alcance: Identificar los procesos de negocio tanto internos como externos (subcontratados) y las operaciones necesarias para cumplir con obligaciones legales y contractuales.

Identificar las partes interesadas clave en el proceso, así como sus roles y responsabilidades con el objetivo de acordar la política de continuidad y su alcance. Los procesos de soporte que son fundamentales y los servicios de TI relacionados deben ser identificados.

DSS04.02 Mantener una estrategia de continuidad: Identificar posibles causas de incidentes

importantes para evaluar el impacto ocasionado en el negocio la interrupción de los procesos críticos de la JAFAP, con el objetivo de establecer la cantidad de tiempo necesario para recuperar el proceso.

Analizar la probabilidad de amenazas que generan pérdida en la continuidad del negocio, con el objetivo de identificar las medidas para prevenir dichos incidentes y que en caso de ocurrir se logre disminuir su impacto.

El departamento de TI debe realizar el análisis de los requerimientos de continuidad del negocio para reconocer las estrategias. Es importante determinar las personas responsables de tomar decisiones clave para la aplicación de los planes de continuidad. Cada opción técnica estratégica conlleva recursos y costos identificados para generar recomendaciones de mejoramiento y finalmente, los ejecutivos de negocio deben aprobar las opciones técnicas viables y efectivas desde la perspectiva de coste, aseguramiento de la recuperación y continuidad de la JAFAP ante un incidente o desastre.

DSS04.03 Desarrollar e implementar una respuesta a continuidad del negocio: Realizar y mantener los planes de continuidad del negocio operativos (BCP) mediante los cuales se establezcan los procedimientos que permitan la continuidad de los procesos críticos del negocio, también se deben incluir enlaces a los planes de continuidad de proveedor de servicios externos a la JAFAP.

Los planes de continuidad deben contener las condiciones y los procedimientos para la recuperación de los procesos de negocio, así como la actualización y conciliación de bases de datos para salvaguardar la integridad de la información.

Establecer y documentar todos los recursos (personas, instalaciones e infraestructura) clave para realizar los procedimientos de continuidad y recuperación de los procesos de negocio, así como los requerimientos de información de respaldo de los planes (planes y documentos físicos, ficheros de datos, y otros).

Establecer y definir las habilidades necesarias para que los colaboradores realicen la ejecución de los planes de continuidad y sus procedimientos. Los planes y la documentación soporte será distribuida entre todos los interesados y autorizados, los mismos deben estar al alcance de todos.

DSS04.04 Ejercitar, probar y revisar el BCP: El plan de continuidad de negocio (BCP) debe ser efectivo y capaz de afrontar los riesgos del negocio, para verificar que el plan es completo es necesario establecer los objetivos para ejercer y probar los sistemas del plan (de negocio, administrativos, operacionales, logísticos, procedimentales y técnicos).

Establecer con las partes interesadas los ejercicios y pruebas del plan de continuidad (se deben planificar de acuerdo con lo establecido en el plan de continuidad), para su realización es necesario asignar los roles y responsabilidades. Una vez finalizados los ejercicios y las actividades de las pruebas, se debe realizar un análisis de los resultados de la revisión con el fin de generar recomendaciones para mejorar el plan de continuidad vigente.

DSS04.05 Revisar, mantener y mejorar el plan de continuidad: El plan y la capacidad de continuidad debe ser revisado periódicamente, considerando los objetivos de negocio estratégicos y operativos esto para determinar que continúe siendo idóneo, adecuado y efectivo.

Si se presentan cambios en el plan de continuidad, se debe considerar la necesidad de realizar una revisión del análisis de impacto en el negocio. Los cambios en procedimientos, planes, infraestructura, responsabilidades y funciones deben ser recomendados y comunicados a la dirección quien los aprueba y realiza mediante el proceso de gestión de cambios.

El plan de continuidad se revisa periódicamente con el objetivo de evaluar el impacto de nuevos o mayores cambios en la Organización de la Empresa, sistemas operativos, tecnologías, procesos de negocio, sistemas de aplicaciones, infraestructura y acuerdos de externalización.

DSS04.06 Proporcionar información en el plan de continuidad: Realizar regularmente planes de formación en donde se explique a detalle los procedimientos, roles y responsabilidades de los colaboradores encargados de realizar el plan de continuidad, evaluaciones de riesgos, análisis de impacto, comunicación con los medios y respuestas a incidentes o desastres. Según los resultados de los ejercicios y las pruebas se deben supervisar las habilidades y las competencias de los colaboradores.

DSS04.07 Proporcionar acuerdos de respaldo: Es esencial para la JAFAP contar con respaldos de seguridad de datos, sistemas, aplicaciones y documentación, esto acorde a la planificación definida. Mantener respaldos adecuados o asegurar que se encuentran resguardadas de otra forma las aplicaciones, sistemas, documentación, datos mantenidos o procesados por terceras partes.

Establecer los requerimientos para el almacenamiento de las copias de seguridad las cuales deben cumplir con los requisitos de negocio y tomar en consideración el acceso requerido a dichas copias de seguridad.

Es importante que el departamento de TI concientice a todos los colaboradores y les otorgue las capacitaciones necesarias en Planes de Continuidad de Negocio (BCP). Todas las copias de seguridad deben ser probadas y archivadas regularmente, las mismas deben ser legibles.

DSS04.08 Ejecutar revisiones post-reanudación: Posteriormente a la reanudación de los procesos de negocio y servicios que fueron afectados por incidentes o desastres es necesario evaluar la adecuada implementación del Plan de Continuidad de Negocio (BCP). En la evaluación se debe determinar cuán efectivo es el plan, las capacidades de continuidad, infraestructura técnica, estructura organizativa, relaciones, habilidades, competencias, funciones, responsabilidades y la recuperación ante incidentes presentados.

Establecer las debilidades u omisiones del Plan de Continuidad de Negocio (BCP) así como sus capacidades y posteriormente realizar las recomendaciones para la mejora de este, para finalmente obtener la autorización de la dirección para realizar los cambios en el plan y aplicarlos a través del proceso de control de cambios de la JAFAP.

Área: Gestión de Proyectos

La Organización debe administrar sus proyectos de TI de manera que logre sus objetivos, satisfaga los requerimientos, cumpla con los términos de calidad, tiempo y presupuesto óptimos preestablecidos.

BAI01 Gestionar los programas y proyectos

Con el fin de alcanzar los beneficios del negocio y reducir el riesgo de retrasos y costos inesperados, asegurando el valor y la calidad de los entregables del proyecto, se deben gestionar los programas y proyectos alineados a la estrategia corporativa mediante los procesos de iniciación, planificación, control, ejecución y cierre de proyectos sumado a una revisión post implementación. Este proceso de gestión debe considerar las siguientes actividades:

BAI01.01 Mantener un enfoque estándar para la gestión de programas y proyectos: Establecer y mantener un enfoque para la gestión de proyectos que permita la revisión y toma de

decisiones alineado al entorno de la empresa y las buenas prácticas.

