UNIVERSIDAD DE COSTA RICA
Ciudad Universitaria Rodrigo Facio

Facultad de Ciencias Económicas
Escuela de Administración de Negocios

Proyecto Final de Graduación

Propuesta de una metodología para la gestión de la seguridad y control de la información en Tecnologías de Información de fundaciones, con base en un análisis de la normativa vigente aplicable por la Contraloría General de la República y por el Consejo Nacional de Supervisión del Sistema Financiero para el sector regulado.

Estudiantes:

Carlos Esteban Alvarado Rivera	A80330
Olman Mata Mata	A83770
José María Vargas Guillén	A76772
Luciano Visoná Castillo	A87055

Miembros del Comité Asesor:
Tutor: Máster Michel Angulo Sosa
Lector: Máster Gino Ramírez Solís
Lector: Licenciado John Rojas Soto

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

San José, Costa Rica

II Ciclo, 2016

UNIVERSIDAD DE COSTA RICA
FACULTAD DE CIENCIAS ECONÓMICAS

Acta # 36-16

Acta de la Sesión 36-16 del Comité Evaluador de la Escuela de Administración de Negocios, celebrada el 28 de noviembre de 2016, con el fin de proceder a la Defensa del Trabajo Final de Graduación de ***Carlos Esteban Alvarado Rivera, carné A80330, Olman Francisco Mata Mata, carné A83770, José María Vargas Guillén, carné A76772, y Luciano Visona Castillo, carné A87055;*** quienes optaron por la modalidad de Seminario de Graduación.

Presentes: Roberto Porras León, quien presidió, Michel Angulo Sosa, como Tutor, Gino Ramírez Solís y John Rojas Soto, como lectores y Kenneth Sánchez Villalobos, quien actuó como Secretario de la Sesión.

Artículo 1

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

Artículo 2

Los estudiantes hicieron la exposición del Trabajo Final titulado **"Propuesta de una metodología para la gestión de la seguridad y control de la información en Tecnologías de Información de fundaciones con base en un análisis de la normativa vigente aplicable por la Contraloría General de la República y por el Consejo Nacional de Supervisión del Sistema Financiero para el sector regulado."**

Artículo 3

Terminada la disertación, los miembros del Comité Evaluador, interrogaron a los postulantes 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 Satisfactoria, y lo declaró Aprobado.
(Satisfactorio /insatisfactorio) (Aprobado /no aprobado)

Artículo 6

El Presidente del Comité Evaluador comunicó en público a los aspirantes, el resultado de la deliberación y los declaró: *Licenciados en Contaduría Pública.*

Se les indicó la obligación de presentarse al Acto Público de Juramentación. Luego se dio lectura al acta que firmaron los miembros del Comité y los estudiantes a las 7:50pm horas.

Roberto Porras León
Representante Director de la Escuela

Carlos Esteban Alvarado Rivera
Carné *A80330*

Michel Angulo Sosa
Tutor del Trabajo

Olman Mata Mata
Carné *A83770*

Gino Ramírez Solís
Lector

José María Vargas Guillén
Carné *A76772*

John Rojas Soto
Lector

Luciano Visona Castillo
Carné *A87055*

Kenneth Sánchez Villalobos
Secretaria 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:_____

Cartago, 15 de noviembre del 2016

Señores:

Universidad de Costa Rica

Escuela de Administración de Negocios

Estimados señores:

Yo, María Fernanda Sanabria Coto, cédula de identidad 1-1429-0780, Bachiller en Filología Española y perteneciente a la Asociación Costarricense de Filólogos carné 225, hago constar que he revisado el Proyecto de Graduación denominado:

Propuesta de una metodología para la gestión de la seguridad y control de la información *en Tecnologías de Información de fundaciones, con base en un análisis de la normativa vigente aplicable por la Contraloría General de la República y por el Consejo Nacional de Supervisión del Sistema Financiero para el sector regulado.*

Dicho documento fue elaborado por los estudiantes:

Esteban Alvarado Rivera	A80330
Olman Mata Mata	A83770
José María Vargas Guillén	A76772
Luciano Visoná Castillo	A87055

Esto con el fin de optar por el grado académico de Licenciatura en Contaduría Pública de la Universidad de Costa Rica. He revisado y corregido aspectos tales como construcción de párrafos, vicios del lenguaje trasladados a lo escrito, ortografía, puntuación y otros relacionados con el campo filológico. **Por lo tanto considero que está listo para ser presentado.**

Atentamente,

Fernanda Sanabria Coto

María Fernanda Sanabria Coto

Asociación Costarricense de Filólogos. Carné No: 225

Cédula de identidad: 1-1429-0780

Universidad de Costa Rica
Sede Rodrigo Facio
Escuela de Administración de Negocios
San Pedro, 2016

Propuesta de una metodología para la gestión de la seguridad y control de la información en Tecnologías de Información de fundaciones, con base en un análisis de la normativa vigente aplicable por la Contraloría General de la República y por el Consejo Nacional de Supervisión del Sistema Financiero para el sector regulado.

Trabajo Final de Graduación sometido a consideración de la Escuela de Administración de Negocios de la Universidad de Costa Rica, para optar por el grado de Licenciatura en Contaduría Pública.

Sustentantes:

Carlos Esteban Alvarado Rivera	**Olman Mata Mata**
José María Vargas Guillén	**Luciano Visoná Castillo**

Aprobado por:

Máster Michel Angulo Sosa
Tutor Trabajo Final de Graduación

_____
Máster Gino Ramírez Solís
Lector Trabajo Final de Graduación

_____
Licenciado John Rojas Soto
Lector Trabajo Final de Graduación

_____
Máster. Roberto Porras León
Tribunal- Director.
(Presidente de la sesión)

_____
Lic. Luis Kenneth Sánchez Villalobos
Tribunal-Repres. Profesores
(Secretario de la sesión)

Derechos propiedad intelectual

Dedicatorias

Quiero dedicar este trabajo de manera especial a mis padres Miguel Alvarado Orlich y Mirna Rivera Araya, quienes han sido mis mentores, me han apoyado durante mi estudio y me han enseñado que mediante el esfuerzo y la constancia se pueden obtener todas las metas que se propongan, pero más importante me han dado su amor incondicional. De igual forma dedicarlo a mis hermanos Daniel y Sofía quienes siempre me han ayudado en todas las maneras posibles a lograr mis metas.

A los profesores de la Universidad de Costa Rica, quienes se han esforzado por enseñarme las bases para poder desarrollarme como profesional e inculcarnos los valores y principios de esta gran institución, pero en especial dedicado a nuestro Tutor Michel Angulo Sosa quien se ha esforzado por ayudarnos a completar este proyecto y a ser mejores profesionales. Y finalmente a mis compañeros por su dedicación y esfuerzo.

"Yo creo bastante en la suerte. Y he constatado que, cuanto más duro trabajo, más suerte tengo."-Thomas Jefferson

Carlos Esteban Alvarado Rivera

Dedico este proyecto a la Universidad de Costa Rica por formarme tanto como una mejor persona, así como un buen profesional. A todos los profesores, colegas y amigos que fueron participes en este proceso, ya sea de manera directa o indirecta que ayudaron a mi desarrollo.

Al amor incondicional de mi familia, especialmente a mis padres que fueron mis mayores promotores durante este proceso, al apoyo y motivación para cada día seguir adelante. A nuestro tutor Michel Ángulo Sosa, que sin su apoyo no hubiese sido posible la culminación del mismo.

"Al final no importa si las cosas no salen como queremos. Porque vale más tener cicatrices por valiente que la piel intacta por cobarde"
Bruce Lee

Olman Mata Mata

Primero doy gracias a Dios por la salud, la sabiduría y la paciencia que me dio para alcanzar la culminación de este proyecto.

Dedico a mi familia por el apoyo y los consejos, a mi padre que aunque ya no se encuentra a mi lado me guía y me da la fuerza desde el cielo, a quien debo mucho de lo que soy y por el cual estoy logrando esta meta. ¡Gracias papá!

Finalmente doy gracias a mis compañeros de proyecto por el compromiso y la responsabilidad en todo momento, a nuestro tutor Michel Angulo por su ayuda, su sentido crítico y sus bromas… ¡Gracias Profe!; y a los demás profesores que de una manera u otra han colaborado a lo largo de este proyecto.

"No existe una manera fácil. No importa cuán talentoso seas, tu talento te va a fallar si no lo desarrollas. Si no estudias, si no trabajas duro, si no te dedicas a ser mejor cada día"
-Will Smith

José María Vargas G.

Primero quiero agradecer a Dios, por todo lo que me ha dado y permitirme llegar hasta este punto de mi vida.

Agradezco a mi padre Héctor, quiero dedicarle que siempre con calma, paciencia y paz se logran las cosas, a mi madre Yorleny que me enseñó a no rendirme nunca, a mi hermana Giuliana quiero dedicarle que con esfuerzo y una actitud positiva cualquier meta es posible. A mis tíos y tías que siempre estuvieron ahí, a mis amigos más cercanos gracias por ayudar directa e indirectamente en este proyecto.

También a nuestro tutor Michel, sin su guía y su apoyo no podríamos haber finalizado el mismo. Y a todos mis colegas les dedico estas frases.

"El trabajo que nunca se empieza, es el que más tarda en finalizarse."
- J.R.R Tolkien

"No necesitamos de la magia para transformar nuestro Mundo. Ya todos llevamos todo el poder que necesitamos dentro de nosotros."
-J.K Rowling

Luciano Visoná Castillo.

Reconocimientos y Agradecimientos

Agradecemos a la Universidad de Costa Rica por la formación académica y humanista que nos ha brindado y permitido desarrollarnos tanto como profesionales en nuestro campo, como personas defensoras de los principios y valores que esta institución representa.

A la Fundación de la Universidad de Costa Rica nuestro profundo agradecimiento por brindarnos la gran oportunidad de desempeñar nuestro proyecto, así como el interés mostrado por el departamento de T.I. y por los jerarcas de la institución.

A todos los profesores que fueron parte de este proyecto y nos brindaron su pericia personal y profesional, en especial nuestro reconocimiento a nuestro tutor, Michel Angulo Sosa por su visión crítica y consejos a lo largo de este proyecto, a nuestro lector Gino Ramírez, por sus aportes y observaciones, y a nuestro lector John Rojas por su colaboración en nuestro trabajo.

Por último, queremos agradecer a nuestras familias, las cuales estuvieron dándonos su apoyo incondicional sabiendo que para lograr una meta se deben hacer sacrificios y que todo sacrificio tiene su recompensa.

Índice

Resumen Ejecutivo

Título: Propuesta de una metodología para la gestión de la seguridad y control de la información en Tecnologías de Información de fundaciones, con base en un análisis de la normativa vigente aplicable por la Contraloría General de la República y por el Consejo Nacional de Supervisión del Sistema Financiero para el sector regulado.

Estudiantes: Carlos Esteban Alvarado Rivera, Olman Mata Mata, José Vargas Guillén y Luciano Visoná Castillo.

El presente proyecto de investigación fue realizado con el propósito de brindar a las fundaciones, sociedades sin fines de lucro y empresas sin alguna regulación específica, una herramienta que les permita mejorar sus procesos de control y seguridad de la información. Lo anterior debido a la falta de normativas y supervisión en este campo, aunado a los cambios constantes en las tecnologías que traen consigo grandes retos en la protección de los datos, mejoras en los tiempos de respuesta y acceso a la información en caso de alguna eventualidad.

Con el fin de mejorar el control y la seguridad de la información, maximizar su gestión administrativa, así como minimizar los riesgos asociados a su operación y de rendición de cuentas, es que surge la tarea de elaborar una metodología.

Ahora bien, para el desarrollo de esta propuesta metodológica se llevaron a cabo ciertos pasos previos, que sirvieron para lograr el cumplimiento del objetivo principal antes descrito. Dichos pasos se muestran a continuación:

1. El entendimiento de la evolución de las fundaciones, su marco teórico en términos del uso y soporte de las Tecnologías de Información (TI) para la administración de la seguridad y el control de la información.

2. El estudio de la Fundación de la Universidad de Costa Rica para la Investigación (FUNDEVI) como fundación específica a la que se le propuso dicha metodología y la cual está anuente a poderla aplicar; aquí se abarca desde su marco de operaciones, su ámbito de acción y su desarrollo en términos de TI para la administración de la seguridad y el control de la información.

FUNDEVI fue considerada apta para formar parte de este proyecto, ya que es una fundación bien establecida con importantes funciones y beneficios que impulsan el progreso del país.

3. La realización de una encuesta a las cuatro fundaciones de las universidades estatales (FUNDEVI, FUNDATEC, FUNDAUNA Y FUNDAPREDI) con la finalidad de identificar y valorar cuál es el estatus y las áreas críticas que les compete en materia de la seguridad y control de la información dentro de las fundaciones.

Como resultado de las encuestas se identificaron congruencias y diferencias que podrían ser oportunidades de mejora abordadas mediante la aplicación de la metodología.

4. Se analiza y compara la gestión de la seguridad y tecnologías de la información según el marco regulatorio aplicable en el ámbito nacional.

Por un lado, la Superintendencia General de Entidades Financieras (SUGEF), mediante el acuerdo SUGEF 14-09, que mantiene una regulación estricta a las entidades que supervisa, aplicando obligatoriamente 17 de los 34 procesos del marco COBIT.

Por otro lado, la Contraloría General de la República (CGR) con sus *Normas Técnicas para la gestión y el control de las Tecnologías de Información*, obliga a los entes supervisados a mantener un estricto control de Tecnologías de Información y a mantener una adecuada gestión de los riesgos.

Con lo anterior se desarrolló la propuesta metodológica, que viene a convertirse en un instrumento esencial y de interés para las instituciones que requieran de procedimientos, planes de acciones para responder con mayores y mejores controles evitando que la información sea manipulada de manera no autorizada, sea errónea o se genere de manera incompleta afectando la toma de decisiones. En la misma se establecen buenas prácticas mediante una serie de procesos que se deben adoptar, los mismos son rigurosos pero a la vez permiten ser ajustados a las necesidades y características de cada entidad de acuerdo a su entorno.

Y es así como se logró la consecución de dicha propuesta metodológica con la que se pretende lograr la adopción de una cultura de control de la información que abarque a toda la organización y promueva una serie de iniciativas que servirán para el cumplimiento de sus objetivos organizacionales.

Palabras Claves: Propuesta metodológica, Control y Seguridad, Tecnologías de Información (TI), Superintendencia General de Entidades Financieras (SUGEF), Contraloría General de la República (CGR), Marco de COBIT, Fundación de la Universidad de Costa Rica para la Investigación (FUNDEVI).

Introducción

"Estamos atados a la tecnología. Renunciar a ella es muy difícil en el terreno personal [...] pero en el ámbito profesional, económico y de funcionamiento de la sociedad en su conjunto, es directamente impensable. Y esto conlleva enfrentarse a esos peligros que la acompañan." (Pérez, 2014, p 3.). Siendo uno de estos peligros la fuga, malversación y/o pérdida de la información.

Aún más, hoy cuando las organizaciones están optando por la digitalización de documentos, por distintas razones, pero que aun así conllevan los mismos riesgos. "…digitalizamos para la ampliación del acceso, la preservación y conservación, la reducción de costos, optimización físicamente del espacio de almacenamiento físico, la transformación de servicios o la recuperación de la información." (Gonzáles, 2007, p 1,). Añadiendo también un propósito de mantener toda la información en un mismo lugar, facilitando su acceso; lamentablemente no solo a los usuarios con acceso, sino también a terceros no autorizados. Es por eso que hoy por hoy toda organización, privada, pública, con lucro o sin lucro va a requerir de un plan de acciones para resguardar la información, ya que "...la pérdida de información sensible puede producirse accidental o malintencionadamente, pero, en cualquier caso, puede y suele acarrear un daño económico y de prestigio, afectando a la empresa y su marca asociada" (Berciano, 2014, p.1,). Pocas organizaciones saben cómo hacerle frente a la protección de la información y es aún menor el número de quienes tienen un plan preventivo, para mitigar el riesgo de la pérdida o filtración de la información.

La propuesta que se desarrollará en este proyecto va dirigida hacia las fundaciones, parte muy importante de toda sociedad actualmente, ya que, como dijo Alan D. Solomont, embajador de EEUU en España, en una entrevista para el periódico El País: "no podemos depender del gobierno para todo. Además, creo que es bastante claro que no puede hacerlo todo. Lo cual es totalmente cierto, y ya todo un movimiento se ha dado cuenta de esto."

(Aguirre, 2012, párraf. 4). Cansados de esperar una acción por parte del gobierno y con una necesidad que seguirá creciendo en la sociedad, es que nacen las fundaciones.

Estas organizaciones tienden a enfocar sus esfuerzos en el bienestar social de la humanidad.

> Dado que las fundaciones son independientes de los gobiernos, también tienen mayor libertad para asumir riesgos, para considerar programas que sólo darán sus frutos a largo plazo o para experimentar con organizaciones altamente descentralizadas. Los resultados de su experiencia pueden sugerir innovaciones de utilidad en el sector oficial, así como ofrecer advertencias acerca de consecuencias imprevistas. (Scott, 2004, p 11.).

Es decir las fundaciones como entes privados e independientes asisten las diferentes acciones del gobierno para atender las necesidades presentadas en la sociedad.

Con el fin de impulsar la investigación para generar un bien social como lo es la trata de enfermedades, apoyo a la educación, etc.; son inyectados miles de dólares en fundaciones. A modo de ejemplo la Fundación Bill y Melinda Gates es la mayor impulsadora en investigación medicinal y erradicación de la pobreza extrema en el mundo, habiendo destinado un monto aproximado a los 30.1 billones de dólares a estas y otras causas. (Fundación Bill and Melinda Gates, 2014)

Es en la unión de estos dos ejes, la seguridad de la información y las fundaciones, en que se basa este trabajo de investigación, ya que si bien toda fundación tiene que "presentar, por ley, un informe contable de las actividades de la fundación a la Contraloría General de la República" (Ley de las Fundaciones Número 5338, 1973) y que "en las fundaciones actuales el Estado debe velar además porque el patrimonio sea utilizado para la obtención del objetivo propuesto" (Centro de información jurídica, 2007, párraf.06), no existe un marco regulatorio dirigido directamente a las fundaciones, que dicte cómo

accionar, es decir no hay recurso alguno que ayude a las fundaciones a prevenir; es hasta que la Contraloría General de la República dicte que hay irregularidades que se toman acciones.

Esto está respaldado por el oficio, en respuesta al informe No-DFOE-SOC-1-2008 de fecha 01 de febrero del 2008, con título *Informe sobre los mecanismos de control establecidos por la Universidad de Costa Rica en la actividad de vinculación externa realizada con la coadyuvancia de la Fundación de la Universidad de Costa Rica para la Investigación (FUNDEVI).* En este se hace alusión a la Contraloría General de la República y su accionar sobre la FUNDEVI, el cual expone que:

> "por tratarse las fundaciones de sujetos de derecho privado, jurídicamente no deben sujetarse a nadie más que a la ley y a la Constitución Política, de ahí que al ser las fundaciones sujetos de derecho privado, la Contraloría General no puede unilateralmente imponer criterios, dar lineamientos o directrices concretas y, mucho menos órdenes" (Contraloría General de la República, 2009, p.6).

Por lo tanto, a pesar de que FUNDEVI está sujeto a la supervisión de la CGR, según el Artículo 15 de la Ley de Fundaciones, ésta sigue siendo un ente privado sin fines de lucro, por lo que no está obligado a acatar la normativa de dicha entidad.

Si bien, todas las fundaciones tienen aspectos diferentes a todas las une la misma condición, son de carácter privado, es decir, puede hacer todo aquello que no esté expresamente prohibido (Centro de información jurídica, 2007)). Por ende, la metodología propuesta en este trabajo para la gestión y control de la información en Tecnologías de Información es totalmente aplicable a otras fundaciones, dentro del territorio nacional.

En este trabajo se pretende comparar los diferentes marcos regulatorios y normativos del sector regulado costarricense contra la forma en que la Fundación de la

Universidad de Costa Rica para la Investigación, (FUNDEVI) realiza sus labores relacionadas con la gestión de la seguridad y control de la información. A partir de esta comparación se creará una metodología para que las diferentes fundaciones del país puedan aplicarla para mejorar la gestión y seguridad de la información.

Justificación

Actualmente existen muchas fundaciones que operan sumas importantes de dinero sin aplicar un marco regulatorio que les permita mantener una gestión de la seguridad y control de la información en Tecnologías de Información ideal, la falta de regulaciones en este tipo de entidades puede provocar riesgos potenciales y desfavorables como desfalcos, hurtos y estafas que terminen afectando su situación económica y comprometiendo el fin por el cual fue creada cada organización.

Es por esto que es necesario brindar una metodología a la cual puedan optar estas organizaciones, con el fin de mejorar el control y la seguridad de la información. Dicha metodología es importante porque coadyuvará a buscar la mejora en su gestión administrativa, minimizar los riesgos asociados a su operación y de rendición de cuentas.

El proyecto se aplicará en una organización sin fines de lucro como es la Fundación de la Universidad de Costa Rica para la Investigación (FUNDEVI), pero la metodología también podrá ser empleada por cualquier otra fundación que maneje recursos y no cuente con una regulación explícita.

Para la realización de este trabajo de investigación es necesario reconocer, analizar y adaptar los marcos regulatorios existentes a nivel nacional desde la óptica de control interno, riesgos, Tecnologías de Información y comunicación, así como su seguridad.

Como parte de los marcos regulatorios aplicables al sector regulado se encuentra el Acuerdo SUGEF 14-09 *Normas técnicas para la gestión y el control de las Tecnologías de Información* una amplia guía basada en COBIT, específicamente en la aplicación de 19 procesos que el CONASSIF considera esenciales para la adecuada gestión de las Tecnologías de Información; mientras que para el sector público se encuentran las *Normas técnicas para la gestión y el control de las Tecnologías de Información* donde se definen las diferentes características que deben tener los entes regulados por la Contraloría General

de la República para tener un adecuado control interno en esta área, y son estos dos marcos los que se utilizarán como puntos de comparación para la realización del proyecto.

Alcance

El alcance de este proyecto es la elaboración de una metodología para la gestión de la seguridad y control de la información que le permita a FUNDEVI u otras fundaciones mantener una adecuada administración de estos.

Esta metodología se elaborará a partir del estudio y análisis del marco normativo aplicable a las organizaciones que sean reguladas por las entidades de control estatal, y que sea adaptable a FUNDEVI. El fin de esta metodología es que se convierta en una herramienta valiosa para la gestión de la seguridad y control de la información y que agilice la identificación, evaluación y gestión de riesgos asociados.

El proyecto contendrá un análisis comparativo de los resultados obtenidos a partir de una encuesta que se realizará a las cuatro fundaciones de las universidades estatales costarricenses (FUNDEVI, FUNDATEC, FUNDAUNA Y FUNDAPREDI). Esta encuesta cubrirá temas relacionados con el manejo actual de la gestión de la seguridad y control de la información en las T.I. y del marco normativo que se aplica en el sector regulado. Este análisis comparativo estará enfocado desde la óptica de control interno que valorará cuáles de las regulaciones podrían adaptarse a las fundaciones para realizar una gestión eficiente y suficiente de la seguridad y control de la información.

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

Limitaciones

Una de las limitaciones que se encuentra es el escaso acceso a la información y documentación brindada por parte de los empleados de la fundación en el cumplimiento de los objetivos del proyecto. Para solucionar esta limitante, se buscará la colaboración del área administrativa para coordinar con el personal el acceso a la información.

Otra limitante es el tiempo con que cuentan en la fundación para brindar la atención a consultas y coordinar reuniones; esto debido principalmente a la numerosa lista de obligaciones que conforman sus operaciones diarias. La alternativa propuesta para solventar lo anterior se da a partir de un programa de trabajo monitoreado de manera constante y que se pueda ajustar al rumbo que vaya tomando el desarrollo del proyecto, además de una lista de requerimientos detallada, actualizada y en la cual puedan generarse observaciones relacionadas con la documentación o información que se solicite, eso sí, siendo controlada de manera mutua por la fundación y por los creadores del proyecto.

Además, existe la limitación de una no aceptación por parte de algunas de las fundaciones antes indicadas que formarán parte del proyecto, aparte de FUNDEVI (FUNDATEC, FUNDAUNA Y FUNDAPREDI). Podría darse una no colaboración con el desarrollo de la encuesta que se propone, la cual sirve como medio de recopilación de información para el desarrollo de la metodología señalada en los objetivos de este trabajo. Es por ello que de manera preventiva, se comunicará el objetivo del proyecto de manera amplia, se responderá a consultas y se mantendrá comunicación constante con éstas para obtener su colaboración.

Finalmente, debe considerarse como limitación la aprobación y aceptación de la metodología que se proponga posterior al análisis realizado y las investigaciones que por tiempo determinado se den en la fundación. El plan de acción para reducir el riesgo de que esto pueda darse, viene ligado al proceso de comunicación que se tenga con las personas directamente relacionadas en el desarrollo de este proyecto, así como las reuniones

previamente realizadas en donde se puntualizarían aspectos de interés, preferencias y orientaciones que FUNDEVI desearía priorizar y así tener una idea clara de sus necesidades y poder obtener un beneficio mutuo que es lo que se espera.

Objetivo General

Proponer una metodología para la gestión de la seguridad y control de la información en Tecnologías de Información mediante un análisis de la normativa vigente dictada por la Contraloría General de la República y por el Consejo Nacional de Supervisión del Sistema Financiero, orientada a las fundaciones para mejorar su gestión y minimizar los riesgos asociados a su operación.

Objetivos Específicos

1. Contextualizar la evolución de las fundaciones, su marco teórico en términos del uso y soporte de las Tecnologías de Información para administración de la seguridad y el control de la información.

2. Describir el marco de operaciones de FUNDEVI, su ámbito de acción y su desarrollo en términos de Tecnologías de Información para la administración de la seguridad y el control de la información.

3. Analizar y comparar la gestión operativa de FUNDEVI, mediante una evaluación que determine las debilidades en la identificación y valoración de la seguridad y el control de la información con los marcos regulatorios existentes con base en la normativa vigente aplicable para el sector regulado.

4. Desarrollar una metodología para la gestión de la seguridad y control de la información en Tecnologías de la Información, basado en el marco normativo aplicable en el sector regulado por la Contraloría General de la República y por el Consejo Nacional de Supervisión del Sistema Financiero, para ser aplicada por las fundaciones.

5. Formular y exponer las conclusiones y recomendaciones derivadas del resultado de la investigación.

Perspectivas teóricas

A continuación se desarrolla un marco teórico que tiene como finalidad dar una noción clara y fundamentada del proyecto, manteniendo en todo momento la orientación y el conocimiento necesario para ubicar al lector con respecto a todos aquellos términos relacionados e incluidos en el trabajo de investigación.

Uno de los temas importantes a considerar es el concepto de *riesgo* que según la Superintendencia General de Entidades Financieras, en el acuerdo 2-10 llamado: *Reglamento sobre Administración Integral de Riesgos*, se define como:

> La posibilidad de pérdidas económicas debido a eventos adversos. Entre otros riesgos, pero no limitados a éstos, las entidades financieras pueden enfrentar riesgo de crédito, riesgo de precio, riesgo de tasas de interés, riesgo de tipo de cambio, riesgo de liquidez, riesgo operativo, riesgo de Tecnologías de Información, riesgo legal, riesgo de reputación, riesgo de legitimación de capitales y riesgo de conglomerado. (Superintendencia General de Entidades Financieras, 2010). En pocas palabras, es la posibilidad de perjuicio

Es importante que las entidades reguladoras evalúen la administración de riesgos que realizan las organizaciones, por esto es que la SUGEF con el fin de tener una perspectiva clara de los riesgos de cada entidad, emite una calificación global para cada una de estas, compuesta por una calificación cuantitativa y por una cualitativa. La calificación cuantitativa consta de seis elementos sujetos a análisis denominados CAMELS, (Capital, Activo, Manejo o Gestión, Evaluación de resultados, Liquidez y Sensibilidad a riesgos de mercado, por su acrónimo en español).

La calificación cuantitativa contempla aspectos meramente financieros que se derivan de los módulos contables de la entidad, mientras que la calificación cualitativa contempla aspectos como planificación, políticas y procedimientos, administración de

personal, sistemas de control, sistema de información gerencial y Tecnologías de Información.

Como parte de este proyecto es necesario delimitar *los riesgos desde el punto de vista de Tecnologías de Información*, los cuales se definen como:

> La posibilidad de pérdidas económicas derivadas de un evento relacionado con el acceso o uso de la tecnología, que afecta el desarrollo de los procesos del negocio y la gestión de riesgos de la entidad, al atentar contra la confidencialidad, integridad, disponibilidad, eficiencia, confiabilidad y oportunidad de la información (Superintendencia General de Entidades Financieras, 2010).

Es por eso que en la actualidad todas las organizaciones (sin importar su industria) están expuestas a las amenazas de pérdidas o daños y deben valorar sus riesgos.

La *valoración de riesgos* se define como la "determinación de la frecuencia probable de la ocurrencia de un problema y del daño potencial si el problema llegara a ocurrir. Se utiliza para determinar el costo-beneficio de un control" (Laudon & Laudon, 2012, glos.06). Luego de determinar el valor del riesgo y el costo de los controles, se toma la decisión de mitigar, trasladar o aceptar estos. Este procedimiento es esencial en la seguridad y control de la información y debe realizarse. Es importante, por tanto, llevar un adecuado control de los riesgos asociados a las Tecnologías de Información, dado que estas son transversales a todos los procesos en organizaciones modernas.

Los *datos* se definen como "flujos de elementos en bruto que representan los eventos que ocurren en las organizaciones o en el entorno físico antes de ordenarlos e interpretarlos en una forma en la que las personas puedan comprender y usar" (Laudon & Laudon, 2012, p.15). El conjunto de estos datos, que por sí solos no tienen ningún significado al momento de procesarse dan como resultado la *información*, la cual se define

como: “datos que se han modelado en una forma significativa y útil para los seres vivos” (Laudon & Laudon, 2012, p.15). La propia información posee valor y las organizaciones estructuran sus operaciones de acuerdo con los sistemas informáticos que se diseñan para la creación, almacenamiento y transferencia de la misma. Es un activo importante para toda organización, por lo que es crucial su protección e integridad.

Las *Tecnologías de Información* se definen como “todo aquel hardware y software que necesita usar una empresa para poder cumplir con sus objetivos de negocio” (Laudon & Laudon, 2012, glos.13); Asimismo, en las normas técnicas para la gestión y control de las TI, elaboradas por la Contraloría General de la República se definen las Tecnologías de Información como el “conjunto de tecnologías dedicadas al manejo de la información organizacional. Término genérico que incluye los recursos de: información, software, infraestructura y personas relacionadas.”(Contraloría General de la República, 2007). Actualmente, la mayoría de organizaciones utilizan, en diferente medida, las Tecnologías de Información, ya sea para brindar servicios, controlar procesos, procesar datos y almacenar información, además de otras actividades relacionadas.

Es importante señalar que las acciones cotidianas tanto laborales como personales se facilitan mediante el uso de los sistemas de información, ya que han adquirido un rol fundamental en todos los ámbitos en que se desenvuelve el ser humano, desde las finanzas empresariales, la comunicación, la educación, la salud, etc. Es crucial el análisis de los sistemas de información para la valoración apropiada de un sistema de administración de riesgos, de la seguridad y control de la información en las organizaciones como tal; ya que es en este donde se encuentra definido el uso de los *recursos de Tecnologías de Información* que son, según indica la Contraloría General de la República de Costa Rica: “Aplicaciones, información, infraestructura (tecnología e instalaciones) y personas que interactúan en un ambiente de TI de una organización” (Contraloría General de la República, 2007).

Los *sistemas de información* se definen como "el conjunto de componentes interrelacionados que recolectan (o recuperan), procesan, almacenan y distribuyen información para apoyar la toma de decisiones, la coordinación, el control, el análisis y la visualización de una organización" (Laudon & Laudon, 2012, p.33). La efectividad de los mismos depende también del uso y controles que se designen para el usuario final, ya que este no es parte del sistema en sí, pero es quien omite procedimientos o los realiza incorrectamente a la hora de utilizar el sistema, convirtiéndose en una amenaza al diseño y propósito original, creando vulnerabilidades en el sistema con sus acciones.

La *vulnerabilidad* es "la situación creada, por la falta de uno o varios controles, con la que la amenaza pudiera acaecer y así afectar al entorno informático" (González, 2001, p.45). La importancia de una metodología apropiada para el control y seguridad de información radica en diseñar controles eficientes y suficientes para minimizar las vulnerabilidades.

Es por lo anterior que desde mucho tiempo atrás las organizaciones han visto la necesidad de buscar maneras con las cuales se pueda minimizar este tipo de riesgo, que principalmente puede traer consigo el no cumplimiento de las metas organizacionales. A raíz de esta preocupación nace un término importante por definir como lo es el control de la información.

El control de la información cumple un papel vital dentro de todo proceso organizacional. Por esta razón es difícil pensar en el desarrollo de las tecnologías de la información y el procesamiento de la información que estas brindan sin vincular el término *controles*, pues son estos los que permiten dar un grado de soporte a nivel de transparencia, exactitud, entre muchos otros. Por lo tanto, puede decirse que los controles de la información son aquellos que vienen a dar el surgimiento de la seguridad de la información.

Se define, según la Asociación Española para la Calidad, a la *Seguridad de la Información* como "aquella protección de la información y de los sistemas de la

información del acceso, uso, divulgación, interrupción o destrucción no autorizada" (Asociación Española para la Calidad, 2013, parráf.1).

La seguridad de la información se crea desde la parte logística, es decir, es importante para toda organización la creación de planes o procedimientos (ISACA, 2012). Éstos indican las acciones convenientes y necesarias con respecto a la manipulación y divulgación de la información entre departamentos y con terceros. Además, es clave el compromiso y la confidencialidad con los que cada empleado reacciona ante estas situaciones.

Son muchos los retos con los que se enfrenta la seguridad de la información, y en su mayoría se deben a la falta de inversión que se da en esta área (Ernst & Young, 2011). Los costos en los que se incurre para que las herramientas con las que cuentan se mantengan sólidas y actualizadas frente a las distintas amenazas que surgen a partir de la globalización son muy altos. Un proceso continuo de capacitación del recurso humano es otro factor en el cual se debe poner atención, pues en ocasiones la seguridad de la información no es la correcta debido al poco conocimiento y el número de errores que se dan desde el momento en que ingresan los datos, hasta que estos son suministrados a quienes los requieren para el desarrollo de sus tareas.

Es por eso que en la actualidad las organizaciones, específicamente en el área administrativa, han considerado importante vincular la seguridad de la información con aspectos que la fortalecen, entre ellos: la ejecución y control de responsabilidades, políticas en materia de buenas prácticas con el manejo informativo, entre otros. Se busca obtener el máximo cumplimiento en sus procesos y la culminación según los objetivos propuestos (ISACA, 2012). A partir de estas acciones surge lo que se conoce como el Gobierno de Tecnologías de la Información.

Un *Gobierno de TI* "es parte integral del gobierno corporativo y consiste en el liderazgo, los procesos y las estructuras que aseguran que las tecnologías de la organización apoyen los objetivos y estrategias de la empresa" (Comín, 2005, p.14).

El factor de su planificación es uno de los aspectos más complejos, y se debe a razones como el tipo de organización en que se implementará, el recurso técnico, económico y humano con el que se cuenta, así como el alcance y resultados que se desean obtener. Por otro lado, el monitoreo y seguimiento que se le dé posterior a su implementación es crucial para que no se desvíe el fin por el cuál fue puesto en marcha, pues de lo contrario se obtendrían resultados no deseados.