El enfoque debe cubrir todo el ciclo de vida de los programas y proyectos, incluyendo la gestión de la integración, gestión del alcance, recursos, riesgos, costos, calidad, tiempo, comunicaciones, gestión de interesados, gestión de adquisiciones y la gestión de riesgos.

BAI01.02 Iniciar un programa: Iniciar un plan de realización de beneficios de los programas proyectos, en donde se acuerden los responsables del patrocinio y aprobación de los programas y proyectos.

Designar los gerentes dedicados a los programas y proyectos que cuenten con las competencias y habilidades adecuadas para una gestión eficiente y efectiva de estos.

BAI01.03 Gestionar el compromiso de las partes interesadas: Asegurar el intercambio de información precisa, consistente y oportuna a todas las partes interesadas de los programas y proyectos.

Con el fin de cumplir con lo indicado anteriormente, se requiere la planificación de la forma en que las partes interesadas serán identificadas, analizadas, comprometidas y gestionadas a lo largo del ciclo de vida de los proyectos.

Medir la efectividad del compromiso de las partes interesadas y tomar acciones cuando sea necesario, mediante un análisis de los intereses y requisitos de estas.

Asignar la responsabilidad ejecutiva para cada proyecto, incluido el logro de beneficios, control de costos, gestión de riesgos y la coordinación de las actividades de los proyectos.

BAI01.04 Desarrollar y mantener el plan de programa: Definir y documentar un plan de programa que cubra todos los proyectos de la Organización, en el cual se detallen los productos y servicios a obtener las habilidades y cantidad de personal requeridos, así como las partes interesadas.

Preparar un presupuesto del programa donde se refleje los costos del ciclo de vida completo, así como los beneficios financieros y no financieros asociados.

BAI01.05 Lanzar y ejecutar el programa: Planificar, dar recursos y asignar las responsabilidades para cada proyecto del programa.

Establecer oficinas de gestión de programas y proyectos, planificando auditorías, revisiones

de calidad y revisión de los beneficios realizados.

BAI01.06 Supervisar, controlar e informar de los resultados del programa: Supervisar y controlar el rendimiento del programa general y de los proyectos dentro del programa, incluyendo la contribución al negocio y a las TI.

Gestionar el desempeño de los programas y proyectos versus la planificación en los criterios clave, por ejemplo, alcance, calidad, costos y tiempo para identificar desviaciones al plan y tomando las acciones correctivas cuando sean necesarias.

BAI01.07 Lanzar e iniciar proyectos dentro de un programa: Crear un entendimiento del alcance del proyecto a las partes interesadas, mediante una declaración clara y escrita en donde se defina la naturaleza, alcance y beneficios esperados de los proyectos.

Asegurar que cada proyecto tenga uno o más patrocinadores con autoridad suficiente para gestionar la ejecución del proyecto.

Confirmar que la definición del proyecto describa los requerimientos para el plan de comunicación con las partes interesadas.

BAI01.08 Planificar los proyectos: Establecer y mantener un plan de proyecto formal, aprobado e integrado para guiar la ejecución del proyecto y controlarlo durante su ciclo de vida. El plan debe incluir los entregables del proyecto, criterios de aceptación, estimaciones de recursos necesarios, hitos (punto o evento significativo dentro de un proyecto o programa) y la ruta crítica.

Definir las líneas base del proyecto (alcance, costos, tiempo y calidad), con la revisión y aprobación respectiva y su incorporación en el plan integrado de proyectos.

Mantener los planes de proyecto y cualquier plan secundario (riesgos, calidad, plan de beneficios) actualizado, para reflejar su progreso real y los cambios aprobados.

BAI01.09 Gestionar la calidad de los programas y proyectos: Preparar y ejecutar un plan, procesos y prácticas de gestión de calidad, revisado y acordado por las partes interesadas.

Identificar y definir las actividades y prácticas de aseguramiento de la calidad durante la planificación del programa y del proyecto.

Realizar actividades de control y de aseguramiento de la calidad de acuerdo con lo definido en el plan de gestión de la calidad y demás requerimientos de la Organización.

BAI01.10 Gestionar el riesgo de los programas y proyectos: Establecer un enfoque de gestión de riesgos del proyecto, el cual incluya la identificación, análisis, respuesta, mitigación, supervisión y control de los riesgos.

Definir los responsables de los planes de respuesta a los riesgos, así como la gestión y comunicación del riesgo dentro de la estructura de Gobierno del proyecto.

Mantener y revisar el registro de los riesgos potenciales del proyecto y analizar periódicamente el estado de estos.

BAI01.11 Supervisar y controlar proyectos: Establecer un conjunto de criterios de medición del desempeño del proyecto en donde se incluya al menos el alcance, los costos, el tiempo y el nivel de riesgo del proyecto.

Evaluar el impacto de las desviaciones del proyecto según lo planificado, comunicarlo a los interesados y proponer los ajustes cuando correspondan.

Definir un sistema de control de cambios al proyecto de forma en que todos los cambios a la línea base sean adecuadamente revisados, aprobados e incorporados en el plan de proyecto.

BAI01.12 Gestionar los recursos y los paquetes de trabajo del proyecto: Identificar las necesidades de recursos del negocio y del proyecto, para definir los perfiles y responsabilidades de las tareas.

Definir y acordar las responsabilidades sobre los procesos de adquisición de bienes y servicios requeridos para el proyecto.

BAI01.13 Cerrar un proyecto o interacción: Definir y aplicar los pasos para el cierre del proyecto donde se incluyan revisiones post implementación que evalúen si el proyecto obtuvo los resultados y beneficios planificados.

Obtener la aceptación de los entregables del proyecto y la transferencia de resultados a los interesados.

Documentar las lecciones aprendidas de los participantes del proyecto con el fin de utilizarlas en proyectos futuros.

BAI01.14 Cerrar un programa: Realizar el cierre del proyecto mediante la aprobación formal, la validación de los entregables y la comunicación de cierre.

El proyecto debe ser eliminado del portafolio de inversiones activas de la Organización.

BAI03 Gestionar la identificación y la construcción de soluciones

La Organización debe establecer soluciones puntuales y rentables que permitan soportar la estrategia del negocio y los objetivos planteados, para lograr esto debe contemplar los siguientes elementos:

BAI03.01 Diseñar soluciones de alto nivel: Crear un diseño de acuerdo con los estándares de diseño de la Organización, en consonancia con el negocio, la estrategia de TI, la arquitectura empresarial, los estándares de seguridad de la información, las leyes y regulaciones aplicables.

Establecer las especificaciones de diseño de alto nivel que traduzcan las soluciones propuestas en productos que satisfagan los requerimientos organizacionales.

Remitir el diseño final a las partes interesadas o patrocinador del proyecto para la debida aprobación basada en los criterios establecidos.

BAI03.02 Diseñar los componentes detallados de la solución: Desarrollar, documentar y elaborar diseños detallados considerando los procesos de negocio, controles, manuales, aplicaciones, soporte e infraestructura de TI.

Diseñar las etapas de procesamiento de la aplicación que incluya reglas de negocio, controles automatizados, casos de uso y tipos de transacciones.

BAI03.03 Desarrollar los componentes de la solución: Desarrollar procesos de negocio, servicios de soporte, aplicaciones, infraestructura y repositorios de información basados en las especificaciones acordadas.

Cuando el desarrollo de soluciones sea contratado a un proveedor externo, se debe asegurar que el mantenimiento, soporte y licenciamiento estén incluidos en las obligaciones contractuales.

Evaluar la configuración y eficiencia de las soluciones adquiridas y su interoperabilidad con las demás aplicaciones, sistemas operativos e infraestructura existente.

BAI03.04 Obtener los componentes de la solución: Crear y mantener un plan de adquisiciones de los componentes de la solución., considerando los costos, riesgos y actualizaciones requeridas a lo largo del ciclo de vida del proyecto.

Revisar y aprobar los planes de adquisiciones tomando en cuenta los costos, beneficios de conformidad técnica con los estándares de arquitectura empresarial.

Registrar los recibos de todas las adquisiciones realizadas, tanto de software como de infraestructura y otros activos.

BAI03.05 Construir soluciones: Integrar y configurar los componentes de la solución de TI con las especificaciones y requerimientos de calidad, considerando los roles de los usuarios y las partes interesadas.

Implementar pistas de auditoría durante la configuración e integración del hardware y software para proteger los recursos y asegurando la disponibilidad e integridad.

Asegurar la interoperabilidad de los componentes de la solución mediante pruebas de soporte.

Asegurar que el software adquirido o desarrollado cumpla con los requerimientos definidos en el caso de negocio.

BAI03.06 Realizar controles de calidad: Definir un plan de calidad y prácticas que incluya criterios de calidad, procesos de validación y verificación, definición de cómo se revisará la calidad y los roles y responsabilidades.

Supervisar la solución basada en los requerimientos del proyecto, las políticas empresariales y las metodologías de desarrollo.

Mantener un registro de las revisiones, resultados y correcciones realizadas, para repetir las evaluaciones en los casos en que se consideren necesarios.

BAI03.07 Preparar pruebas de la solución: Crear un plan de pruebas integradas con el fin de verificar que la solución opera satisfactoriamente en el entorno real, entrega los resultados y beneficios esperados.

Crear un entorno de pruebas que soporte el alcance completo de la solución para reflejarlo lo más fielmente las condiciones reales de operación.

Establecer procedimientos de prueba para la evaluación de la operativa de la solución, asegurando la definición de los papeles, responsabilidades, criterios de prueba y la aprobación por las partes interesadas y por el patrocinador del proyecto.

BAI03.08 Ejecutar pruebas de la solución: Realizar las pruebas de las soluciones y sus componentes de acuerdo con el plan de pruebas definido, incluidos dueños de los procesos y usuarios finales de la solución.

Identificar, registrar y clasificar los errores durante las pruebas. Se deben repetir las pruebas hasta que los errores significativos hayan sido resueltos.

Registrar los resultados de las pruebas y comunicarlos a las partes interesadas.

BAI03.09 Gestionar los cambios a los requerimientos: Evaluar el impacto de las solicitudes de cambio a la solución durante la fase de desarrollo en el caso de negocio y en el presupuesto, con el propósito de categorizarlas y priorizarlas.

Asegurar la comprensión y aprobación de los resultados de los procesos de cambio por las partes interesadas y el patrocinador.

BAI03.10 Mantener soluciones: Desarrollar y ejecutar un plan de mantenimiento de los componentes de la solución, que incluya revisiones periódicas respecto a las necesidades del negocio, estrategias de actualización, riesgos y requerimientos de seguridad.

De requerirse cambios mayores a la solución, se deben considerar los procesos de gestión de cambios indicados en el apartado anterior.

Área: Decisiones sobre asuntos estratégicos de TI

Los superiores deben apoyar la gestión de TI y ayudar en la toma de decisiones estratégicas ligadas a TI, logrando un equilibrio en los recursos y la adecuada atención a las unidades de la Organización.

APO01 - Gestionar el Marco de Gestión de TI

APO01.01 Definir la estructura organizativa: Establecer un comité estratégico de TI a nivel de gerencia, con el objetivo de apoyar la gestión de TI y la correcta aplicación de las políticas relacionadas. Así mismo, velar por la continuidad, resolución de conflictos y el uso adecuado de los recursos.

APO02 - Gestionar la Estrategia

APO02.5 Definir un plan estratégico y la hoja de ruta: Obtener apoyo de las partes interesadas y aprobación de las políticas y planes confeccionados.

Área: Cumplimiento de obligaciones relacionadas con la gestión de TI

La Organización debe identificar y velar por el cumplimiento del marco jurídico que tiene incidencia sobre la gestión de TI y que pueda afectar los objetivos y la operación de la Entidad.

MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos

La Empresa debe asegurar el cumplimiento de los requisitos externos que le sean aplicables mediante las siguientes actividades:

MEA03.01 Identificar requisitos externos de cumplimiento: Asignar responsables de identificar y supervisar los cambios legales, regulatorios y contractuales aplicables a la utilización de recursos de TI.

Identificar los requerimientos legales sobre protección de datos, controles internos, información financiera y propiedad intelectual.

Mantener un inventario actualizado de los requisitos legales, regulatorios y contractuales que apliquen a la JAFAP, así como su impacto a la Organización y las acciones necesarias para su cumplimiento.

MEA03.02 Optimizar la respuesta a requisitos externos: Revisar y ajustar las políticas y procedimientos internos según los cambios externos en la legislación y regulaciones aplicables al negocio.

Comunicar oportunamente a los colaboradores las actualizaciones generadas por cambios en el entorno legal y regulatorio.

MEA03.03 Confirmar el cumplimiento de requisitos externos: Evaluar regularmente las políticas y procedimientos internos con el fin de asegurar el cumplimiento de requisitos legales y regulatorios.

Gestionar las deficiencias en el cumplimiento de políticas, estándares y procedimientos con

el propósito de disminuir el riesgo operacional.

Documentar los incidentes relacionados con incumplimiento de políticas, procedimientos y regulaciones con el fin de mantener un registro de lecciones aprendidas.