Son muchas las ventajas que se pueden obtener si las organizaciones logran establecer de manera adecuada y alineada el Gobierno de TI con los objetivos empresariales. Por ejemplo: "maximizando así los beneficios, capitalizando las oportunidades y ganando ventajas competitivas" (COBIT 4.1, 2007, p.5).

Los conceptos expuestos anteriormente deberían ser puestos en práctica en todas aquellas entidades reguladas en Costa Rica, sin embargo, existen entidades no reguladas como son las fundaciones y organizaciones sin fines de lucro que podrían beneficiarse con la aplicación de alguna metodología basada en este marco regulatorio.

Es importante tomar en cuenta que FUNDEVI, fundación en la cual se llevará a cabo este proyecto, no se encuentra dentro la regulación estatal. *Regulación* según la ARESEP se define como:

> …una forma de intervención pública, que restringe, influye o condiciona las actuaciones de los agentes económicos, obligando a las empresas a actuar conforme la ley y reglamentos… (ARESEP, 2012).

Por la naturaleza de sus actividades las *fundaciones*, según la Ley N°5338, son definidas como "…entes privados de utilidad pública, que se establezcan sin fines de lucro y con el objeto de realizar o ayudar a realizar, mediante el destino de un patrimonio, actividades educativas, benéficas, artísticas o literarias, científicas, y en general todas aquellas que signifiquen bienestar social." (Ley de las Fundaciones N°5338, 1973), cuentan con su propia ley y reglamento, estos regulan principalmente la forma de su constitución, manejo de las mismas y administración de los resultados financieros de sus actividades por ser entidades sin fines de lucro, como se mencionó en la definición anterior.

La Escuela de Leyes de la Universidad Cornell expone en uno de sus artículos que:

> Una organización sin fines de lucro es un grupo organizado con fines distintos de generación de resultados y en el que ninguna parte de los ingresos de la organización está distribuido a sus miembros, directores o funcionarios… pueden tomar la forma de una sociedad anónima, una empresa individual (por ejemplo, contribuciones caritativas individuales), asociación sin personería jurídica, asociación, fundación…" (Cornell University Law School, 2001, párraf. 01),

Dentro de la legislación costarricense sobre las actividades de las fundaciones se presenta en el Artículo Número 7 de la Ley Número 5338 lo siguiente: "Las fundaciones no tienen finalidades comerciales. Sin embargo, podrán realizar operaciones de esa índole para aumentar su patrimonio, pero los ingresos que obtengan deberán destinarlos exclusivamente a la realización de sus propios objetivos."(Ley N°5338, act.2001)

La labor realizada por el Consejo Nacional de Supervisión del Sistema Financiero y por la Contraloría General de la República se da con el fin de mejorar las transacciones de activos financieros y proteger la economía según la Superintendencia General de Valores; el sistema financiero costarricense "se rige por las legislaciones que regulan las transacciones de activos financieros y por los mecanismos e instrumentos que permiten la

transferencia de éstos entre ahorrantes e inversionistas, cumpliendo así una importante función en toda la economía". (Superintendencia General de Valores, 2010).

Por otra parte es importante definir el término *metodología*, parafraseando a Sabino (1996) en su obra *El Proceso de la Investigación*, la metodología no es más que una simple guía para las tareas cotidianas cuando surge una duda sobre qué hacer. En pocas palabras es el método para llevar a cabo ciertas acciones para un determinado objetivo. (Sabino, 1996)

Por esta razón, para el desarrollo de cualquier proyecto es necesario tener un plan a seguir, con objetivos establecidos y acciones que se deben realizar para lograrlos, este conjunto es lo que conforma una metodología. Adicionalmente, el autor Sabino dice que "ella es como un mapa que podemos consultar con provecho cuando nos sentimos perdidos, como una guía o referencia que nos puede ofrecer información, consejos de valor, hasta el estímulo que es necesario recibir cuando el éxito nos resulta esquivo". (Sabino, 1996, p.151).

Por otra parte Sabino afirma que: "para entender que la metodología no es un simple recetario, para quitarle su carácter manualesco, es preciso discutirla mientras se realiza investigación, en contacto con los problemas y las dudas que surgen durante el propio proceso de creación...". (Sabino, 1996, p.152). Por lo tanto hay que tener claro que la metodología va a ser una guía, pero no debe ser estática o rígida, pues debe irse modificando si quien la realiza lo considera pertinente, ya que probablemente lo que se había establecido anteriormente, hoy ya sea obsoleto, por esta razón hay que cuestionarla, discutirla con otros expertos y analizar si todavía sigue vigente.

Aunque existen muchas formas de hacer las tareas, hay técnicas para que estas sean ordenadas, eficaces, eficientes y demás. Según Alonso (2003), las técnicas son: "los procedimientos operativos rigurosos, bien definidos, trasmisibles y susceptibles de ser aplicados repetidas veces en las mismas condiciones". (Alonso, 2003). Por otro lado, Ackoff afirma que: "las técnicas [...] son maneras de usar las herramientas científicas"

(Ackoff, 1962 p. 42 citado en De la Mora, 2006). Sintetizando las dos definiciones se puede obtener como conclusión que las técnicas son instrumentos para ayudar aún más en las actividades a realizar, claro está que estas deben estar relacionadas con los objetivos por alcanzar.

Una vez planteado un objetivo es importante buscar las actividades idóneas para alcanzarlo, la mejor manera de hacerlo es mediante el planteamiento de una *estrategia*, que se puede definir como: "un curso de acción planeado para la ejecución de actividades claramente definidas y dirigidas hacia el fin de un objetivo previamente establecido" (De la Mora; 2006, p.47). Según esta definición hay que establecer objetivos antes de establecer actividades. El mismo autor menciona que una *actividad* "es un hecho determinado, que se debe de hacer en un tiempo determinado", mientras que un *objetivo* es "el resultado concreto de un proceso final que concluye y ha sido fijado como consecuencia de las alternativas que se tuvieron". Cabe destacar que un objetivo está conformado por varias actividades, pero una actividad no está conformada por varios objetivos. Al mismo tiempo es necesario recalcar que las actividades son dinámicas, es decir que denotan acciones, caso contrario a los objetivos que son estáticos, no denotan acción alguna. (De la Mora; 2006, p.47).

Metodología de la investigación

En este proyecto de investigación el medio para recolectar los datos se determina según el contexto de su fuente, ya sea primaria o secundaria, y va de acuerdo al desarrollo de cada uno de los objetivos anteriormente propuestos.

Para el cumplimiento del primer objetivo, se recolecta información de una fuente secundaria como la consulta en libros, leyes, normativas y otros materiales disponibles en internet. Con esto se pretende abarcar aspectos desde los orígenes y el desarrollo de las fundaciones, hasta su relación con las Tecnologías de Información, específicamente seguridad y control de la información.

Con el fin de alcanzar el segundo objetivo propuesto se recurre a las fuentes secundarias mencionadas anteriormente, además se toma en cuenta el material proporcionado por FUNDEVI, como documentación interna, políticas, reglamentos, procedimientos, bitácoras y demás documentos o en materia de sus operaciones, Tecnologías de Información, seguridad y controles. Por otra parte se emplean fuentes primarias como entrevistas a los colaboradores de la fundación para cubrir lo necesario en dichos temas. Con lo anterior se recaba información en materia de las operaciones de la FUNDEVI, la aparición, vinculación e influencia de las Tecnologías de Información en la seguridad y control de la información como fuente importante para la consecución de las metas o fines de una institución.

En lo que respecta al objetivo tres, se recolecta la información a través de material proporcionado por FUNDEVI (documentos o entrevistas) en materia de sus operaciones, Tecnologías de Información, seguridad y controles; así como por medio de una encuesta, fuente primaria creada como parte del proyecto, (Anexo # 1), la cual va dirigida a instituciones no lucrativas similares a FUNDEVI. Se desea analizar y comparar operativamente a FUNDEVI con respecto a otras entidades de su mismo sector, con el fin de conocer los pros y contras para un mejor desempeño en las áreas relacionadas. Así

mismo, se procede a realizar un análisis comparativo de las normativas que rigen para el sector regulado del país; esto con el fin de tener una claridad y base que permita obtener mayores herramientas para la ejecución del próximo capítulo.

Para el objetivo cuatro se recopila información de una fuente primaria a través de lo recabado en la encuesta; el proceso de tabulación, comparación y criterios se hará considerando la normativa aplicable y contrastada con la realidad de las fundaciones investigadas en los capítulos anteriores, manteniendo el objetivo principal de este trabajo. El fin que se desea lograr es una metodología que permita evaluar y administrar de manera eficaz y eficiente la seguridad y el control de la información en Tecnologías de la Información.

. Para el cumplimiento del objetivo cinco se toman en cuenta todas las fuentes de información expuestas en los párrafos anteriores, a partir de los resultados obtenidos se llega a las conclusiones y se sugieren las recomendaciones que tienen como fin mejorar la gestión de la seguridad y control de la información en Tecnologías de Información de las fundaciones desde una administración eficiente y eficaz en este departamento.

Son diversos los recursos que intervienen para la ejecución de este trabajo, el complemento y la adecuada vinculación serán la clave para que la metodología antes descrita se desarrolle según lo planteado.

Capítulo I. Desarrollo de las fundaciones como organizaciones no lucrativas y contextualización del uso de las tecnologías de información en el ámbito organizacional costarricense.

Las fundaciones en la actualidad se han convertido en importantes entidades de colaboración y apoyo para la sociedad. Cabe señalar que actualmente la consolidación organizacional y financiera, en muchas de ellas, tanto a nivel nacional como internacional, son resultado del esfuerzo, el recurso económico y el fin por el cual fueron creadas.

La base de lo indicado en el párrafo anterior es el ejemplo del Fondo de las Naciones Unidas para la Infancia (UNICEF), pues se ha convertido en una organización que ayuda a los niños desde hace muchos años. Hoy, UNICEF "cuenta con un personal integrado por más de 7.000 personas que cumple funciones en 57 países y territorios del mundo, en áreas de educación, deporte, salud, ayuda humanitaria, entre otros". (UNICEF, 2015, párraf 2).

1.1 Evolución de las fundaciones en el mundo.

Muchas instituciones de beneficio social en el mundo no hubieran llegado a formarse sin la ayuda de movimientos históricos, en donde grupos de apoyo, buscando beneficios por un bien común, lucharon contra aquellos sectores que se oponían y lograron que se les diera la importancia correspondiente. Las fundaciones son instituciones que toman fuerza día a día.

No está de más puntualizar que una fundación, según describe Pérez (2002) especialista en constitución y gestión de fundaciones, es "… como la personificación de un fin: por esto no tiene socios ni miembros y existen en cuanto persista un fin." (Pérez 2002, párraf. 1).

Ahora bien, desde sus inicios las fundaciones reflejan los ideales de sus fundadores y en todo momento se busca el cumplimiento de los objetivos establecidos. Para tener mayor claridad y fundamento de lo antes señalado es importante citar lo que el escritor y analista Valero (1969) dice en su obra *La Fundación como forma de Empresa*, puesto que se evidencia la creación de tres niveles en el desarrollo de las fundaciones, iniciando por el Derecho Romano, luego el Derecho Medieval y seguidamente la Edad Media.

El Derecho Romano nace en el período del Imperio Romano con el reconocimiento de la Iglesia por el Estado y el apoyo de ésta en la promoción del amor por el prójimo, el destino de bienes para tal fin y en favor del pueblo.

En esta etapa del proceso de desarrollo de las fundaciones se impulsan dos eventos claves y ubicados en el Derecho Público:

Uno fue, y según Valero (1969) señala:

> "la conexión insoluble de tales establecimientos y liberalidades, con la realización de fines benéfico-sociales por su medio, ya que la consideración de este tipo de fines, es precisamente lo que conduce a la eliminación de disposiciones concretas que impedían tal forma de actuar, o la asimilación del trato jurídico de las nuevas figuras o instituciones anteriores… (Valero, 1969).

Así mismo, este autor consideraba que un evento clave fue la administración de las fundaciones en su mayoría manejadas por la iglesia, quedaba a cargo de los funcionarios eclesiásticos designados y supervisados por el obispo.

Para esa época la influencia y el poder de decisión que llegó a tener el sector eclesiástico, en especial a los ojos del Estado, vino a convertirse en un logro fundamental para el desarrollo y el origen de los diferentes movimientos que empezaron a darse por el

mundo. Anteriormente, cualquier sector manifestante de proclamación hacia una sociedad más caritativa y con fines por un bien en común era casi nulo; ya que cualquier expresión de este tipo venía a traer consecuencias negativas para sus fundadores.

Finalmente, se empieza a conocer un cambio importante en el desarrollo social, que aunque el poder era centralizado en la Iglesia, se buscaba en gran manera que ésta sirviera como canal para llegar a los sectores de necesidad y con limitaciones notorias.

Para el siguiente nivel, y es en donde inicia el Derecho Medieval, se empieza a dar una variación de la definición y el fin de las fundaciones, ya que se inicia la separación de este tipo de organizaciones con la Iglesia; a raíz del surgimiento de entidades privadas que establecieron instituciones benéficas y con auténtica propiedad sobre ellos. Eso sí, la iglesia se mantuvo al tanto del cumplimiento de los fines de estas nuevas entidades privadas que patrimonialmente se encontraban bajo el mando del fundador.

Ya para el siglo XII, la Iglesia emprende su lucha contra las organizaciones propias. Valero (1969) hace mención de lo importante que fue el Derecho canónico medieval para la Iglesia en este proceso, él dice:

> "… empieza por recoger como principio básico, la norma de que la voluntad del fundador debe ser respetada en cualquier circunstancia. Así mismo, este Derecho fija las medidas necesarias para garantizar la voluntad del fundador y la exigencia de la intervención de la autoridad eclesiástica para su creación, así como la exclusiva retribución para suprimir, agregar o segregar fundaciones. Además, reconoce a la fundación autónoma como persona jurídica y en haber profundizado notablemente en la naturaleza propia de la persona jurídica institucional" (Valero, 1969).

Ahora bien, a pesar de que la Iglesia en esta época mantenía un poder importante en la administración y control de estos movimientos en beneficio de la sociedad, se empieza a

observar un fuerte ideal que pretende liberarse de éste para surgir como un grupo de carácter privado e independiente en busca de sus objetivos.

Ya para la etapa de la Edad Media se comienzan a transformar las fundaciones, hasta ahora eclesiásticas, en instituciones autónomas, ajenas a las regulaciones de la Iglesia. Con ello el proceso de gestión y sus finalidades dejaron de ser exclusivamente de carácter religioso y empezaron a proyectarse a otras áreas del sector social.

El Estado empezó a intervenir en el destino de bienes a perpetuidad a las fundaciones, por miedo al poder económico que estas organizaciones pudiesen ir adquiriendo. Luego el Estado se enfocó por la ayuda social y el bienestar de los necesitados como consecuencia de su intervención y las fundaciones empezaron a preocuparse por tener utilidad de las actividades que llevaban a cabo.

Como se puede ver, las organizaciones privadas lograron su independencia y se les dio el derecho de trabajar por un bien propio y establecido; cabe señalar que a raíz de las transformaciones que se dieron en las etapas antes señaladas, siempre se mantuvo la búsqueda por un bien común y el desarrollo de la sociedad.

La evolución que han tenido las fundaciones a lo largo del tiempo y a nivel global, ayudaron de manera considerable en el bienestar y la colaboración social.

Para Pérez (2002) “El origen de las fundaciones es muy antiguo y casi infinitas sus variedades. Donde hay más libertad, hay más liberalidad y más facilidad para su constitución y actividades. Así en el ámbito anglosajón el campo de las fundaciones supone un volumen muy alto de actividad económica”. (Pérez, 2002, párraf. 4).

Es difícil poder describir de manera minuciosa toda la evolución en las últimas décadas, pues son muchos los acontecimientos que se han dado a raíz de la búsqueda y el

cumplimiento de los objetivos fundacionales. Pero se fijarán situaciones importantes que se han presentado.

Entre ellos, para finales del siglo XIX e inicios del siglo XX, Andrew Carnegie y John D. Rockefeller impulsaron la creación de las fundaciones privadas con la creencia de que el ciudadano y la riqueza final es privada, y que son fundamentales para crear un bienestar público, al igual que sus convicciones religiosas, esto según comenta Joan E. Spero en su artículo *Global Philanthropy and Global Governance the role of U.S. Private and Corporate Foundations in Improving the Human Condition* (Spero, 2014).

Para ellos dos, estas instituciones tenían el objetivo de mejorar la sociedad tratando la raíz de los problemas sociales, como por ejemplo: la pobreza, la hambruna y la enfermedad.

Ahora bien, puede citarse que para el siglo XX se enfrentaron situaciones críticas, puesto que los recursos eran limitados y el sector bancario carecía debido a la crisis de 1929. Sin embargo, para los años 1940 y 1950 se dio un repentino crecimiento puesto que los donantes preferían aportar los fondos a las fundaciones y no a los fideicomisos bancarios de ayuda filantrópica.

En el año 1970 se dio un cambio en la Ley de Reforma Fiscal de los EEUU, a partir de ello estas instituciones recibieron un trato especial en categoría de instituciones de beneficencia pública. Ante esta situación decreció el ataque en el que se encontraban porque estaban exentas de impuesto sin ninguna regulación.

Desde el año 2000 en adelante, el desarrollo de las fundaciones ha sido más notorio en diversos sectores del mundo. Por ejemplo, en los Estados Unidos de América, gran impulsador y pionero de las fundaciones, ya que por muchas razones históricas y culturales han recurrido a las organizaciones sin fines de lucro, incluidas las fundaciones, para proveer servicios públicos y equilibrar el poder del gobierno y los negocios.

La evolución y alto desarrollo de las fundaciones en este país de América del Norte se debe en primer lugar a su tamaño y experiencia; las fundaciones tienden a empezar localmente y a extender su alcance geográfico a medida que sus recursos y experiencia aumentan.