MEA03.04 Obtener garantía del cumplimiento de requisitos externos: Obtener confirmación sobre el cumplimiento de políticas y procedimientos internos, así como de leyes y regulaciones externas mediante procesos de evaluación realizados tanto como por colaboradores de la JAFAP como por terceros independientes como por ejemplo auditores externos.

Obtener declaraciones de proveedores de servicio de TI sobre el cumplimiento de las leyes y regulaciones aplicables.

Supervisar e informar los incidentes de incumplimiento y en los casos en que se considere necesario investigar las causas generadoras del incumplimiento.

4.6. Metodología de mantenimiento

La presente propuesta está basada en los resultados de la evaluación de los procesos de la JAFAP por lo cual para la aplicación y mantenimiento del presente modelo de Control Interno se deberán considerar los siguientes elementos:

- Planes a corto y largo plazo de la Organización: Considerar los planes estratégicos y operacionales con el fin de orientar el modelo de Control Interno al logro de los objetivos de la Entidad.
- Políticas y prácticas de Gobierno: Evaluar periódicamente los planes, procedimientos y bases de conocimiento de la JAFAP para identificar oportunidades de mejora.
- Capacidades y recursos disponibles: Tener identificados los recursos con los que cuenta la Organización y evaluar la necesidad de ajustes tanto en el recurso humano como en la estructura financiera.
- Evaluación del entorno y de los procesos de las diferentes áreas: Analizar el comportamiento de la industria para identificar las oportunidades y amenazas de la Organización.
- Evaluación del desempeño y eficacia de los procesos contables gestionados por tecnologías de información: Medir la eficiencia y eficacia de los procesos mantenidos en la Entidad con el fin

de obtener información para la toma de decisiones.

- Grado de satisfacción de los usuarios: Considerar la opinión y evaluación de los servicios por parte de los usuarios para determinar cómo se desempeñan los procesos y el personal.
- Requerimientos legales o normativos: Identificar los cambios en las leyes y regulaciones asociadas al negocio y aplicar las actualizaciones pertinentes.
- Resultados obtenidos de auditorías internas y externas: Implementar las recomendaciones y oportunidades de mejora obtenidas en los procesos de revisión internos y externos.

Capítulo V. Conclusiones y recomendaciones

5.1 Conclusiones

La evolución de las tecnologías y la competitividad del mercado financiero costarricense han llevado a las organizaciones a contar con procesos y marcos de control los cuales permitan una operación eficiente, eficaz y que, a su vez, contribuyan con el logro de sus objetivos, en el caso de la JAFAP mejorar el bienestar y calidad de vida de los afiliados.

Las organizaciones deben garantizar una estructura de control adecuada orientada a disminuir el impacto de factores internos y externos los cuales afectan la finalidad de la Entidad. A su vez, los procesos contables mediados por tecnologías de información son fundamentales para la toma de decisiones y mejorar la rentabilidad de la Entidad. Mediante la propuesta de un modelo de Control Interno se busca proporcionar a la JAFAP una herramienta para medir, evaluar y controlar los procesos contables mediados por tecnologías de información con base en las mejores prácticas de COBIT 5 y la normativa vigente aplicada por la Contraloría General de la República (N-2-2007-CO-DFOE).

En este proyecto se desarrolló un análisis del mercado financiero costarricense, una descripción de la estructura administrativa de la JAFAP y la relación del departamento contable con el de TI, un análisis y comparación de los procesos contables vinculados con TI y por último la propuesta de un modelo de Control Interno basados en los resultados obtenidos. Dado lo anterior, se presentan las siguientes conclusiones:

- El mercado financiero costarricense se encuentra conformado por una gran cantidad de Bancos, Cooperativas, Empresas Financieras no Bancarias, entre otras, las cuales brindan una amplia cartera de productos y servicios a sus clientes, lo cual la JAFAP se desempeña en un mercado altamente competitivo. Ante esto, la Entidad ha apostado por estrategias para acercarse con sus afiliados, como lo son el establecimiento de sucursales en todas las sedes y recintos de la Universidad de Costa Rica, así como ofrecer una variedad de productos y servicios dirigidos a satisfacer las necesidades de sus clientes.

- Las entidades del sector financiero se encuentran reguladas por el Consejo Nacional de Supervisión del Sistema Financiero (CONASSIF), sus órganos adscritos y la normativa correspondiente emitida por estos según el marco legal vigente, sin embargo, dada la naturaleza jurídica de la JAFAP, está no se encuentra sujeta a dichas normativas y las regulaciones correspondientes, por lo contrario cuenta con autonomía para la toma de decisiones y el establecimiento de políticas, normas y procedimientos relacionados con su actividad.
- Existen diferentes marcos de referencia de Control Interno tanto a nivel nacional como internacional que pueden adoptar las organizaciones con el fin de proporcionar seguridad razonable sobre el cumplimiento de los objetivos, garantizar eficiencia y eficacia en las operaciones, cumplir con el ordenamiento jurídico y técnico, así como garantizar la confiabilidad y oportunidad de la información.
- La evolución de las tecnologías de información y su vinculación con los procesos contables permiten a las empresas acceder a la información financiera de manera rápida garantizando su completitud y confiabilidad, facilitando la toma de decisiones, así como mejorar la gestión interna. Dado esto, es de vital importancia el establecimiento de mecanismos de Control Interno orientados a los procesos contables gestionados mediante tecnología de información.
- La JAFAP cuenta con una estructura organizativa y manual de Organización donde se establecen formalmente las funciones y responsabilidades de cada uno de los departamentos de la Entidad, así como con manuales de procedimientos para los diferentes procesos de la operación diaria de la Organización, para identificar las actividades y los responsables de estas.
- Con el resultado de la identificación y evaluación de los procesos contables vigente en la JAFAP se determinó que existe desconocimiento por parte de los colaboradores respecto a los procedimientos relacionados a los diferentes procesos y las actividades de control ejecutadas para mitigar los riesgos asociados.

Adicionalmente, se identificaron áreas de revisión donde la JAFAP no cuenta con procedimientos documentados y aprobados según lo establecido por las Normas Técnicas para la gestión y control de las Tecnologías de Información de la Contraloría General de la

República Capítulo I “Normas de Aplicación General” (N-2-2007-CO-DFOE), lo cual representa una oportunidad de mejora para la gestión de la Entidad.

- La propuesta de Control Interno se basa en el análisis del marco regulatorio de la Contraloría General de la República para la gestión y control de tecnologías de información mediante un análisis de COBIT 5, con el propósito de contribuir al fortalecimiento de la Organización, cumplir con los objetivos propuestos y minimizar los riesgos asociados.

  Las actividades de control propuestas permiten a las organizaciones estandarizar los controles de TI y, a su vez, alinear los objetivos de TI con los organizacionales con el fin de contribuir al logro de estos, así como mejorar la eficacia y eficiencia de las operaciones.

5.2 Recomendaciones

Una vez elaborada la propuesta de un modelo de Control Interno para el proceso contable con base en la normativa vigente aplicada por la Contraloría General de la República mediante un análisis de COBIT 5 y según las conclusiones indicadas anteriormente, se presentan las recomendaciones:

- Se recomienda a la JAFAP la adopción de buenas prácticas y estándares reconocidos de Control Interno y de gestión de procesos con la debida adaptación a la realidad de la Empresa, enfocados en la implementación de actividades para generar valor dentro de la Entidad y sean utilizados como referencia para la mejora de la operación, aumentar la rentabilidad del negocio y, al mismo tiempo, aprovechar las oportunidades y contrarrestar las amenazas.

- Se recomienda contar con un programa de inducción y capacitación al personal de nuevo ingreso a la JAFAP y adicionalmente un programa de actualización a los colaboradores actuales, con el fin de aumentar los conocimientos teóricos y prácticos de los procesos en que participan, así como los papeles y responsabilidades asociados, con el fin de brindar los conocimientos, habilidades y actitudes necesarias para alcanzar el máximo desempeño.

- Se recomienda establecer canales internos de comunicación para la correcta divulgación de los procedimientos y demás actividades de Control Interno implementados por la Administración, con el fin de garantizar que estos sean de conocimiento por todos los

colaboradores.

- Se recomienda a la Administración de la JAFAP la realización periódica de autoevaluaciones de Control Interno con el objetivo de evaluar la eficacia de los controles internos implementados, identificar las oportunidades de mejora y plantear los planes de acción correspondientes para corregir las debilidades encontradas contribuyendo así al fortalecimiento del Sistema de Control Interno, el cumplimiento de la misión, visión y objetivos de la Empresa.
- Se recomienda a la JAFAP la implementación de la propuesta realizada en el presente trabajo de investigación, mediante la cual se brinde una guía de buenas prácticas y actividades para medir, evaluar y controlar la gestión de los procesos contables relacionados con tecnología de información.
- Se recomienda a la Administración implementar un proceso de actualización de la propuesta de Control Interno para el adecuado mantenimiento, donde se consideren al menos los planes a corto y largo plazo de la Entidad, políticas y prácticas de Gobierno, capacidades, recursos disponibles, evaluación del entorno y de los procesos de las diferentes áreas, grado de satisfacción de los usuarios, requerimientos legales o normativos y resultados obtenidos de auditorías internas y externas.

ANEXOS

ANEXO #1: Cuestionario Área de Crédito y Cobro

Cuestionario: Crédito y Cobro			
Preguntas	**Respuesta 1**	**Respuesta 2**	**Respuesta 3**
1. ¿El personal a cargo conoce los procedimientos para otorgar créditos?	Sí	Sí	Sí
2. ¿Con qué periodicidad se le brinda capacitación a los colaboradores de crédito y cobro?	Permanente	Continuamente	Se brinda capacitación de forma constante.
3. ¿El personal se capacita constantemente para el uso del sistema SIBU?	Sí	Sí	Sí
4. ¿Los cambios a realizar en los módulos de crédito y cobro son comunicados previamente al personal?	Sí	Sí	Sí
5. ¿Cuáles departamentos tienen acceso a la información crediticia de los afiliados?	Los accesos los determina el área de TI	Los funcionarios del departamento de crédito, y cualquier Otro puesto que así lo requiera con la debida autorización del nivel jerárquico con potestad para dar dicho permiso.	Crédito y Cobro, Tesorería, Inteligencia de negocios, Auditoría.
6. ¿Se verifica mediante la revisión de planilla mensual el estatus de los afiliados (activo e inactivo) en el sistema SIBU?	No	No tiene conocimiento	Sí
7. ¿Para las solicitudes de créditos se corrobora que los datos del sistema de constancias salariales de la UCR coincidan con los datos del sistema SIBU?	Sí	Sí	Sí
8. ¿Se verifica que los requisitos para la solicitud de créditos sean ingresados correctamente al sistema (*Check list*)?	Sí	Sí	Sí
9. ¿Para los créditos sobre aportes se verifica que sea correcto el tipo (corriente o no fiduciario) y monto máximo del crédito suministrado por el sistema SIBU?	Sí	Sí	Sí

Cuestionario: Crédito y Cobro			
Preguntas	**Respuesta 1**	**Respuesta 2**	**Respuesta 3**
10. ¿Se verifica que la información suministrada por el sistema SIBU relacionada al Cash Back sea correcta?	Sí	Sí	Sí
11. ¿Existe segregación de funciones en cuanto a la realización, revisión y aprobación de créditos?	Sí	Sí	Sí
12. ¿Qué cargos están involucrados en la realización, revisión y aprobación de créditos?	Supervisor, Sub-Jefatura y Jefatura-	Analistas, Jefaturas	Supervisión de Sede, Sub-Jefatura de Crédito y Cobro, Jefatura de Crédito y Cobro.
13. ¿Se realizan respaldos de los expedientes de crédito digitales?	Sí	Sí	Sí
14. ¿Con qué frecuencia se realizan los respaldos de los expedientes de crédito digitales?	De conformidad con el envío al área de Archivo.	Siempre	forma diaria
15. ¿Existe historial crediticio de los afiliados?	Sí	Sí	Sí
16. ¿El historial crediticio de los afiliados se encuentra respaldado?	Sí	Sí	Sí
17. ¿Cómo se verifica que los rebajos de planilla y los rebajos de afiliados pensionados (documento realizado por TI) sean los correctos?	El área de TI realiza el proceso validando y procesando las inconsistencias.	No aplica	Se verifica contra el estado de cuenta de cada persona afiliada.
18. ¿Cómo verifica el departamento de cobro que las deducciones ejecutadas por TI se apliquen correctamente en el sistema SIBU?	Al inicio de mes se toma una muestra para validar la correcta aplicación.	No aplica	El departamento de Crédito y Cobro realiza una revisión de la aplicación de planilla.
19. ¿La aplicación del pago de cuotas se actualiza de manera inmediata en el sistema SIBU?	Sí	Sí	Sí
20. ¿Se verifica que los depósitos realizados por afiliados para el pago de cuotas no hayan sido aplicado con anterioridad?	Sí	No tiene conocimiento	Sí