Por otro lado, en el sector europeo su desarrollo se dio de manera más lenta durante el siglo XX, debido a las diferentes situaciones:

> La raíz es obviamente la ruptura económica y el empobrecimiento que produjeron las dos guerras mundiales y la depresión, que arruinó muchas fortunas familiares. En la segunda mitad del siglo, las condiciones fueron más estables y prósperas y las fundaciones resurgieron. Pero su tamaño y ámbito de actuación están limitados por el relativamente alto nivel de presión fiscal. (Scott, p.36, 2003).

Cuando las fundaciones maduran pueden extender su alcance geográfico. Muchas de las fundaciones activas hoy en el mundo comenzaron con actividades locales para luego extender sus fines u objetivos a otras regiones. Por tanto, pueden llevar a cabo programas de donación o apoyo institucional a sectores en vías de desarrollo o diezmados por diferentes situaciones como guerras, situaciones políticas, entre otros.

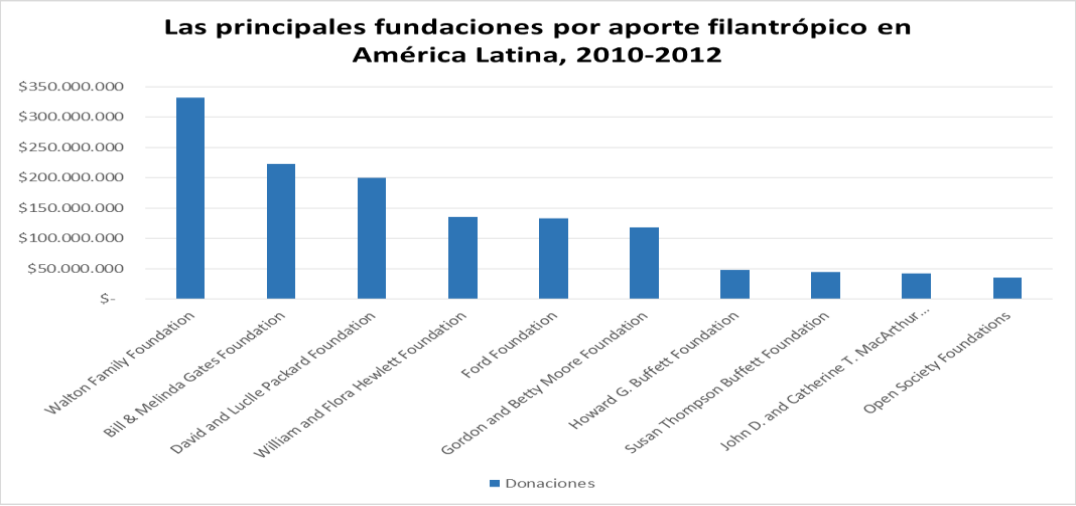
Ejemplificando lo antes señalado, se puede mencionar que en la actualidad la visión de muchas fundaciones es a nivel macro. Ya los aportes de las grandes fundaciones son más notorios en sectores en desarrollo, tal es el caso de las fundaciones creadas en los Estados Unidos y el apoyo que están dando a Latinoamérica.

Según la investigación realizada por Foundation Center (fuente de información en materia de actividad filantrópica a nivel mundial) en apoyo con la Seattle International Foundation:

> Entre 2007 Y 2009, 319 fundaciones estadounidenses otorgaron aportes filantrópicos para América Latina por $1,7 mil millones. Estos donativos fueron destinados a organizaciones en América Latina, así como a organizaciones ubicadas en los Estados Unidos y en el extranjero con programas internacionales dirigidos a la región. Este total refleja el 9,8 por ciento del total de dólares con enfoque internacional otorgados por fundaciones estadounidenses. (Foundation Center, 2014, p.04).

De lo anterior, cabe señalar el desempeño de diez principales fundaciones por los aportes que realizaron durante este período en América Latina. Entre ellas es importante mencionar a *Walton Family Foundation* que donó US$332 millones, lo cual en un gran porcentaje fue aportado al fondo perpetuo de su programa de becas internacionales. Este programa financia becas para alumnos de Centroamérica y México que deseen estudiar en universidades de Arkansas. Otra fundación a resaltar es la de *Bill & Melinda Gates Foundation*, la cual donó US$223 millones del 2010 al 2012, dinero que ha sido destinado a diferentes áreas de colaboración, desarrollo y bien social.

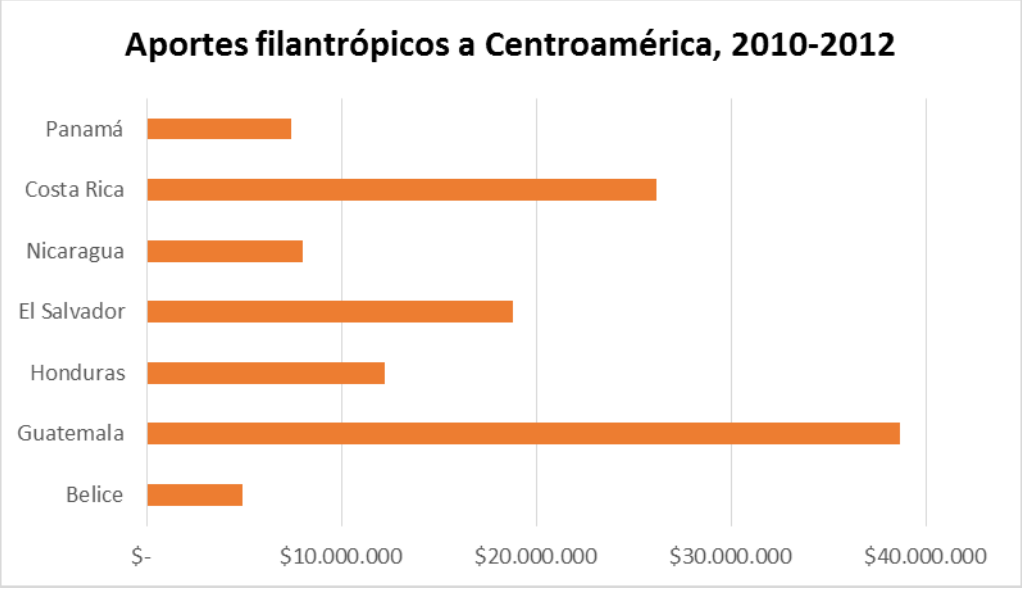
Cuadro No. 1 Aportes filantrópicos en América Latina, 2010-2012



Fuente: Foundation Center 2014, datos de los aportes basados en donativos de $10,000 o más proveniente de 1,000 de las fundaciones más grandes de Estados Unidos.

Específicamente para Centroamérica, entre el año 2010 y 2012 se dieron aportes importantes a manera de donativos para dicha región. Estos aportes llegaron a colaborar en programas y actividades de beneficio social. La asignación del total de estos fondos destinados fueron otorgados según indica Foundation Center de la siguiente manera: "el cuatro por ciento (US$20,4 millones) a 85 organizaciones con sede en Centroamérica. Ochenta y cinco organizaciones en Centroamérica recibieron 161 aportes filantrópicos por un total de US$20,4 millones. Esto representa el 4,5 por ciento de todos los fondos otorgados para organizaciones en América Latina" (Foundation Center, 2014).

Cuadro No. 2 Aportes filantrópicos a Centroamérica, 2010-2012



Fuente: Foundation Center 2014, incluye donativos otorgados a organizaciones de Centroamérica para su labor en la región u otras partes del mundo, así como a organizaciones en el extranjero con programas internacionales en la Centroamérica.

Las fundaciones como organizaciones no lucrativas a lo largo del mundo han podido salir adelante debido al apoyo económico que han recibido y a la colaboración de organizaciones de su mismo sector, sin embargo, ha sido complicado obtener los recursos que permitan fortalecer sus principios y cumplir con fines establecidos.

Así lo indica Balbis (2001) (investigador en el Centro Latinoamericano de Economía Humana de Montevideo, Uruguay) en un documento creado para el Programa *Gestión de las Transformaciones Sociales* de la UNESCO titulado: *ONGs, Gobernancia y Desarrollo en América Latina y el Caribe*, que: "las ONGs enfrentan problemas de identidad y subsistencia financiera que pueden llegar a modificar su tradicional rol crítico del orden social vigente y reducir su capacidad de formular propuestas alternativas" (Balbis, 2001, p.33).

Cabe señalar que el destino que tengan los recursos entregados a muchas fundaciones causa que los donadores piensen y analicen varias veces para donar. Y es válido que se dé esto; ya que existe el riesgo potencial de que el dinero percibido pueda ser usado para beneficios propios (ya sea de los fundadores o sus colaboradores) y no para el desarrollo en áreas a nivel social como la salud, la educación, la nutrición, entre otros.

En la actualidad han surgido mecanismos que colaboran enormemente para que esta incertidumbre disminuya y se logre una mayor claridad en el buen funcionamiento y cumplimiento de metas por parte de las fundaciones. Tal es el caso de un sello de acreditación creado por la Fundación Lealtad, especializada en la auditoría a organizaciones no lucrativas, lo otorgará a aquellas fundaciones que cumplan con los nueve principios de transparencia, buenas prácticas y eficacia en la gestión alrededor del mundo.

La directora general de la fundación, Patricia de Roda indica: "No es una certificación oficial. Pero después de 15 años analizando ONG damos el paso de crear un distintivo para dar crédito de que una entidad cumple con la transparencia, con su misión y es, además, eficaz en el uso de los fondos". (Diario El País, España, 2015).

1.2 Evolución de las fundaciones en Costa Rica.

La creación de las fundaciones en Costa Rica se da en el período de la Colonia, en donde los habitantes de la ciudad de San José vieron la necesidad de abastecer y suministrar a los aborígenes de educación y catequización, lo cual fue posible a través del dinero que donaban las personas con el recurso suficiente para hacerlo.

Si bien es sumamente importante la educación en cualquier población, nada puede hacer un pueblo educado sin salud. Ya que el estado del desarrollo de la salud y la medicina antes del siglo XX era deficiente, además debido a la pobreza del país existían altas tasas de mortalidad infantil y general por las infecciones. Según Carmona (1994), no habían hospitales con médicos o servicios médicos sistematizados que atendieran a la población durante la Conquista y la Colonia. Esta deficiencia es la que promueve un movimiento humanista, buscando siempre el bienestar social. Por lo que, se iniciaría el desarrollo de las organizaciones sin fines de lucro en el país.

Según el sociólogo William Reuben (1999), para el año 1845, el Dr. José María Castro Madriz, quien posteriormente sería el primer presidente de Costa Rica, presenta a la Cámara de Diputados el proyecto del establecimiento de una organización que se encargaría del manejo del futuro Hospital San Juan de Dios; sentando así la base para la primera organización sin fines de lucro en el país. Seguidamente, otras organizaciones como fueron las organizaciones parroquiales de Damas de Caridad y Damas Vicentinas, seguirían los pasos humanistas del Dr. Castro Madriz.

Esta primera organización sería la Junta de Caridad, que posteriormente se llamaría Junta de Protección Social de San José. Como se mencionó anteriormente, la obligación humanista impulsadora de este movimiento es lo que motivó al benemérito, quien diría ante la Cámara: “Vengo hoy a proponer el cumplimiento de una de nuestras más exigentes obligaciones: el establecimiento de una casa pública de caridad para socorrer a los enfermos...” (Carmona, 1974)

Para demarcar una línea de tiempo, una de las primeras ONG internacionales en Costa Rica es la Cruz Roja (también conocida como el Movimiento de la Cruz Roja y de la media Luna Roja), la cual fue constituida en Ginebra, Suiza en el año 1863. La misma fue fundada para tiempos de guerra en 1885, pero fue disuelta al término de la Intentona de Barrios. No fue sino hasta el año 1921 que se establece su funcionamiento, no solo en tiempos de guerra sino también en tiempos de paz, sentando las bases para la institución actual.

A finales del siglo pasado surgieron dos instituciones, las cuales actuaban de hecho y no de derecho, lo que les trajo problemas legales, pues en Costa Rica no existía un régimen jurídico al respecto. Estos entes fueron: La Institución Barroeta y el Hogar de Ancianos Alfredo y Delia González Flores; las cuales por las limitaciones antes mencionadas se tuvieron que regir única y exclusivamente por medio de su acta constitutiva.

Continuando con los inicios de las fundaciones, en el año 1973 la Asamblea Legislativa en Plenario, traslada a la Comisión de Asuntos Jurídicos un proyecto de ley con el fin de darles carácter de personas jurídicas privadas y con fin de bienestar público a las fundaciones. Es a partir de ello que se buscaba acabar con los problemas legales que estas instituciones habían tenido en el pasado. En resumen lo que el proyecto presentado indicaba era que se iba a describir a las fundaciones como personas jurídicas no estatales pero con fines de beneficio y bienestar social, más no lucrativas.

Finalmente, el presidente de la Asamblea Legislativa Luis Alberto Monge A, envía al Poder Ejecutivo el día 9 de agosto de 1973, para su ejecución y publicación, la Ley No.5338 denominada Ley de las Fundaciones.

Es importante recalcar lo que indica el Artículo No.1 de dicha ley; el cual provee un marco para la figura, así como una idea de sus fines y objetivos. Ya que este artículo dispone lo siguiente:

> Reconoce personalidad jurídica propia a las fundaciones, como entes privados de utilidad pública, que se establezcan sin fines de lucro y con el objeto de realizar o ayudar a realizar, mediante el destino de un patrimonio, actividades educativas, benéficas, artísticas o literarias, científicas, y en general todas aquellas que signifiquen bienestar social.(Ley de las Fundaciones, 1973).

Ya para los años ochenta se dieron varias situaciones en el país que influyeron negativamente en su desarrollo, como el alza de los precios de los productos básicos que aumentaron significativamente en un periodo corto de tiempo, dado que la inflación superó el 80% lo que ocasionó una crisis económica y generó problemas severos en el crecimiento del nivel de la sociedad, tales como el aumento del desempleo y la proporción de pobres en la población, la inestabilidad del tipo de cambio de moneda extranjera y el crecimiento de la deuda pública. Para contrarrestar esto, uno de los medios utilizados para lograr impulsar la reestructuración fue la estimulación de la participación de organizaciones no gubernamentales como las fundaciones, éstos a favor de procesos de gestión de servicios dirigidos a diferentes grupos sociales.

En la actualidad son muchas las fundaciones que colaboran en favor de la sociedad a nivel nacional. Tal es el caso de las cuatro fundaciones que fueron creadas por las universidades públicas de Costa Rica, las cuales han brindado un gran aporte como se verá a continuación:

1. Fundación de la Universidad de Costa Rica para la Investigación (FUNDEVI): Creada en 1988 como un mecanismo para la promoción y gestión de los proyectos de investigación de la Universidad de Costa Rica. Orienta sus prioridades a la organización de eventos académicos y fortalecimiento en áreas operativas. Adicionalmente, procura reforzar las alianzas con las organizaciones internacionales, tanto gubernamentales como privadas, buscando canalizar mejor los recursos que tiene y los que son resultado de donaciones.

Para el año 2014, la Cámara de Industrias de Costa Rica reconoce con el Premio Oro en el Programa a la Excelencia de la Cámara de Industrias de Costa Rica. Este premio obedece a la gestión eficiente en donde reconoce a organizaciones que sobresalen en sus respectivos campos, impulsan el mejoramiento continuo y dan aporte de importancia en beneficio de la sociedad.

2. Fundación para el Desarrollo Académico de la Universidad Nacional (FUNDAUNA): Creada en el 2003 como una institución privada sin fines de lucro y en apoyo a la gestión financiera de los proyectos de la Universidad Nacional de una manera transparente, ágil y en servicio excelente a la sociedad. Adicionalmente, incentiva la captación de recursos a través de la cooperación nacional e internacional para el fortalecimiento académico de la Universidad Nacional y en pro del bien social. Para el año 2012, la Cámara de Industrias de Costa Rica le reconoce con los premios en la categoría de liderazgo y planificación estratégica e innovación y tecnología a FUNDAUNA por su excelente gestión en esos temas y su crecimiento desde su creación.

3. Fundación Tecnológica de Costa Rica (FUNDATEC): Creada en 1987 con la idea de ampliar y mejorar los servicios que imparte el Instituto Tecnológico de Costa Rica (TEC) a diferentes sectores de la sociedad. Encargada de la gestión de los servicios ofrecidos a terceros en temas de facilidad de trámites, gestiones financieras y así haciendo posible las actividades de vinculación; todo lo anterior a través del apoyo de los recursos profesionales e infraestructura que el TEC le pone a disposición. Adicionalmente brinda a la sociedad bienes y servicios científicos y tecnológicos, asesorías, laboratorios, desarrollo e investigación tecnológica, entre otros.

4. Fundación de la Universidad Estatal a Distancia para el Desarrollo y Promoción de la Educación a Distancia (FUNDEPREDI): Creada en el año 2000 como una

> entidad privada y sin fines de lucro con la finalidad de apoyar, promover y facilitar la gestión de los proyectos académicos a partir de actividades de vínculo remunerado de la Universidad Estatal a Distancia (UNED). Esta fundación ofrece servicios bajo una gestión ágil, oportuna y responsable en áreas técnicas y administrativas a todas las instituciones ligadas a los proyectos de investigación, docencia, producción, desarrollo tecnológico, consultorías, entre otros.

Adicionalmente, y con la finalidad de fortalecer estas cuatro instituciones en materia del cumplimiento de sus objetivos, maximización de recursos, valores y expansión en pro del bienestar social, se firmó en junio del 2009, el *Acuerdo de vinculación y cooperación entre FUNDEVI, FUNDAUNA, FUNDATEC Y FUNDEPREDI*, el cual establece:

> La colaboración conjunta en el desarrollo de las actividades, proyectos y actuaciones pertenecientes a líneas de trabajo, comunes que lleven a alcanzar objetivos que reviertan en beneficios mutuos, en apoyo a las Universidades estatales en los campos de la docencia, investigación, transferencia del conocimiento, vinculación externa remunerada y en acción del bienestar social (Acuerdo de vinculación y cooperación entre FUNDEVI, FUNDAUNA, FUNDATEC Y FUNDEPREDI, 2009).