Cuestionario: Crédito y Cobro			
Preguntas	**Respuesta 1**	**Respuesta 2**	**Respuesta 3**
21. ¿Se verifica que los prestamos activos sean cancelados previamente a la entrega de las liquidaciones?	Sí	Sí	Sí
22. ¿Quién verifica la aplicación de ahorros y aportes a los prestamos activos?	Supervisor, Sub-Jefatura y Jefatura	Departamento Cobro	El departamento de Crédito y Cobro.
23. ¿Con qué regularidad recibe el departamento de crédito y cobro el saldo de la cartera de crédito (enviado por el departamento de TI)?	Diario	Semanalmente	Una vez al mes.
24. ¿Se verifica que las gestiones de cobro sean ingresadas al sistema SIBU correctamente?	Sí	Sí	Sí
25. ¿Se verifica que los afiliados incluidos como morosos (base de datos entregada por TI) efectivamente se encuentren con dicho estado en el sistema SIBU?	Sí	No tiene conocimiento	Sí
26. ¿Quién realiza la verificación de los afiliados morosos en el sistema SIBU?	Por medio de la gestión diaria	Departamento de cobro	El departamento de Crédito y Cobro.
27. ¿Con qué frecuencia se revisa la clasificación de morosidad de créditos (Gestión de Cobro y Cobro judicial) en el sistema SIBU?	Mensual	No aplica	Se revisa de forma mensual con los reportes de Morosidad.

ANEXO #2: Cuestionario Área de Contabilidad

Cuestionario: Contabilidad			
Preguntas	**Respuesta 1**	**Respuesta 2**	**Respuesta 3**
1. ¿El área contable posee herramientas para la evaluación de riesgos?	Sí	No	Sí
2. ¿El sistema SIBU contribuye con el logro de los objetivos del área contable?	Sí	Sí	Sí
3. ¿Se le brinda inducción del sistema SIBU al personal contable?	Sí	Sí	Sí
4. ¿El sistema SIBU es sometido a actualizaciones e incorporación de nuevas funciones según requerimientos del personal?	No	Sí	Sí
5. ¿Los funcionarios de contabilidad reciben capacitación sobre las actualizaciones del sistema SIBU?	No	Sí	Sí
6. ¿Existen políticas de seguridad de la información relacionadas al departamento contable?	Sí	Sí	Sí
7. ¿Se requiere un usuario y contraseña para ingresar al módulo de contabilidad en el sistema SIBU?	Sí	Sí	Sí
8. ¿El acceso al área de contabilidad es restringido?	Sí	Sí	Sí
9. ¿Cuáles son los controles de acceso al área contable?	El área de T.I solo brinda acceso a los usuarios del departamento	a los sistemas mediante accesos otorgados por TI y al espacio físico con llaves de acceso	Clave y contraseña y cada asistente tiene las opciones que necesita, son diferentes para todos de acuerdo con los permisos que tengan
10. ¿Existen contratos de confidencialidad con los colaboradores del departamento contable?	Sí	Sí	Sí
11. ¿El departamento de contabilidad cuenta con un plan de contingencia en caso de alguna falla del sistema SIBU?	No	Sí	No

Cuestionario: Contabilidad			
Preguntas	**Respuesta 1**	**Respuesta 2**	**Respuesta 3**
12. ¿Reciben los colaboradores inducción de los procedimientos a realizar en cada puesto contable?	Sí	Sí	Sí
13. ¿Los procedimientos existentes para cada puesto contable son claros y precisos?	Sí	Sí	Sí
14. ¿Para el soporte de los procesos contables se requiere la utilización de información en formato físico?	Sí	No	No
15. ¿Existe respaldo de la información generada por contabilidad?	Sí	Sí	Sí
16. ¿Existe segregación de funciones en la realización, revisión y aprobación de los asientos contables?	Sí	Sí	Sí
17. ¿Cuáles son los cargos involucrados en el proceso de realización, revisión y aprobación de asientos contables?	COORDINAR DE CONTABILIDAD Y SU ASISTENTE INMEDIATA	asistente y coordinador (si este no se encuentra lo hace el subcoordinador)	Asistentes, subcoordinador y coordinador
18. ¿Existe segregación de funciones en la realización, revisión y aprobación de la conciliación de cuentas de cajas, ahorros y conciliación de cheques?	Sí	Sí	Sí
19. ¿Cuáles son los cargos involucrados en el proceso de realización, revisión y aprobación de conciliación de cuentas de cajas, ahorros y conciliación de cheques?	AUXILIARES CONTABLES	asistente y coordinador (si este no se encuentra lo hace el subcoordinador), en el caso de conciliaciones bancarias intervienen los 3 puestos	Asistentes, subcoordinador y coordinador
20. ¿Los datos generados por el sistema SIBU son sometidos a revisión por parte del personal a cargo?	Sí	Sí	Sí
21. ¿Los estados financieros son generados por el sistema SIBU?	Sí	Sí	Sí
22. ¿Se realizan auditorías internas y externas a los procesos de contabilidad?	Sí	Sí	Sí

Cuestionario: Contabilidad			
Preguntas	**Respuesta 1**	**Respuesta 2**	**Respuesta 3**
23. ¿Con qué regularidad se realizan las auditorías internas y externas a los procesos de contabilidad?	ANUALES	auditorías internas cada vez que el área lo estime conveniente, externas anualmente mediante 3 visitas de revisión a lo largo del periodo.	3 veces al año la externa y la interna indefinidamente
24. ¿Los estados financieros se someten a un proceso de revisión y aprobación por el órgano competente?	Sí	Sí	Sí
25. ¿Existen planes de continuidad de negocio en el área contable?	Sí	Sí	No

ANEXO #3: Cuestionario Área de Tecnologías de Información

Cuestionario: Tecnologías de información			
Preguntas	**Respuesta 1**	**Respuesta 2**	**Respuesta 3**
1. ¿Se ha establecido un plan estratégico de TI alineado a la estrategia institucional?	Si	si	si
2. ¿Se ha definido un comité de tecnología que defina prioridades, que asigne recursos y que atienda los requerimientos de la institución?	Si	no	si
3. ¿Se ha elaborado, aprobado, divulgado y se encuentra vigente un procedimiento para ejecutar el plan estratégico de TI?	Si	no	si
4. ¿Se ha elaborado, aprobado, divulgado y se encuentran vigente una metodología de análisis de riesgos?	No	no	no, se encuentra en proceso
5. ¿Se ha elaborado, aprobado, divulgado y se encuentran vigente una lista de amenazas para cada análisis de riesgo?	No	no	Se encuentra en proceso
6. ¿Se ha elaborado, aprobado, divulgado y se encuentran vigente un método para calcular el riesgo inherente y residual?	No	no	si
7. ¿Se ha elaborado, aprobado, divulgado y se encuentran vigente un procedimiento para diseñar el plan de acción como respuesta al riesgo?	No	no	está en proceso
8. ¿Se ha elaborado, aprobado, divulgado y se encuentran vigente un procedimiento para monitorear periódicamente las vulnerabilidades, amenazas y riesgos identificados?	No	no	se encuentra en proceso
9. ¿Se ha elaborado, aprobado, divulgado y se encuentran vigente una política que defina los lineamientos y controles para un marco de seguridad de la información?	No	si	si
10. ¿Se ha elaborado, aprobado, divulgado y se encuentran vigente un procedimiento para la revisión periódica del marco de seguridad de la información?	Si	si	si
11. ¿Se ha elaborado, aprobado, divulgado y se encuentran vigente un plan global de seguridad de TI, donde se defina la implementación de políticas y procedimientos de seguridad de la información?	Si	si	si
12. ¿Se ha elaborado, aprobado, divulgado y se encuentran vigente un procedimiento para la vigilancia del debido cumplimiento de las	Si	si	si

Cuestionario: Tecnologías de información			
Preguntas	**Respuesta 1**	**Respuesta 2**	**Respuesta 3**
responsabilidades de la seguridad de la información?			
13. ¿Se ha elaborado, aprobado, divulgado y se encuentran vigentes acuerdos de confidencialidad y medidas de seguridad específicas, relacionadas con el manejo de la documentación y rescisión de contratos?	Si	si	si
14. ¿La revisión de los servidores se realiza de manera regular?	No tiene conocimiento	Sí	Sí
15. ¿Con qué regularidad se realiza la revisión de los servidores?	No	todo los días y tenemos alertas que nos informan al correo	bimensual
16. ¿Cuenta con acceso restringido el cuarto de servidores?	Sí	Sí	Sí
17. ¿Qué cargos tienen acceso al cuarto de servidores?	Coordinador Infraestructura, Jefatura TI	soporte TI e infraestructura	Coordinador de Infraestructura
18. ¿Se realiza con regularidad el respaldo de las Bases de Datos?	Sí	Sí	Sí
19. ¿Quién realiza los respaldos de las Bases de Datos?	automáticos y DBA	DBA	El DBA
20. ¿Con qué regularidad se realizan los respaldos de las Bases de Datos?	Diarios	todos los días	diario
21. ¿Se ha elaborado, aprobado, divulgado y se encuentran vigente una política que establezca controles de acceso para el manejo de información impresa, visible o almacenada en medios físicos?	Si	no se	no
22. ¿Qué cargos tienen acceso al módulo de seguridad en SIBU?	Oficial Seguridad TI	el compañero de seguridad	el oficial de seguridad
23. ¿Se verifica que los usuarios Activos con acceso al sistema SIBU sean colaboradores actuales de la JAFAP?	Sí	Sí	Sí
24. ¿Con qué regularidad se realiza la revisión de los colaboradores que tienen acceso al sistema SIBU?	No sé	no sé, porque es una tarea del oficial de seguridad	mensual
25. ¿Cómo se verifica que los usuarios Bloqueados e Inactivos no tengan acceso al sistema SIBU?	No se	no sé, porque es una tarea del oficial de seguridad	están bloqueados y registrados

Cuestionario: Tecnologías de información			
Preguntas	**Respuesta 1**	**Respuesta 2**	**Respuesta 3**
26. ¿Cómo se verifica que los usuarios tengan acceso únicamente a los módulos o transacciones relacionados a su puesto?	Perfiles y Roles autorizados	con permisos a nivel de sistema los cuales son revisados por el oficial de seguridad	por roles
27. ¿Se cuenta con medidas de prevención, detección y corrección a lo largo de toda la Organización para proteger los sistemas de información y la tecnología contra software malicioso?	Si	si	si
28. ¿Existe segregación de funciones en cuanto a la realización y revisión de los procesos de TI?	Sí	Sí	Sí
29. ¿Qué cargos están involucrados en la realización y revisión de los procesos de TI?	Jefatura TI y Coordinadores	jefaturas	Jefatura, Coordinador de infraestructura, Oficial de seguridad, Coordinador de desarrollo
30. ¿Cuenta el departamento de TI con un sitio alterno de TI (oficinas fuera de la Universidad de Costa Rica)?	No	No	No
31. ¿Existe conexión mediante VPN entre el sitio alterno y el principal de TI?	Sí	Sí	Sí
32. ¿Quién es el proveedor de internet en el sitio alterno de TI?	ICE	no se es de la UCR	UCR
33. ¿Quién es el proveedor de internet en las oficinas de la JAFAP en la Universidad de Costa Rica?	ICE	ICE	UCR
34. ¿Se cuenta con un contrato *Service Level Agreement (SLA)* con el proveedor de internet (Universidad de Costa Rica o proveedor externo)?	No tiene conocimiento	Sí	Sí
35. ¿Se ha elaborado, aprobado, divulgado y se encuentran vigente una política para la implementación de medidas de seguridad físicas tales como: esquema del perímetro de seguridad, zonas de seguridad, ubicación de equipos críticos, ¿entre otros?	Si	si	Si

Cuestionario: Tecnologías de información			
Preguntas	**Respuesta 1**	**Respuesta 2**	**Respuesta 3**
36. ¿Se ha elaborado, aprobado, divulgado y se encuentran vigente una política, que establezca las responsabilidades sobre el monitoreo y los procedimientos de reporte y resolución de incidentes de seguridad física?	Si	si	Si
37. ¿Cuenta el cuarto de servidores de TI con extintor de CO2 para emergencias?	Sí	Sí	Sí
38. ¿Con qué regularidad se cambia el extintor de emergencias?	No sé la frecuencia, se realiza con todos los demás de la oficina	cada extintor tiene una fecha que indica cuando es, lo hacen mis compañeros de otras aéreas no de TI	cuando se requiere
39. ¿Cuenta el cuarto de servidores de TI con aire acondicionado?	Sí	Sí	Sí
40. ¿Se mantiene una bitácora actualizada y al día, para el control de ingresos y salida de activos de TI y de la Organización?	Si	si	Si
41. ¿Se ha elaborado, aprobado, divulgado y se encuentran vigente una política que defina la propiedad, custodia y responsabilidad sobre los recursos de TI?	Si	no	Si
42. ¿Es auditado externamente el departamento de TI?	Sí	Sí	Sí
43. ¿Con qué regularidad es auditado externamente el departamento de TI?	Cada semestre	una vez al año	frecuente una vez al año
44. ¿Es auditado internamente el departamento de TI?	Sí	Sí	Sí
45. ¿Con qué regularidad se da la rotación del personal de TI?	Baja	no se	no se da
46. ¿Se ha elaborado, aprobado, divulgado y se encuentran vigente una política que promueva la mejora continua de los servicios de TI?	Si	si	no
47. ¿Se ha elaborado, aprobado, divulgado y se encuentran vigente un plan de continuidad de los servicios de TI?	Si	si	no
48. ¿Se tienen documentadas las acciones preventivas y correctivas para mantener una continuidad razonable de los procesos?	Si	si	si

Cuestionario: Tecnologías de información			
Preguntas	**Respuesta 1**	**Respuesta 2**	**Respuesta 3**
49. ¿Se realizan y documentan pruebas para validar que el plan de continuidad de negocio está operando satisfactoriamente?	No sé	si	no

Bibliografía

Libros

- Escoto, L. R. (2007). Banca Comercial. San José, Costa Rica. EUNED.
- Estupiñán, R. (2006). Control Interno y Fraudes (2a Ed.). Bogotá: Ecoe Ediciones.
- Loría, S. M. (2013). El sistema financiero en los últimos 25 años. San José, Costa Rica. Academia de Centroamérica.
- Rodríguez, U. O. (2012). Supervisión Bancaria en Costa Rica: un camino difícil. San José, Costa Rica. Academia de Centroamérica.