También el apoyo y la colaboración de fundaciones internacionales a nivel nacional ha tenido un aporte significativo para la sociedad; tal es el caso de:

UNICEF Costa Rica: la cual se crea basándose en el aporte de vacunas y suministros de salud básica para el país. En la actualidad, trabaja con el Estado, las ONG y la sociedad, centrándose en la adolescencia y los niños. Sigue desarrollándose con la construcción de programas sociales como el Desarrollo de la Primera Infancia, Cantones Amigos de la Infancia, Protección de la infancia, Educación de calidad, Prevención de VIH y sida, entre otros.

Fundación Ana Ross: nace bajo apoyo psicosocial de las personas con enfermedad de cáncer. Preocupados por el proceso de esta dura enfermedad tanto para la persona que la tiene como para sus familiares directos. En la actualidad, sus objetivos se han enfocado de manera más global, puesto que su fin es el mejoramiento de la situación integral del cáncer en nuestro país.

Fundación Costa Rica-Canadá: ésta fundación mantiene a lo largo de los años la visión de sus fundadores. Ha logrado una expansión y desarrollo importante en sus finalidades de bienestar social, en las relaciones de ambos países y en la consolidación de sus procesos. Sus objetivos tienen como pilares importantes el apoyo a las PYMES, la reducción en sectores de extrema pobreza y estado precario, el impulso a la vivienda, entre otros.

Con esto se llega a la conclusión de la importancia de la introducción de las fundaciones a nivel nacional, lo cual ha generado un impacto positivo a través de la historia para el desarrollo social y cultural del país.

1.3 Teoría y aplicación de las Tecnologías de Información para la administración de la seguridad y el control de la información en el sector regulado.

El ámbito regulado se puede segmentar en dos grandes ramas, las cuales son las entidades reguladas por el Consejo Nacional de Supervisión del Sistema Financiero (CONASSIF) el cual es un órgano colegiado de dirección superior, cuyo fin es la supervisión del Sistema Financiero Costarricense. Y aquellas entidades reguladas por la Contraloría General de la República que es el órgano constitucional auxiliar de la asamblea legislativa que supervisa el uso de los fondos públicos.

1.3.1 Ámbito regulado por el Consejo Nacional de Supervisión del Sistema Financiero.

El CONASSIF se creó en el año de 1997 y es el ente encargado de velar por la supervisión que realiza la Superintendencia General de Entidades Financieras (SUGEF), la Superintendencia General de Valores (SUGEVAL), la Superintendencia General de Seguros (SUGESE), y la Superintendencia General de Pensiones (SUPEN); además de aprobar la normativa aplicable a las entidades supervisadas por dichas superintendencias.

Por ende la normativa del CONASSIF cubre bajo su control a todas las entidades que realicen actividades de intermediación financiera dentro del territorio nacional, entidades que participen en el mercado de valores, de fondo de pensiones y de seguros.

En el ámbito de Tecnologías de Información la Superintendencia General de Entidades Financieras mantiene una regulación estricta a las entidades que supervisa, esto mediante el acuerdo SUGEF 14-09 aprobado por el Consejo Nacional de Supervisión del Sistema Financiero en el año 2009 que obliga a estas organizaciones a aplicar el reglamento sobre la gestión de las Tecnologías de Información.

La normativa anterior ha sido aprobada para la SUGEF, esta superintendencia supervisa 53 entidades, entre bancos, financieras, organizaciones cooperativas, entre otras (Superintendencia General de Entidades Financieras, 2016).

El manual pretende mejorar la administración del riesgo tecnológico que requieren las entidades financieras y se realiza aplicando obligatoriamente 17 de los 34 procesos del marco COBIT (los cuales serán mencionados más adelante) que serán revisados tanto por un auditor externo que deberá emitir su criterio anualmente como por miembros de la Superintendencia.

Dicho manual se basa en el cumplimiento de los objetivos definidos en el marco COBIT, los cuales son:

- Alineación Estratégica.
- Administración del Riesgo de TI.
- Entrega de Valor.
- Gestión de Recursos.
- Medición del Desempeño de TI.

El reglamento obliga a las entidades supervisadas a tener un comité de Tecnologías de Información para asesorar y coordinar a la administración en la gestión de los riesgos tecnológicos. Este comité debe estar conformado por un director propietario, el gerente general de la entidad, responsable del área informática y responsable de la función de riesgos de la entidad, el mismo tiene la responsabilidad de cumplir con las siguientes funciones:

- Asesorar en la formulación del plan estratégico de TI.
- Proponer las políticas generales sobre TI.
- Revisar periódicamente el marco para la gestión de TI.
- Proponer los niveles de tolerancia al riesgo de TI en congruencia con el perfil tecnológico de la entidad.
- Monitorear que la alta gerencia tome medidas para gestionar el riesgo de TI en forma consistente con las estrategias y políticas y que cuenta con los recursos necesarios para esos efectos.
- Recomendar las prioridades para las inversiones en TI.
- Proponer el Plan Correctivo-Preventivo derivado de la auditoría y supervisión externa de la gestión de TI.Dar seguimiento a las acciones contenidas en el Plan Correctivo-Preventivo.

Los procesos del Marco COBIT que la superintendencia define como obligatorios son:

PO9 Evaluar y Administrar los riesgos de TI.

PO10 Administrar proyectos.

AI6 Administrar cambios.

DS2 Administrar los servicios de terceros.

DS4 Garantizar la continuidad de los sistemas.

DS5 Garantizar la seguridad de los sistemas.

DS11 Administrar los datos.

ME2 Monitorear y evaluar el control interno.

PO1 Definir un plan estratégico de TI.

PO3 Determinar la dirección tecnológica.

PO5 Administrar la inversión en TI.

AI3 Adquirir y mantener infraestructura tecnológica.

AI5 Adquirir recursos de TI.

DS3 Administrar el desempeño y la capacidad.

DS9 Administrar la configuración.

DS10 Administrar los problemas.

DS12 Administrar el ambiente físico.

Dicho cumplimiento de los procesos mencionados anteriormente debe ser revisados por una auditoría externa al menos cada dos años, la auditoría se basa en los criterios establecidos por la *Information Systems Audit and Control Association* (ISACA). El auditor

que lleve a cabo la ejecución debe ser certificado CISA (*Certified Information Systems Auditor*), y no debe haber prestado servicios relacionados con Tecnologías de Información a la entidad en los últimos tres años, entre otros requisitos definidos en la normativa.

Ese informe de auditoría servirá para dar una clasificación sobre la gestión de TI a la entidad, la cual debe ser valorada para analizar la gestión de riesgos de esta y para juzgar la situación económica financiera de las organizaciones supervisadas; incluye el riesgo de solvencia, riesgo de liquidez, riesgo por variaciones en las tasas de interés, riesgo cambiario, riesgo de crédito y riesgo operacional. , según la calificación definida por la superintendencia de la ficha CAMELS (según su acrónimo en español que se detalla Capital, Activos, Manejo o Gestión, Evaluación de rendimientos, Liquidez, Sensibilidad a riesgo de mercado) en el acuerdo SUGEF 24-00 (Superintendencia General de Entidades Financieras, 2016).

Por lo tanto, si la entidad incumple con una adecuada administración de los riesgos tecnológicos de acuerdo con los procesos del marco COBIT obligatorios, su calificación cualitativa de la situación económica financiera, conforme al acuerdo SUGEF 24-00 *Reglamento para juzgar la situación económica-financiera de la entidades fiscalizadas*, se verá afectada y la superintendencia estará en su facultad de sancionar a la entidad por su incumplimiento.

1.3.2 Ámbito regulado por la Contraloría General de la República

Él otro ámbito costarricense regulado es el sector supervisado por la Contraloría General de la República, el cual establece medidas para la seguridad y control de la información mediante el documento N-2-2007-CO-DFOE denominado *Normas Técnicas para la gestión y el control de las Tecnologías de Información*. El documento establece los criterios de control que los responsables de la gestión de Tecnologías de Información deben establecer, mantener, evaluar y perfeccionar. Dicha normativa es de acatamiento

obligatorio para las instituciones sujetas a la supervisión de la Contraloría General de la República.

Esta norma se divide en 25 lineamientos que se categorizan en los siguientes capítulos:

- Normas de Aplicación General.
- Planificación y Organización.
- Implementación de Tecnologías de Información.
- Prestación de servicios y mantenimiento.
- Seguimiento.

En dicha normativa, se obliga a los entes supervisados a mantener un estricto control de las Tecnologías de Información y a mantener una adecuada gestión de los riesgos, los cuales deben ser valorados por vía del Sistema Específico de Valoración del Riesgo Institucional (SEVRI). De igual forma obliga a las entidades, entre otras cosas, a proteger los recursos de TI y a comprometer al personal con la seguridad de la información y con la planificación adecuada y gestión de los proyectos organizacionales.

La normativa que regula tanto las entidades supervisadas por la Contraloría General de la República como por la Superintendencia General de Entidades Financieras obliga a las organizaciones supervisadas a administrar los riesgos tecnológicos y alinear los recursos de TI para lograr alcanzar los objetivos institucionales de cada una.

De esta forma se evidencia la existencia de las diferentes regulaciones a nivel de normativa que se son aplicables en los diferentes sectores a nivel nacional.

1.4 Teoría y aplicación de las Tecnologías de Información para la administración de la seguridad y el control de la información en las fundaciones.

La aplicación de las Tecnologías de Información para administrar la seguridad y el control de la información en las fundaciones, aparece junto con el desarrollo de las mismas en las empresas del sector privado. Desde la década de los 80 hasta el periodo actual, las compañías se han enfocado en realizar una inversión importante en las Tecnologías de Información con el fin de agilizar los procesos de sus negocios, un ejemplo de esto es la creación de la Asociación Nacional de Informática en el año 1982 ante la necesidad de agrupar a los profesionales de esta rama, debido a la alta demanda de las computadoras para los trabajos realizados en las diferentes entidades, esto influyó en que los desarrolladores intentaran día a día mejorar los sistemas para el manejo de la información, incrementando los estándares de seguridad y control de la misma.

Este desarrollo ha tenido gran impacto en los esquemas de negocio de las empresas, ya que ha modificado factores importantes en la forma de almacenamiento de datos, desarrollo de procesos automatizados, comunicación y análisis de resultados para la toma de decisiones. Por ende los modelos de negocio se han modificado de acuerdo a las facilidades que se han ido desarrollando con el paso de los años desde su forma de producción y venta, hasta la entrega de productos y servicios.

Por esta razón la seguridad de la información se vuelve un factor determinante en el desarrollo de las entidades para mantener estándares de calidad en los productos y servicios brindados, tanto es así que en Estados Unidos algunas de

> "las nuevas leyes federales de seguridad y contabilidad, que requieren que muchas empresas almacenen sus mensajes de correo electrónico por cinco años, aunadas a las leyes existentes laborales y de salud, que solicitan que las empresas almacenen los datos de exposición química de los empleados por hasta 60 años, estimulan el crecimiento de la información digital a una tasa estimada de 5 exabytes al año…" (Laudon & Laudon, 2012, p.06).

Lo anterior deja en evidencia que la necesidad de expansión y desarrollo tecnológico se vuelve cada vez más crítica en el desarrollo de los negocios.

Debido al crecimiento tan precipitado en los últimos años de las Tecnologías de Información, y los cambios constantes que se viven en el día a día, se generan retos en la protección de los datos de todas las entidades y mejoras en los tiempos de respuesta y acceso a la información en caso de alguna eventualidad.

Debido a lo anterior se requiere una actualización constante y un mayor control de la información, ya que un inadecuado manejo de los activos informáticos propios, de empleados, benefactores o de sus clientes, podría generar responsabilidad legal.

De acuerdo con lo mencionado anteriormente, el adecuado manejo de las Tecnologías de Información para la administración de la seguridad y control de la información es vital en todas las entidades, por lo que para su correcta administración y evaluación se deben emplear controles tanto generales como de aplicación.

Según mencionan Laudon & Laudon (2012, p.308) en su libro *Sistemas de Información Gerencial*, existen controles generales y controles específicos. Los primeros hacen mención a controles sobre el diseño, seguridad y uso de los recursos tecnológicos (contemplando hardware, software y procedimientos manuales) enfocados en la infraestructura tecnológica organizacional para mantener su entorno de control en general; mientras que los segundos se enfocan en aplicaciones específicas como procesos de registro de facturación o controles de inventarios, estos son desarrollados para procedimientos automáticos y manuales con el fin de validar que se está procediendo de una forma completa y precisa, y se clasifican como controles de entrada, controles de procesamiento y controles de salida.

Con esto se soporta la importancia de la implementación de las Tecnologías de Información para una adecuada administración de la seguridad y el control de la información en las fundaciones.

Capítulo II. Fundación de la Universidad de Costa Rica para la Investigación (FUNDEVI)

Como parte del desarrollo de este capítulo se procederá a explicar la historia, estructura, funciones, operaciones, responsabilidades, composición del departamento de Tecnologías de Información, así como la evolución de la administración de la seguridad y control de la información que mantiene la Fundación de la Universidad de Costa Rica para la Investigación (FUNDEVI).

Gran parte de la información presente en este capítulo fue obtenida por medio de la página web oficial de FUNDEVI y una entrevista realizada al personal a cargo del departamento en estudio.

2.1. Descripción General de FUNDEVI

2.1.1. Reseña Histórica

La Fundación para la Investigación de la Universidad de Costa Rica (FUNDEVI), fue creada en año de 1988 por el Dr. Fernando Durán Ayanegui, Rector de la Universidad de Costa Rica en ese período; y amparada a la normativa presupuestaria No. 73 de la Ley 7015.

Dos años después se aprobó la Ley de Promoción de Desarrollo Científico y Tecnológico No.7069, la cual colaboró en gran manera al desarrollo de este tipo de organizaciones; ya que autorizaba a las instituciones de educación superior a crear fundaciones para fines más limitados, incluidos en la normativa presupuestaria antes indicada.

El convenio de cooperación y alianza entre la Universidad de Costa Rica (UCR) y FUNDEVI, fue firmado por el rector de la Universidad de Costa Rica Dr. Luis Garita Bonilla y el presidente de la fundación el Dr. Primo Luis Chavarría el 15 de junio de 1991.

Posterior a este acuerdo se declara a FUNDEVI por parte de la UCR como una institución de apoyo institucional, donde ambas se comprometen a aunar esfuerzos y recursos para apoyar, promover y desarrollar actividades en beneficio, principalmente de la investigación y la transferencia de tecnología.

Ahora bien, para diciembre de 1999 se aprueban lineamientos para la Vinculación Remunerada de la Universidad de Costa Rica con el Sector Externo, en los cuales se oficializó a FUNDEVI como mecanismo de administración de recursos provenientes del vínculo externo. En estos se definen los procedimientos en los cuales se establece la participación de las Vicerrectorías y las Unidades Académicas en la administración y control de cada proyecto o programa en FUNDEVI.

2.1.2. Descripción de FUNDEVI

Desde hace muchos años las fundaciones se han convertido en entes de carácter y beneficio social que favorecen en gran manera al desarrollo y crecimiento de muchos sectores alrededor del mundo. La mayoría de estos sectores buscan salir adelante a pesar de la limitación en sus recursos económicos, de infraestructura, de tecnología, entre otros, así como las dificultades que se les presenta para abastecer a la totalidad de la población involucrada.

Una de las fundaciones en nuestro país que forma parte importante de lo antes señalado y en la que basaremos el proyecto de graduación, es FUNDEVI; la cual trabaja de manera conjunta con la Universidad de Costa Rica (Institución pública, autónoma y soberana) en aspectos de bienestar social, como se menciona a continuación.

> FUNDEVI colabora a nivel de gestión de proyectos, ayuda en el fortalecimiento de capacitación en el área de investigaciones y funciona como pilar importante en diversos logros en el área de acción social. Además, mediante la administración de cuentas financieras, se convierte en una entidad facilitadora en el manejo ágil y flexible de los fondos públicos y privados de los diferentes proyectos en los que participa. (Fundación de la Universidad de Costa Rica para la Investigación, 2011)

En la actualidad FUNDEVI ha tenido un alto desempeño como entidad sin fines de lucro y se ha comprometido en el cumplimiento de sus objetivos, tanto a corto como a largo plazo, procurando que su fin se encuentre plasmado como bastón de referencia para mantener la identidad de colaborador social que ha caracterizado a la institución hasta hoy.

Como parte de su estructura organizacional y su establecimiento como institución formal y comprometida con el desarrollo de la sociedad, cuenta con una misión, visión, valores, objetivos y diversas políticas para no desviarse de los antes mencionados.

FUNDEVI es una institución que mantiene como misión centrarse en: “Apoyar los fines y propósitos de la Universidad de Costa Rica, mediante el fomento de las actividades del vínculo externo y la gestión ágil, efectiva y transparente de los procesos administrativos y financieros, orientados por una cultura de calidad”. (Fundación de la Universidad de Costa Rica para la Investigación, 2011)

Con el cumplimiento de su misión y al poder servir de apoyo a la Universidad de Costa Rica y a terceros en sus proyectos, tiene como visión llegar a: “Ser una fundación reconocida, nacional e internacionalmente, por su excelencia en el fomento y la gestión de recursos para programas y proyectos científicos, tecnológicos y humanísticos, que contribuyan al desarrollo integral de la Nación”. (Fundación de la Universidad de Costa Rica para la Investigación, 2011)

FUNDEVI tiene dentro de sus valores el compromiso y el apego a las buenas prácticas para cumplir con sus objetivos institucionales, esto con la finalidad de actuar de manera responsable, además inculca el respeto de los principios individuales y colectivos de las personas, desarrolla el trabajo en equipo por el bien de los objetivos comunes en un marco de solidaridad y respeto, y finalmente realiza sus actividades con calidad pues esto permite entregar a los usuarios finales la satisfacción de servicios basados en eficiencia, eficacia y mejora continua.