Trabajos Finales de Graduación

- Canales, G., Gamboa, S., Gonzalez, J. y Gonzalez, R. (2014). Propuesta de una estructura de Control Interno y de un sistema de registro de costos y asignación de precios de venta para la empresa Muebles Olmi, S.A. Seminario de grado para optar al grado de Licenciatura Contaduría Pública. Universidad de Costa Rica. Costa Rica
- Mora, Y. (2017). Los sistemas de información contable y su relación con las herramientas tecnológicas. Trabajo de grado para optar por el título de Especialista en estándares Internacionales de contabilidad y auditoría. Universidad de Bogotá Jorge Tadeo Lozano. Bogotá.
- Posso, R. (2014). Diseño de un modelo de Control Interno en la empresa prestadora de servicios hoteleros Eco Turísticos Nativos Activos Eco Hotel La Cocotera, que permitirá el mejoramiento de la información financiera. Tesis de Grado. Universidad de Cartagena. Colombia.
- Ramírez y Donoso (2006). Metodología ITIL: Descripción, funcionamiento y aplicaciones. Seminario de título. Universidad de Chile.

Informes

- Banco Central de Costa Rica (2020). Programa Macroeconómico 2020-2021. Recuperado de: https://activos.bccr.fi.cr/sitios/bccr/publicaciones/DocPolticaMonetariaInflacin/Programa_Macroeconomico_2020-2021.pdf
- Banco Central de Costa Rica (2020). Comentario de la Economía Nacional N.º 5 - 2020. Recuperado de: https://activos.bccr.fi.cr/sitios/bccr/publicaciones/DocPolticaMonetariaInflacin/Comentario_economia_nacional_05_2020.pdf
- Committee of Sponsoring Organizations of the Tredway Commission - COSO (2013). Internal Control-Integrated Framework.
- Information Systems Audit and Control Association, ISACA (2012). COBIT 5, Un Marco de Negocio para el Gobierno y la Gestión de TI de la Empresa.
- Junta de Ahorro y Préstamo de la Universidad de Costa Rica, JAFAP (2020). Manual de Organización.
- Junta de Ahorro y Préstamo de la Universidad de Costa Rica, JAFAP (2020). Reglamento JAFAP Reforma Integral.

Normas

- Instituto de Normas Técnicas de Costa Rica (2011). Gestión de Riesgos. Principios y directrices. INTE/ISO 31000:2011.

Referencias Electrónicas

- Asamblea Legislativa de la República de Costa Rica, Costa Rica (2002). Ley No. 8292 Ley General de Control Interno. Recuperado de: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=49185&nValor3=52569&strTipM=TC

- Boccazzi, C. y Negrete, J. (2015). *Evaluación de Riesgos Tecnológicos y Percepción de la población residente y turista de las comunas de Quintero y Puchuncaví.* Proyecto Académico. Universidad Austral de Chile. Chile. Recuperado de: https://www.redalyc.org/pdf/2233/223353236004.pdf
- Cano, G. y García, M. (2018). Las TICS en las empresas: evolución de la tecnología y cambio estructural en las organizaciones. Revista Científica Dominio de las Ciencias. Recuperado de: https://dominiodelasciencias.com/ojs/index.php/es/article/view/762/pdf
- Contraloría General de la República, Costa Rica (2009). Normas de Control Interno para el Sector Público N-2-2009-CO-DFOE. Recuperado de: https://cgrfiles.cgr.go.cr/publico/docsweb/documentos/control-interno/nci-publico-n-2-2009-co-dfoe.pdf
- Contraloría General de la República, Costa Rica (2007). Normas Técnicas para la gestión y el control de Tecnologías de Información N-2-2007-CO-DFOE. Recuperado de: https://cgrfiles.cgr.go.cr/publico/docsweb/documentos/auditoria/normas-tecnicas-gestion-ti-n-2-2007-co-dfoe.doc
- Córdova, M., Taopanta, G. y Rojas, L. (2019). Tecnologías de Información y Comunicación (TICS) Aplicadas a las Organizaciones empresariales. Revista contribuciones a la Economía. Recuperado de: https://www.hacienda.go.cr/Sidovih/uploads//Archivos/Articulo/tics-organizaciones-empresariales.pdf
- De Vita Montiel, N. (2008). Tecnología de información y comunicación para las organizaciones del siglo XXI. Revista del Centro de Investigación de Ciencias Administrativas y Gerenciales. Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=3217615
- Hiberus Tecnología (2019). ITIL® 4, todas las novedades de ITIL en 2019. Recuperado de: https://www.hiberus.com/crecemos-contigo/novedades-itil-v4/
- Junta de Ahorro y Préstamo de la Universidad de Costa Rica, Costa Rica (2012). *Reseña histórica, Misión y visión.* Recuperado de: http://www.jafapucr.com/Inicio.aspx

- Norton (2021). ¿Qué es el software malicioso y cómo puedo evitarlo? Recuperado de: https://mx.norton.com/internetsecurity-malware.html
- Santillana, R. (2013). Auditoría interna, tercera edición, Pearson Educación, México. Recuperado de: https://catedrafinancierags.files.wordpress.com/2012/04/auditoria-interna-juan-ramc3b3n-santillana.pdf
- Superintendencia General de Entidades Financieras, Costa Rica (2017). Reglamento General de Gestión de la Tecnología de Información. Recuperado de: https://www.sugef.fi.cr/normativa/normativa_vigente/SUGEF%2014-17%20(v2_%2017abr2017).pdf
- Superintendencia de Pensiones, Costa Rica (2017). Reglamento de Riesgos. Recuperado de: https://www.supen.fi.cr/documents/10179/18106/Reglamento+de+Riesgos
- Organización Latinoamericana y del Caribe de Entidades Fiscalizadoras Superiores (2015). El Control Interno desde la perspectiva del enfoque COSO –su aplicación y evaluación en el sector público-. Recuperado de: https://www.olacefs.com/wp-content/uploads/2016/03/15.pdf