El logro de los objetivos de FUNDEVI responde a una relación con la Universidad de Costa Rica y se deben a una comunicación permanente y transparente, que le da un valor agregado en sus actividades.

Algunos objetivos estratégicos incorporados de FUNDEVI van enfocados a:

- Mejorar continuamente los servicios que ofrece la Fundación, con respecto a los atributos de pertinencia, agilidad, transparencia y fidelidad.
- Desarrollar el talento humano mediante la evaluación y formación continua que garantice colaboradores competentes.
- Controlar el Sistema de Gestión de Calidad (SGC) cumpliendo con los requerimientos establecidos en los capítulos de la Norma ISO 9001-2008, para garantizar su eficacia.
- Fomentar el posicionamiento de la Fundación fortaleciendo la imagen, la comunicación y la difusión de las posibilidades de vínculo externo de las unidades operativas de la UCR.
- Contribuir proactivamente con el fortalecimiento de los medios de enlace entre la Universidad y la Fundación, con el fin de mejorar la actividad de vínculo externo.
- Consolidar los mecanismos de comunicación de la Fundación con la UCR, para la rendición de cuentas y retroalimentación.

- Asegurar que los procesos de gestión, contemplen los elementos de responsabilidad social y ambiental.

Algunas políticas bajo las que se rige FUNDEVI son las siguientes:

- Política de calidad: la Fundación, en cumplimiento de su misión como mecanismo de apoyo a la Universidad de Costa Rica (UCR) en las actividades de vínculo externo se compromete a: Brindar servicios de excelencia, así como sistemas de información accesible y confiable para los usuarios. Además de cumplir con los requisitos del Sistema de Gestión de la Calidad y mejorarlo continuamente. Finalmente, facilitar la vinculación y cooperación de las Unidades Operativas de la UCR, con los sectores sociales y productivos, fortaleciendo el posicionamiento de la Fundación como un mecanismo ágil y transparente en la gestión de los recursos.
- Política de enlace UCR-Fundación: la base fundamental sobre la que opera la Fundación es que "existe para hacer más Universidad", regida bajo normas establecidos por la Universidad de Costa Rica, en materia de vinculación externa, con el fin de ejecutar conjuntamente la finalidad de orden público, asignada tanto por la Constitución Política como por la ley a estas instituciones, la cual es “impulsar el progreso nacional por medio de las actividades de investigación y de transferencia científica y tecnológica".(Fundación de la Universidad de Costa Rica para la Investigación, 2011)
- Política de transparencia: las acciones de la Fundación se realizan siguiendo los preceptos de la sana administración y la rendición de cuentas, de modo que se garantice la transparencia y se consolide así, la confiabilidad de la comunidad universitaria y de la sociedad en general.
- Fomento del vínculo externo: la Fundación colabora con las Unidades Operativas de la UCR, para incrementar los proyectos científicos, tecnológicos y humanísticos, que contribuyen al desarrollo y bienestar integral de la sociedad.

El fundamento jurídico en el que se basaron para constituir FUNDEVI se presenta a continuación:

- FUNDEVI como mecanismo idóneo para agilizar la gestión de las actividades universitarias: sus actividades están debidamente respaldadas por un Convenio de Cooperación suscrito con la Universidad de Costa Rica. En donde la faculta para llevar a cabo la gestión administrativa de los programas y proyectos universitarios y le autoriza para suscribir los acuerdos necesarios para la ejecución y desarrollo logístico de estos.
- Ente universitario, constituido para agilizar, sin evadir controles: la Contraloría General de la República define a FUNDEVI como: "un ente instrumental de la Universidad, no estatal y constituida con la finalidad de agilizar sus actuaciones, sin evadir controles".
- La Fundación se enmarca bajo dos modalidades de acción, una al actuar como una entidad privada estrechamente relacionada con la Universidad y otra como un mecanismo gestor de proyectos y actividades de vinculación de las Unidades Universitarias.
- Inscrita en el Registro Público de Costa Rica: FUNDEVI se encuentra inscrita en el Registro Público de Costa Rica, personería jurídica No. 3-006-101757, tomo 91, folio 158, asiento 226. Por tanto, y soportada además por la Ley de las Fundaciones del país a realizar sus propios actos con autonomía administrativa y financiera para el desempeño de sus funciones con plena capacidad jurídica para adquirir derechos y contraer obligaciones. (Fundación de la Universidad de Costa Rica para la Investigación, 2011).

La Fundación trae diversos beneficios a la Universidad de Costa Rica y a la sociedad, por medio de sus importantes servicios, tal es el caso de la investigación y desarrollo tecnológico, la cual suministra a los diferentes sectores conocimientos desarrollados o adaptados por la Universidad, por medio de un convenio o contrato de

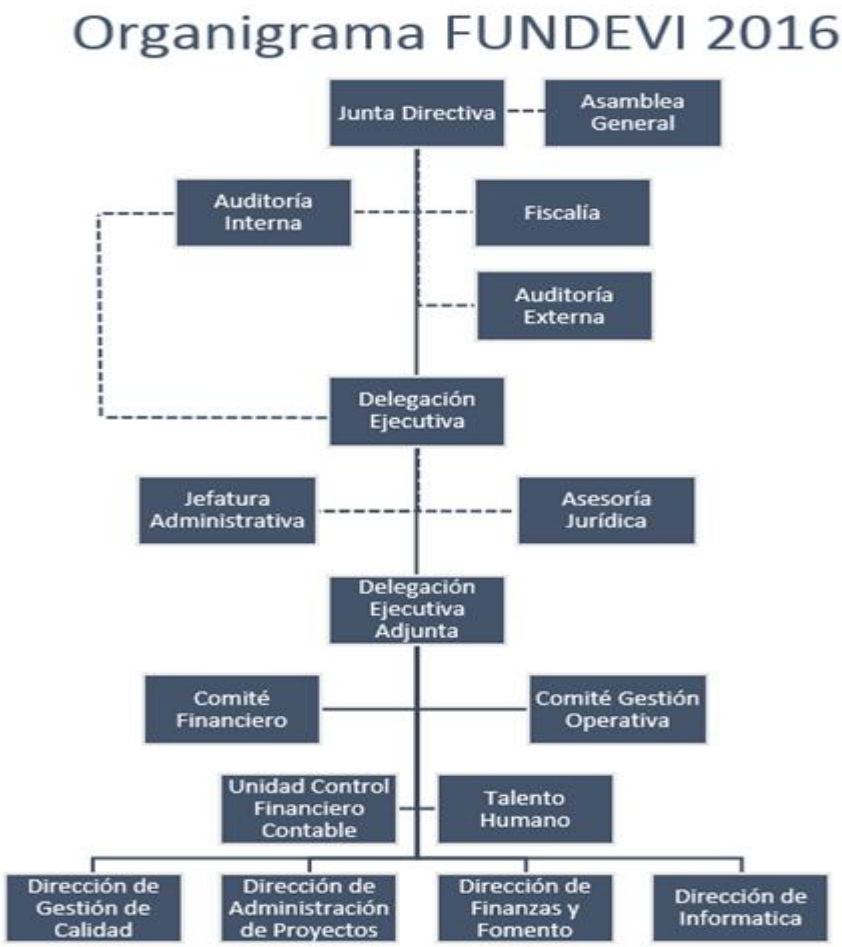
licencia, autorización, permiso o concesión de uso, a cambio de algún tipo de contraprestación. Además, produce y vende bienes de carácter científico, tecnológico o intelectual generados en la institución y resultado de las actividades académicas de la Universidad de Costa Rica.

De igual forma organiza actividades de capacitación y asesorías especializadas que definen y dan respuesta clara a incidentes específicos a través del conocimiento y tecnologías existentes, que no requieren de un proceso de investigación y que respondan a términos de referencia precisos y resultados específicos.

Además, colabora con la sociedad brindando servicios de laboratorio en materia de análisis físicos, mecánicos, químicos, biológicos y microbiológicos de materiales y productos, servicios técnicos que son proporcionados mediante profesionales, procedimientos y equipos especializados; servicios de certificación que garantizan el cumplimiento de requerimientos específicos por parte de un bien, proceso, servicio o sistema y que culminan con la emisión de un certificado o sello, de acuerdo con normas nacionales o internacionales, entre otros.

Adicionalmente, realiza servicios administrativos los cuales son proporcionados a diversidad de proyectos; servicios como la: administración de ingresos y egresos (colones, dólares y euros), controles e informes de ejecución presupuestaria, administración laboral y salarial, trámites de contratación de servicios profesionales, apertura y manejo de fondos de trabajo, trámites administrativos y legales en procesos licitatorios, adquisición de instrumentos financieros como garantías de participación y cumplimiento y verificación de cumplimiento de términos contractuales.

2.1.3 Descripción de estructura interna de FUNDEVI



Fuente: Elaboración propia del gráfico, 2016. Información obtenida del Sitio Web Fundación de la Universidad de Costa Rica, Organización Interna de FUNDEVI, 2016

Asamblea

La fundación cuenta con una Asamblea General, establecida en su Acta Constitutiva que se reúne anualmente. Constituida por el Consejo de Rectoría, el fundador, decanos coordinadores de las Áreas Académicas de la Universidad de Costa Rica, decano del Sistema de Estudios de Posgrado y aquellos que fueran propuestos por la Asamblea

General y admitidos por la Junta Administradora. (Fundación de la Universidad de Costa Rica para la Investigación, 2011)

Junta Administrativa

FUNDEVI es dirigida por una Junta Administrativa, que es el máximo órgano de toma de decisiones de la Fundación. Al día primero de octubre del 2016 está conformada por los siguientes directores:

Presidente

Fernando Manuel Salvador García Santamaría

Tesorero

Marjorie Jiménez Castro

Secretario

Bernal Herrera Montero

Representante de la Municipalidad Montes de Oca

Priscilla Carrillo Castro

Representante del Poder Ejecutivo

Bunny Jeanina Umaña Aguilar

Delegado ejecutivo

La Junta Administrativa es quien designa este puesto, el cual cuenta con facultades de apoderado generalísimo sin límite de suma para representar a FUNDEVI. Ejecuta las

directrices y políticas emanadas por este órgano, dirige, controla y vigila los servicios de la fundación, vela por el cumplimiento de convenios y compromisos adquiridos y además se encarga del desarrollo y cumplimiento de los objetivos estratégicos de corto, mediano y largo plazo. En la actualidad este puesto es ocupado por el M.Sc. Roberto Guillén Pacheco.

Fiscalía

Con el propósito de fortalecer la transparencia y la rendición de cuentas se constituyó una Fiscalía, conformada por profesionales en los campos de las Ciencias Económicas y Derecho.

Auditoría

La Junta administrativa es que designa un Auditor Interno con el fin de garantizar la idoneidad de los mecanismos de control. Adicionalmente, las operaciones de la fundación son objeto de una auditoría externa anual, cuyo informe se presenta a la Junta Administrativa, la Asamblea General y a la Contraloría General de la República.

Auditoría de calidad y Unidad de control interno

FUNDEVI cuenta con un departamento que vela por el buen funcionamiento del control interno de la organización y el buen desempeño de la misma bajo los estándares de calidad. A la fecha de este estudio, la Directora de Gestión de Calidad es la Licda. Marcela Calderón Morales.

Dirección de fomento y Asesoría de proyectos

La Dirección de Fomento y Asesoría, a la fecha de este estudio es la Máster Isabel Martínez Fonseca, ella es la encargada del apoyo al fomento de vínculo remunerado, la asesoría en formulación de proyectos, el apoyo en la negociación y formalización de

contratos y/o convenios, la recepción y negociación de procesos, las relaciones públicas y la comunicación.

Dirección de Administración de Proyectos

Tiene como finalidad la ejecución de los proyectos de Administración de Fondos a Terceros, particularmente en la apertura y cierre de cuentas financieras de proyectos, registro de presupuestos, gestión de fondos de trabajo, aprobación y registro de gastos, entre otros. En el momento en que se realizó este estudio, se encuentra a cargo de la ejecución de *Proyectos 9000* la bachiller Andrea Quesada Fallas.

FUNDEVI se ha consolidado como un modelo de organización para el apoyo de la investigación y la transferencia de tecnología, para ello, se ha especializado en proveer servicios de gestión administrativa, financiera y contable, administrando los recursos de manera ágil, confiable y transparente.

Como valor agregado, se realiza una entrevista a la empresa Abonos del Pacífico S.A (Compañía con más de 20 años de presencia en Costa Rica y Panamá; dedicada a la importación y comercialización de fertilizantes agrícolas), la cual de manera recurrente recibe servicios de FUNDEVI. Lo anterior con la finalidad de tener una visión más real del apoyo que le da está fundación al sector comercial y de desarrollo del país.

En resumen y a grandes rasgos, la empresa considera que los servicios recibidos como la investigación y desarrollo tecnológico (en temas de emisión de N2O piña), capacitaciones y actualizaciones (estudio de suelos, fisiología, mediciones técnicas) y servicios de laboratorio (en suelos, foliares y gases) son excelentes. Además, creen que la fundación ha traído una alianza estratégica, la cual beneficia en gran manera. La empresa expresa disconformidad a nivel del proceso post-prestación del servicio (facturación). (Anexo #2).

Adicionalmente, FUNDEVI cuenta con una amplia lista de entidades, organismos y fundaciones a nivel nacional e internacional que confían la gestión de sus fondos a FUNDEVI, tales como:

- Fundación Bill & Melinda Gates.
- Universidad de Wyoming.
- Universidad de Texas, San Antonio.
- Programa de las Naciones Unidas para el Desarrollo (PNUD).
- Corporación Bananera Costarricense.
- Instituto Nacional de Aprendizaje (INA).
- Instituto Nacional de la Mujer (INAMU).
- RECOPE.
- Instituto del Café.
- Florida Ice and Farm.
- Instituto Costarricense de Electricidad.
- Instituto Nacional de Seguros.
- Autoridad Reguladora de Servicios Públicos.
- Junta de Protección Social.
- Entre otros.

(Fundación de la Universidad de Costa Rica para la Investigación, 2011).

Donaciones

De conformidad con lo que establecen los Artículos 8, 9 y 18 de la Ley Número 5338 Ley de Fundaciones vigente, cláusula tercera del Acta Constitutiva, Artículos 3i inciso b) y 5 inciso b) de FUNDEVI y el criterio externado por la Dirección General de Tributación Directa mediante el oficio AIA-I-03-08, FUNDEVI se encuentra debidamente autorizada para recibir donaciones deducibles como un gasto de la renta bruta. Estos recursos son utilizados para: fondos de apoyo a la innovación, para el apoyo de investigación y acciones tendientes a mejorar el medio ambiente y para el apoyo al bienestar social, artísticos y de las bellas artes.

Por otra parte, se procedió a inscribir a FUNDEVI ante el *Internal Revenue Service* (IRS) de los Estados Unidos de América, y se le asignó el EIN 98-0512224 para poder recibir donaciones de ese país (Fundación de la Universidad de Costa Rica para la Investigación, 2011).

2.2. Descripción del departamento de Tecnologías de Información

2.2.1. Importancia de las Tecnologías de Información de FUNDEVI y su vinculación con los demás departamentos.

El siguiente análisis se realizó de acuerdo a la entrevista realizada a los funcionarios de FUNDEVI (Ver anexo #3).

Actualmente el Departamento de Tecnologías de Información realiza una serie de labores que permiten a los demás departamentos operar de la mejor manera y ayuda a la organización a lograr sus objetivos estratégicos mediante el apoyo a todas las áreas.

El departamento se compone de dos analistas de sistemas, un profesional de Tecnologías de Información y un técnico especializado en Tecnologías de Información, los cuales realizan las siguientes funciones para apoyar las labores de la organización:

1. El departamento de Tecnologías de Información investiga y recopila información para descubrir nuevas necesidades de los clientes internos mediante entrevistas a los directivos, a los técnicos y mediante estudios de clima organizacional.

2. Una vez determinadas las nuevas necesidades, se realiza un estudio de viabilidad para cada una de ellas y se analiza si se cuenta con los recursos necesarios para atenderlas e incluirlas en el plan anual de trabajo.

3. Este departamento también realiza las funciones de mantenimiento preventivo y correctivo.

4. Realizan mantenimientos programados periódicamente dependiendo de las necesidades de cada equipo, abarcando todos los equipos de la fundación.

5. Realizan respaldos de información categorizados por impacto y por tiempo de recuperación en cuatro niveles, el primer nivel es un respaldo local, el segundo nivel es un respaldo con replicación en un sitio remoto, el tercero es un respaldo en la nube, y el cuarto es un respaldo en medios de almacenamiento magnéticos que está fuera de la organización en una edificación de alta tecnología debidamente diseñada para este fin (por motivos de seguridad no es indicado), entre otros.

En materia de mantenimientos correctivos, tanto de software como de infraestructura, estos se realizan mediante solicitudes que los clientes hacen a través de un sistema informático o por vía telefónica; el profesional de Tecnologías de Información asigna la solicitud dependiendo del área, el encargado analiza si se tiene que subcontratar o

se puede atender la solicitud con los funcionarios del departamento y de acuerdo con el tipo de solicitud se asigna un plan para solucionar el problema con un tiempo máximo dependiendo de la categoría del evento o solicitud.

Una organización tan grande como es la FUNDEVI, no puede arriesgarse a tener actividades solamente reactivas, es decir que actúen solamente cuando un evento afecta indirecta o directamente a la organización. Por lo tanto las actividades preventivas son igual o más importantes que las reactivas, para la continuidad de la organización. Por ejemplo, actualmente los *hackers* están más presentes que nunca y podrían afectar la función más ordinaria de cualquier organización, incluida FUNDEVI, por lo que la seguridad de los datos de las organizaciones podría representar la continuidad de estas y evitaría un gasto de tiempo y recursos en indagar si es posible la recuperación de las informaciones en caso de ser atacados.,

En caso concreto con FUNDEVI, esta actividad preventiva estaría representada por los diferentes niveles de respaldo de datos que van desde copias en servidores locales, hasta copias en discos magnéticos en lugares ajenos a las instalaciones de esta institución.

Claro está que la parte reactiva no puede dejarse de lado, pues siempre se tiene que estar preparado para lo inesperado, es decir que no importa cuánto se trate de minimizar los riesgos, siempre habrá algo en lo que no se pensó que podría ocurrir, por lo que hay que reaccionar lo más rápido posible y arreglar el problema para no causar atrasos en el plan anual de la fundación.

Análisis FODA

El análisis FODA es una estructura conceptual de un análisis sistemático que facilita la adecuación de las amenazas y oportunidades externas con fortalezas y debilidades internas de la organización, en este trabajo basado en la Fundación de la Universidad de

Costa Rica para la Investigación (FUNDEVI), se establecen los factores internos y externos que podrían generar puntos clave para la organización.

Análisis interno

Fortalezas:

- Políticas específicas de calidad.
- Excelencia y mejoramiento continuo.
- Liderazgo y planificación estratégica.
- Enfoque hacia el talento humano y un ambiente laboral adecuado.
- Innovación y tecnología.

Debilidades:

- Falta de regulaciones específicas para los fondos públicos que maneja indirectamente.
- Dependencia directa de proyectos asignados por la Universidad de Costa Rica.
- Mercado limitado a usuarios de la Universidad de Costa Rica.
- Imposibilidad legal de expansión o crecimiento.

Análisis externo

Oportunidades:

- Aparición de nuevas tecnologías y constante necesidad de administración de los recursos.
- El hecho de que nuestro país está ubicado en una subregión con ausencia de conflictos bélicos es atractivo para la inversión extranjera.
- Estandarización de los parámetros de calidad que facilitan el desarrollo de proyectos.

Amenazas:

- Aparición de nuevos competidores más atractivos y/o infraestructuras más modernas.
- Dificultad de acceso al crédito dado el alto volumen de inversión en este negocio.
- Inestabilidad de los precios de servicios públicos e insumos con el consiguiente impacto en el transporte y la alimentación.

2.2.2. Evolución de las Tecnologías de Información para la administración de la seguridad y control de la información dentro de la organización.

En el año 2009 este departamento se componía de un solo colaborador y el 80% de los servicios eran subcontratados, no existía un proceso de planificación y los servicios eran reactivos. El departamento no contaba con funciones de desarrollo de software, los sistemas informáticos se compraban.

En el año 2010 la página web de la FUNDEVI sufrió un ataque malicioso , donde se cambió la página de la fundación por un mensaje del grupo que realizó el ataque Este hecho relevante evidenció las vulnerabilidades que podían existir en seguridad de información en su momento y creó conciencia a la fundación sobre la seguridad de sus sistemas informáticos, posteriormente a este hecho se decidió invertir en infraestructura del departamento de Tecnologías de Información (dispositivos físicos y software necesaria para la institución en el desarrollo de sus operaciones) .

Se decidió que los dos funcionarios con los que se contaba en ese momento tuvieran una especialidad asociada, un colaborador se especializó en seguridad y el otro en software, con el objetivo de abarcar de mejor manera las necesidades informáticas de la fundación. Esta especialización también significó una inversión en equipo y estructuración.

En el año 2011 se cambió la estructura del departamento y se crearon dos sub departamentos, desarrollo de software e infraestructura ambos pertenecientes al área de Tecnologías de Información.

Para mejorar la estructura se analizó la posibilidad de adquirir un software para la fundación pero el elevado costo y el extenso plazo de entrega de los oferentes causaron que se descartara esta posibilidad y se procedió a contratar programadores; primeramente se optó por profesionales independientes en lugar de programadores de planilla pero con el avance de los proyectos se decidió contratar a un analista de sistemas y otra persona para infraestructura, por lo que el esquema cambió a un departamento de cuatro personas que es el que se ha mantenido hasta la fecha en que se realizó el estudio.

El departamento de desarrollo de software funcionó de manera reactiva y se dio prioridad a desarrollar la herramienta y que cumpliera con las necesidades básicas y no tanto a la calidad de software y diseño. Lo cual actualmente se está optimizando, ya que se estaban gastando muchos recursos en mantenimiento.

Actualmente se está negociando una nueva propuesta para reestructurar el departamento. Ya que los funcionarios consideran que es mejor que no se separe en dos segmentos sino que todo el personal vea todos los temas de TI, debido a que el área de infraestructura se encuentra en un estado autómata lo que permitiría que estos colaboradores puedan brindar apoyo al área de desarrollo de software.

Al realizar una revisión general y conocimiento del funcionamiento de FUNDEVI, se identificaron aspectos sobre el estado de las diferentes áreas, así como del control y seguridad de la información que mantienen.

Capítulo III. Análisis y comparación del estado de la gestión y control de la información en las fundaciones, así como de las regulaciones aplicables a las Tecnologías de Información.

En este capítulo se analizan los lineamientos descritos en las regulaciones existentes a nivel nacional, tanto para el sector regulado por el CONASSIF como por la CGR, en materia de Tecnologías de Información, con el fin de comparar las normativas aplicables y determinar las buenas prácticas de la gestión de la seguridad y control de la información utilizada en Costa Rica.

Así mismo, se realiza un análisis de la situación actual de las fundaciones, donde se tomó en cuenta la información de FUNDEVI, y adicionalmente se analizaron tres fundaciones de estructura similar a la anterior, con el fin de obtener un panorama del manejo de la gestión de la seguridad y control de la información de estas organizaciones.

3.1 Identificación y valoración de la seguridad y control de la información dentro de las fundaciones.

Como el presente estudio es comparativo, solo se tomarán en cuenta las cuatro fundaciones pertenecientes a las cuatro universidades públicas. Es decir, solo se comparán las formas de operar en lo que se refiere al control y seguridad de la información dentro de cada fundación.

Estas cuatro fundaciones son las siguientes:

- La Fundación de la Universidad de Costa Rica para la Investigación (FUNDEVI)
- La Fundación para el Desarrollo Académico de la Universidad Nacional (FUNDAUNA)
- La Fundación Tecnológica de Costa Rica (FUNDATEC)

- La Fundación de la Universidad Estatal a Distancia para el Desarrollo y Promoción de la Educación a Distancia (FUNDEPREDI)

Si bien cada fundación es un organismo aparte de cada universidad, todas tienen una relación con la misma. Esto se demuestra dentro de los objetivos de cada una de ellas. Por ejemplo, dentro de los objetivos de FUNDATEC se encuentra: "fortalecer los vínculos del TEC con el sector público y privado, mediante el desarrollo de actividades de investigación y asesoría." Caso muy similar al de FUNDEVI, que dentro de sus objetivos tiene "contribuir proactivamente con el fortalecimiento de los medios de enlace entre la Universidad y la Fundación, con el fin de mejorar la actividad de vínculo externo."

Este es uno de los motivos por los cuales la comparación se realizaría solo con estas cuatro fundaciones. Otro motivo es que las cuatro al tener una relación cercana con las universidades, obtienen recursos públicos y privados (donantes privados).

Es por eso que para conocer más acerca la situación actual de las cuatro fundaciones, se les realizó un cuestionario que daría una idea sobre cómo estas se comparan entre ellas y las diferentes regulaciones y marcos de trabajo relacionado a las Tecnologías de Información, para el sector regulado tanto por la Contraloría General de la República como por el CONASSIF.

El cuestionario se compone de 32 preguntas y están distribuidas en los siguientes apartados:

- Normas de aplicación
- Planificación y organización
- Prestación de servicios y mantenimiento.

A partir de las deficiencias o carencias que surjan del análisis comparativo de las respuestas a las encuestas y los marcos de trabajo, es que se va a plantear la propuesta de la

metodología que reforzaría las mismas. De igual manera se analizaron las fortalezas y estrategias que tengan las fundaciones.

Siempre se tuvo presente que el principal eje para la administración de la seguridad y control de la información, en las diferentes instituciones, debía ser la importancia que estas le daban a las Tecnologías de Información dentro de la organización. A partir de esto se puede denotar qué tan desarrollados estarían el control y la seguridad de la información, al igual que otros aspectos como organigramas, funciones y presupuestos relacionados al área de TI.

Una buena planificación estratégica, objetivos, y demás están bien fundamentadas en las Tecnologías de Información para sus funciones, por lo que se puede argumentar que tendrían una fuerte base sobre el control interno, administración y gobierno de TI.

Si bien existen normativas para mejorar el control interno y seguridad de la información tanto para entes regulados u otras herramientas para organizaciones privadas, no son obligatorios para las fundaciones, por lo que partiendo de las diferentes respuestas recibidas por las cuatro fundaciones se van a destacar las falencias que tienen las mismas al igual que las fortalezas que poseen en dichas áreas.

3.1.1 Resultados de cuestionario aplicado a las fundaciones.

Producto de los cuestionarios realizados en la Fundación de la Universidad de Costa Rica para la Investigación (FUNDEVI), la Fundación de la Universidad Estatal a Distancia para el Desarrollo y Promoción de la Educación a Distancia (FUNDEPREDI), la Fundación Tecnológica de Costa Rica (FUNDATEC) y la Fundación para el Desarrollo Académico de la Universidad Nacional (FUNDAUNA) se pretende ubicar dentro de éstas la importancia que se les da a las Tecnologías de Información en sus organizaciones.

Lo anterior enfocado al desarrollo y crecimiento que han tenido en los últimos años, así como el apoyo e interés que le han dado a las Tecnologías de Información para la realización de sus diferentes operaciones; tanto así que están inmersas dentro de la planificación estratégica, objetivos e inclusive dentro de la misión de cada una de estas organizaciones.

Además, es necesario para las fundaciones que las Tecnologías de Información se mantengan actualizadas y en óptimas condiciones, para mantener un cumplimiento de las metas establecidas y no quedarse atrás con las nuevas demandas del mercado en cuanto a la eficiencia y eficacia de las Tecnologías de Información.

Para lo anterior es necesario contar con recursos monetarios, los cuales deben ser contemplados en el presupuesto de las fundaciones. Siendo el caso para estas cuatro fundaciones, donde todas tienen un apartado dentro de su presupuesto, con diferentes direcciones que van desde renovaciones de licencias y equipos, hasta mantenimiento de páginas web.

Propiamente en la encuesta realizada, se procedió a tabular las respuestas obtenidas por parte de a las fundaciones a las que se les aplicó. Lo anterior a partir de la categorización con un nivel de escala del 0 a 5, en donde estos indican: si no cumple los criterios solicitados (0), cumple deficientemente (1), cumple parcialmente bajo (2), cumple moderadamente (3), cumple parcialmente alto (4) y cumple satisfactoriamente con los criterios solicitados (5).

Obteniendo como resultado las siguientes notas finales y promediadas para las fundaciones:

Notas finales

FUNDEVI: 71.72%

FUNDAUNA: 63.45%
FUNDATEC: 53.10%
FUNDEPREDI: 44.14%

Nota promediada: 58.10%

Si se desea ver más a detalle considerar el Anexo #4 y el archivo en formato Excel *Tabulación de respuestas a encuesta* que se incluye de manera complementaria a este trabajo.

Como resultado de lo antes señalado y ya analizando a fondo, se identificó que existen congruencias y diferencias en el manejo de las mismas dentro de los siguientes sectores:

- Manejo de un Departamento de TI
- Políticas de Seguridad
- Riesgos de TI
- Mantenimiento de Datos y TI

Estos puntos son desarrollados en el siguiente apartado.

3.1.2. Puntos de alta y baja congruencia entre las fundaciones.

Como se menciona anteriormente, producto de los resultados de los cuestionarios se identificaron los puntos altos y bajos de congruencia en el manejo de las TI en la Fundación de la Universidad de Costa Rica para la Investigación (FUNDEVI) , la Fundación de la Universidad Estatal a Distancia para el Desarrollo y Promoción de la Educación a Distancia (FUNDEPREDI), la Fundación Tecnológica de Costa Rica (FUNDATEC) y la Fundación para el Desarrollo Académico de la Universidad Nacional (FUNDAUNA), mismos que se desarrollan a continuación:

Departamento de TI

Según el análisis que se realizó a las diferentes respuestas, se denota una importancia muy alta y una dependencia considerable en cuanto a las Tecnologías de Información, por lo que se podría argumentar qué tan necesario sería un órgano interno que desarrolle las mismas dentro de las organizaciones. A lo que se demuestra que tres (FUNDEVI, FUNDAUNA y FUNDATEC) sí mantienen un departamento, o al menos un encargado, para el desarrollo de operaciones relacionadas con las Tecnologías de Información. La fundación que no posee un departamento o encargado (FUNDEPREDI), acude a servicios proporcionados por terceros, para no quedarse atrás con sus similares en el manejo de las Tecnologías de Información, sin embargo, deberían considerar quÉ factores pueden generar un riesgo, así como un estudio previo de la empresa que brinda los servicios.

Políticas de seguridad para las TI

Se realiza un análisis de la importancia de la seguridad de la información, donde se demuestra que las cuatro tienen políticas de seguridad a niveles muy distintos entre ellas, que van desde el uso de políticas de la universidad que representa, hasta políticas propias y en constante actualización. Como lo es FUNDEUNA que posee políticas de seguridad y manuales de procedimientos, mientras que FUNDEPREDI realizó un acoplo de las políticas y procedimientos de la UNDED. Por otro lado FUNDATEC y FUNDEVI las han desarrollado, sin embargo, están en revisión y actualización.

Las políticas y procedimientos para la seguridad de la información deberían poseer prioridad a nivel de toma de decisiones en junta directiva, sin embargo en algunos casos se mantienen en revisión o en otros se carece de las mismas, por lo que se debería dar un seguimiento adecuado a la revisión final de estas, claro está sin dejar de lado las constantes actualizaciones.

Para el desarrollo de políticas de seguridad y manuales propios, siempre hay un documento que sirve de base para las mismas. COBIT, como era de esperar es uno de estos, por lo que se puede argumentar que tienen una fuerte base sobre el control interno, administración y gobierno de TI. Por otro lado, una hace alusión a la ISO 27000 que contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI). Cabe destacar que ninguna mencionó utilizar el marco normativo de la Contraloría General de la República, como base para el desarrollo de políticas o manuales internos, lo cual sorprende pues al ser fundaciones de universidades públicas, tienen cierta relación con la Contraloría, mas no hacen uso de la herramienta que tiene este ente.

Dentro de las políticas de seguridad de la información de las organizaciones deben haber ciertos apartados como: contratos de confidencialidad y compromiso por parte de los empleados, controles de accesos a las instalaciones, salidas y entradas de equipos, bitácoras de actualizaciones o cambios, al igual que procedimientos para el desecho y/o reutilización de equipos de TI y políticas para el desecho y control de documentos físicos.

Si bien estos apartados no eliminan en su totalidad la fuga o pérdida de información, se reduce el riesgo en gran medida, al igual que se tendría un mejor control sobre la información delicada que pueda manejar la organización. Es primordial destacar la importancia que se les dé a estas políticas internas dentro de cada organización al igual que los manuales de procedimientos para casos como estos, pues son los controles de calidad y seguridad de la información.

Riesgos de TI

Ante la inminente presentación de algún riesgo, los cuales están presentes en todas organizaciones, como lo es el posible daño a la propiedad, tanto por terceros como por

agentes externos como desastres naturales, pérdida de información y accesos no autorizados a los sistemas; los controles de las diferentes organizaciones deberían ser equivalentes.

Los riesgos varían de organización a organización, por lo que un sistema de valorización de riesgos metódico es importante considerarlo, pues así se valorarían los posibles riesgos constantemente, no dejando de lado la determinación, evaluación y gestión de riesgos; lo cual podría comprometer a la organización en un futuro incierto.

Es importante mencionar que con un sistema de valorización se dejaría de lado la parte subjetiva de la valorización de riesgos que se podrían presentar en la organización. Si bien una planificación no asegura que la ejecución sea perfecta, esta ayuda a que sea más eficiente y eficaz, por lo que si hay un equipo que se encargue de estos puntos las tareas serán más sencillas.

En uno de los casos se posee una estructura ideal para la identificación de necesidad y riesgos, mientras que en las otras tres se denota la necesidad de una persona a nivel interno que posea conocimiento sobre las condiciones y normas de control de suministros e infraestructura.

Mantenimiento de Datos y TI

En lo que respecta al mantenimiento de las TI, en tres organizaciones delegan partes de sus operaciones a terceros, que van desde mantenimiento de sistemas, soporte técnico, sistemas contables, respaldos de la información, hardware, hasta *hosting* e impresiones.

A pesar de que algunas tienen departamentos exclusivos para TI, siempre está presente el *outsourcing*, solo que en algunas está presente en operaciones que sí pueden pertenecer a la misma fundación, mientras en otras es solo un sistema contable. Por lo que hay que valorar la importancia de determinar muy bien qué tareas se pueden entregar a terceros y cuáles es más beneficioso mantenerlas dentro de la organización.

Estos contratos son muy delicados en cuanto a detalles y alcances que tienen los mismos. Por lo que es destacable que en todas las fundaciones hay un encargado o una parte que controla estos contratos con terceros. Un detalle muy delicado es el tema de renovaciones de estos. Los contratos pocas veces son indefinidos; es decir que no tienen un plazo definido que relacione ambas partes, por lo que hay que tener muy en claro los criterios para la renovación de estos, a lo cual todas las fundaciones respondieron que se evalúan anualmente todos los contratos, y dependiendo de este análisis se renuevan.

Cabe destacar que cuando se habla de renovar no necesariamente hay un nuevo contrato en sí, sino que al no cortarse el mismo se mantiene con las mismas condiciones, en otras palabras se renueva automáticamente.

Siempre se busca que los datos no sean solo eso, se busca que los datos se vuelvan información, por lo que diferentes software procesan los mismos. Aun así siempre hay riesgos de que esta no sea lo que se busca al final, es decir que no sea válida. Por lo que sería importante tener algún control sobre la información procesada, a lo que respondieron que sí tienen controles como son la auditoría interna y externa, los cuales validarían la información administrativa, financiera, etc.

De igual manera mencionan controles como flujos de aprobación, los cuales incluyen procesos de procesamiento, revisión y autorización. Todos estos controles denotan la importancia que le dan a la información dentro de la fundación.

Para ingresar datos a los equipos es necesario un sistema, el cual puede ser creado dentro de la misma organización o provisto por un tercero. No importa cuántas pruebas se realicen antes de sacar la versión final, siempre hay posibilidad de fallas. Estos sistemas no son libres de errores, los cuales pueden ir desde simples fallas hasta errores que comprometan las operaciones de la fundación. La mayoría de las ocasiones los primeros en notarlos son los mismos usuarios de estos. Pero no siempre el usuario sabe cómo solucionarlos. Por tanto es necesario que la organización tenga cómo hacerle frente a los

mismos, desde la identificación hasta la resolución de los problemas en sistemas y procesamientos de información.

Una vez procesada la información hay que almacenarla, siendo este almacenamiento fundamental para todas las organizaciones pues la pérdida de información es uno de los riesgos organizacionales de más alto impacto. Por lo tanto, se cuestionó sobre los procesos que utilizan para mitigar el mismo. Todas las organizaciones cuestionadas tienen procesos de respaldo de información, es decir que guardan por aparte la información en caso de fallas. Lo que cambia entre ellas es la periodicidad con la que realizan los respaldos, que van desde cada tres horas hasta mensualmente, esto dependiendo del tipo de información y medio de almacenamiento.

Con esto se concluye que el manejo de las TI a nivel de la Fundación de la Universidad de Costa Rica para la Investigación (FUNDEVI) , la Fundación de la Universidad Estatal a Distancia para el Desarrollo y Promoción de la Educación a Distancia (FUNDEPREDI), la Fundación Tecnológica de Costa Rica (FUNDATEC) y la Fundación para el Desarrollo Académico de la Universidad Nacional (FUNDAUNA), poseen manejo de las áreas críticas con ciertas variaciones, sin embargo, al final similares y en algunos casos con oportunidades de mejora que podrían ser abordadas mediante la aplicación de una metodología adecuada basada en las mismas normas.

3.2 Gestión de la seguridad y Tecnologías de la Información de acuerdo a la normativa regulatoria.

3.2.1 Análisis de la gestión de la seguridad y tecnologías de la información según el marco regulatorio aplicable por la Contraloría General de la República.

En materia de Seguridad y Control de las Tecnologías de la Información para el Sector Público se encuentra la Normativa N-2-2007-CO-DFOE denominada *Normas Técnicas para la Gestión y Control de las Tecnologías de Información*, la cual es creada

por el Órgano Constitucional y Auxiliar de la Asamblea Legislativa, llámese: Contraloría General de la República.

"Esta normativa es de acatamiento obligatorio para, quien la pone en vigencia, la Contraloría General de la República y las instituciones y órganos sujetos a su supervisión. Su inobservancia generará las responsabilidades que correspondan de conformidad con el marco jurídico que resulte aplicable". (Contraloría General de la República de Costa Rica, 2007).

Su creación permite establecer criterios de control y procurar una mejor gestión de las Tecnologías de la Información dentro de las organizaciones; ajustada a la realidad y necesaria en un ámbito tecnológico tan dinámico como el que se da en la actualidad.

Así mismo, es importante indicar que "los responsables de las organizaciones o en su derecho de la gestión de TI deben establecer, mantener, evaluar y perfeccionar el marco de control de conformidad con lo que establece la Ley General de Control Interno No.8292" (Contraloría General de la República de Costa Rica, 2007). Lo anterior debido a que es parte esencial en el desarrollo y acato a diferentes apartados establecidos en esta normativa de la Contraloría.

La normativa *N-2-2007-CO-DFOE Normas Técnicas para la Gestión y Control de las Tecnologías de Información* se compone de cinco capítulos, cada uno de ellos tiene apartados que lo desarrollan.

En primer lugar establece la importancia de tener claro que la introducción de las Tecnologías de la Información (llámense TI) debe ir enfocada hacia y para la organización en la que se implementan; a los objetivos y metas organizacionales, a la maximización de los recursos con que se cuenta, a las necesidades de los usuarios y como parte colaboradora en ejecución de procesos vinculados.

Asimismo se establece la necesidad de las TI de trabajar de manera eficaz y eficiente, las mismas deben ser flexibles a las necesidades que el entorno le demande, tanto interna como externamente. Que pueda aprovechar las oportunidades y/o consolidar las fortalezas, que pueda valorar y controlar los riesgos como herramienta para combatir las amenazas y/o minimizar las debilidades.

Las Normas establecen los siguientes apartados:

- Marco estratégico de TI: el jerarca debe traducir sus aspiraciones en materia de TI en prácticas cotidianas de la organización, mediante un proceso continuo de promulgación y divulgación de un marco estratégico constituido por políticas organizacionales que el personal comprenda y con las que esté comprometido.
- Gestión de la calidad: la organización debe generar los productos y servicios de TI de conformidad con los requerimientos de sus usuarios con base en un enfoque de eficiencia y mejoramiento continuo.
- Gestión de riesgos: la organización debe gestionar de manera continua los riesgos que esté integrada al sistema específico de valoración del riesgo institucional y considere el marco normativo que le resulte aplicable.
- Gestión de la seguridad de la información: la organización debe garantizar de manera razonable la confidencialidad, integridad y disponibilidad de la información. Debe documentar e implementar una política de seguridad de la información y los procedimientos correspondientes, asignar los recursos necesarios para lograr los niveles de seguridad requeridos:
  - La implementación de un marco de seguridad de la información.
  - El compromiso del personal con la seguridad de la información.
  - La seguridad física y ambiental.
  - La seguridad en las operaciones y comunicaciones.
  - El control de acceso.

  - La seguridad en la implementación y mantenimiento de software e infraestructura tecnológica.
  - La continuidad de los servicios de TI.
- Además debe establecer las medidas de seguridad relacionadas con:
  - El acceso a la información por parte de terceros y la contratación de servicios prestados por éstos.
  - El manejo de la documentación.
  - La terminación normal de contratos, su rescisión o resolución.
  - La salud y seguridad del personal.
- ·Implementación de un marco de seguridad de la información: la organización debe:
  - Establecer un marco metodológico que incluya la clasificación de los recursos de TI, según su criticidad, la identificación y evaluación de riesgos, la elaboración e implementación de un plan para el establecimiento de medidas de seguridad, la evaluación periódica del impacto de esas medidas y la ejecución de procesos de concienciación y capacitación del personal.
  - Mantener una vigilancia constante sobre todo el marco de seguridad y definir y ejecutar periódicamente acciones para su actualización.
  - Documentar y mantener actualizadas las responsabilidades tanto del personal de la organización como de terceros relacionados.
- Compromiso del personal con la seguridad de la información: el personal de la organización debe conocer y estar comprometido con las regulaciones sobre seguridad y confidencialidad, con el fin de reducir los riesgos de error humano, robo, fraude o uso inadecuado de los recursos de TI. Para ello, el jerarca, debe:
- Informar y capacitar a los empleados sobre sus responsabilidades en materia de seguridad, confidencialidad y riesgos asociados con el uso de las TI.
- Implementar mecanismos para vigilar el debido cumplimiento de dichas responsabilidades.

- Establecer, cuando corresponda, acuerdos de confidencialidad y medidas de seguridad específicas relacionadas con el manejo de la documentación y rescisión de contratos.

● Seguridad física y ambiental: la organización debe proteger los recursos de TI estableciendo un ambiente físico seguro y controlado. Debe considerar:

  - Los controles de acceso a las instalaciones.
  - La ubicación física segura de los recursos de TI.
  - El ingreso y salida de equipos de la organización.
  - El debido control de los servicios de mantenimiento.
  - Controles para el desecho y reutilización de recursos de TI.
  - La continuidad, seguridad y control del suministro de energía eléctrica, cableado de datos y de las comunicaciones inalámbricas.
  - El acceso de terceros.
  - Los riesgos asociados con el ambiente.

- Seguridad en las operaciones y comunicaciones: la organización debe implementar las medidas de seguridad relacionadas con la operación de los recursos de TI y las comunicaciones, minimizar su riesgo de fallas y proteger la integridad del software y de la información. Para ello debe:
  - Implementar los mecanismos de control que permitan asegurar la no negación, la autenticidad, la integridad y la confidencialidad de las transacciones y de la transferencia o intercambio de información.
  - Establecer procedimientos para proteger la información almacenada en cualquier tipo de medio fijo o removible (papel, cintas, discos, otros medios), incluso los relativos al manejo y desecho de esos medios.
  - Establecer medidas preventivas y correctivas con respecto a software malicioso o virus.

- Control de acceso: la organización debe proteger la información de accesos no autorizados. Para dicho propósito debe:
  - Establecer un conjunto de políticas y procedimientos relacionados con el acceso a la información, software de base y aplicación, a las bases de datos y a las terminales y otros recursos de comunicación.
  - Clasificar los recursos de TI en forma explícita, formal y uniforme de acuerdo con términos de sensibilidad.
  - Definir propiedad, custodia y responsabilidad sobre recursos de TI.
  - Establecer procedimientos para la definición de perfiles, roles y niveles de privilegio, y para la identificación y autenticación para el acceso a la información.
  - Asignar derechos de acceso a los usuarios de los recursos de TI.
  - Implementar el uso y control de medios de autenticación que identifiquen y responsabilice a quienes utilizan los recursos de TI.
  - Establecer controles de acceso a la información impresa, visible en pantallas o almacenada en medios físicos.
  - Establecer los mecanismos necesarios (pistas de auditoría) que permitan un adecuado y periódico seguimiento al acceso a las TI.
  - Manejar de manera restringida y controlada la información sobre la seguridad de las TI.

- Seguridad en la implementación y mantenimiento de software e infraestructura tecnológica. La organización debe:
  - Definir previamente los requerimientos de seguridad que deben ser considerados en la implementación y mantenimiento de software e infraestructura.
  - Contar con procedimientos claramente definidos para el mantenimiento y puesta en producción del software e infraestructura.

- Mantener un acceso restringido y los controles necesarios sobre los ambientes de desarrollo, mantenimiento y producción.
- Controlar el acceso a programas fuente y a los datos de prueba.

- Continuidad de los servicios de TI: La organización debe documentar y poner en práctica, en forma efectiva y oportuna, las acciones preventivas y correctivas necesarias con base en los planes de mediano y largo plazo de la organización, la evaluación e impacto de los riesgos y la clasificación de sus recursos de TI según su criticidad.

En cumplimiento de este punto y como manera de seguimiento y mejora continua la Contraloría General de la República emitió en 2007 y 2012, las directrices D.5.2007-CO-DDI y D-1-2012-DC-UTI**,** las cuales se encontraban relacionadas y ligadas con el propósito de documentar e implementar una política de S*eguridad de la Información y los procedimientos correspondientes*, así como asignar los recursos necesarios para lograr los niveles de seguridad requeridos y considerar lo que establece la normativa en mención.

- Gestión de proyectos: la organización debe administrar sus proyectos de TI de manera que logre sus objetivos, satisfaga los requerimientos y cumpla con los términos de calidad, tiempo y presupuesto óptimos preestablecidos.
- Decisiones sobre asuntos estratégicos de TI: el jerarca debe apoyar sus decisiones sobre asuntos estratégicos de TI en la asesoría de una representación razonable de la organización que coadyuve a mantener la concordancia con la estrategia institucional.
- 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.

Es de resaltar lo importante que viene a ser el compromiso, la motivación y la no resistencia al cambio por parte de los usuarios.

En todo momento se debe pensar que las funciones y los objetivos en la gestión de TI deben ir orientadas a la misión, visión y las metas de la organización en la se desarrollen. Tener claro con qué recursos se cuenta (económicos, humanos, de infraestructura) para planear y posteriormente desarrollar las TI; así como el apoyo con el que se cuente (la Junta Directiva, la Administración y en especial de los empleados como principales usuarios de los sistemas), la valoración de un marco FODA (Fortalezas, Oportunidades, Debilidades y Amenazas) y a partir de todo ello la decisión de factibilidad para ejecutar o no el proyecto.

Un proyecto como estos debe procurar la optimización de las funciones en las áreas que se ejecuten o relacionadas, en donde la eficiencia, eficacia, oportunidad, integridad y confidencialidad sean parte importante. Como resumen de lo dicho, se habla de Arquitectura de la Información.

Las ideas, los procesos y su ejecución pueden estar claros pero no materializados sin una adecuada infraestructura tecnológica. La planeación y organización en este apartado es de suma importancia, lo cual debe ser tomado con sumo cuidado. Para un jerarca es importante cuestionarse los requisitos para el buen funcionamiento, cuidado y mantenimiento de las Tecnologías de Información en la organización.

También se establecen dentro de la normativa de manera más específica que la planificación de las Tecnologías de Información debe lograr que las TI apoyen su misión, visión y objetivos estratégicos mediante procesos de planificación que logren el balance óptimo entre sus requerimientos, su capacidad presupuestaria y las oportunidades que brindan las tecnologías existentes y emergentes.

Las entidades supervisadas por la CGR deben contar con un modelo de arquitectura de información, la cual debe optimizar la integración, uso y estandarización de sus sistemas de información, que capture y comunique, en forma completa, exacta y oportuna, sólo la información que sus procesos requieren.

También se encuentran en la obligación de contar con una infraestructura tecnológica que mantenga el equilibrio que debe existir entre sus requerimientos y la dinámica y evolución de las TI.

El jerarca debe asegurar la independencia de la función de TI respecto de las áreas usuarias y que ésta mantenga la coordinación y comunicación con las demás dependencias tanto internas y como externas. También se debe optimizar el uso de los recursos financieros invertidos en la gestión de TI procurando el logro de los objetivos de esa inversión, controlando efectivamente dichos recursos y observando el marco jurídico que al efecto le resulte aplicable.

Posterior a la toma de decisión a favor de implementar las TI acorde a las necesidades de la organización, es fundamental que no se olvide el fin por el que se crean. El logro de los objetivos organizacionales, el cumplimiento de la visión y misión serán los pilares que en todo momento se deben seguir.

Claro está que el apoyo de la administración, la asignación clara de responsabilidades por parte de los usuarios o áreas vinculadas, el control en los accesos al sistema, o en su caso la autorización previa de la persona correspondiente, así como los recursos con los que se debe contar para su ejecución eficaz y efectiva es de importancia para que su implementación se realice acorde a lo planeado y organizado con anterioridad.

Ahora bien, la actitud proactiva al momento de implementar las TI juega un papel fundamental. Es decir, ser preventivo en vez de correctivo. Tomar las previsiones del caso en materia de riesgos es clave en esta etapa; aún más considerando que ya el software seleccionado e implementado, así como su infraestructura tecnológica, se encuentran ajustados y trabajando para satisfacer las necesidades de los usuarios, maximizando procesos y colaborando en la toma de decisiones.

La organización debe implementar y mantener las TI requeridas en concordancia con su marco estratégico, planificación, modelo de arquitectura de información e infraestructura tecnológica. Para esa implementación y mantenimiento debe:

- Adoptar políticas sobre justificación, autorización y documentación de solicitudes de implementación o mantenimiento de TI.
- Establecer el respaldo claro y explícito para los proyectos de TI tanto del jerarca como de las áreas usuarias.
- Garantizar la participación activa de las unidades o áreas usuarias, así como una asignación clara de responsabilidades.
- Instaurar líderes de proyecto con una asignación clara, detallada y documentada de su autoridad y responsabilidad.
- Analizar alternativas de solución de acuerdo con criterios técnicos, económicos, operativos, y lineamientos previamente establecidos.
- Contar con una definición clara, completa y oportuna de los requerimientos (aspectos de control, seguridad y auditoría bajo un contexto de costo – beneficio).
- Tomar las previsiones para garantizar la disponibilidad de los recursos económicos, técnicos y humanos requeridos.
- Formular y ejecutar estrategias de implementación para minimizar el riesgo de que los proyectos no logren sus objetivos, no satisfagan requerimientos o no cumplan términos de tiempo y costo indicados.
- Promover su independencia de proveedores de hardware, software, instalaciones y servicios.

- La organización debe implementar el software que satisfaga los requerimientos de sus usuarios y soporte efectivamente sus procesos, para lo cual debe:
  - Observar lo que resulte aplicable de la norma 3.1 anterior.
  - Desarrollar y aplicar un marco metodológico que guíe procesos de implementación y definición de requerimientos, estudios de factibilidad,

elaboración de diseños, programación y pruebas, conversión de datos y puesta en producción.

- Establecer los controles y asignar las funciones, responsabilidades y permisos de acceso al personal a cargo de las labores de implementación y mantenimiento de software.
- Controlar la implementación del software para garantizar la integridad de datos y programas en procesos de conversión y migración.
- Definir los criterios para determinar la procedencia de cambios y accesos de emergencia al software y datos, y los procedimientos de autorización, registro, supervisión y evaluación técnica, operativa y administrativa de los resultados de esos cambios y accesos.
- Controlar las distintas versiones de los programas que se generen como parte de su mantenimiento.

La organización debe adquirir, instalar y actualizar la infraestructura necesaria para soportar el software de conformidad con los modelos de arquitectura de información e infraestructura tecnológica y demás criterios establecidos. Como parte de ello debe considerar lo que resulte aplicable de la norma 3.1 anterior y los ajustes necesarios a la infraestructura actual.

La organización debe obtener satisfactoriamente el objeto contratado a terceros en procesos de implementación o mantenimiento de software e infraestructura. Para lo anterior, debe:

- Observar lo que resulte aplicable de las normas 3.1, 3.2 y 3.3 anteriores.
- Establecer una política relativa a la contratación de productos de software e infraestructura.
- Contar con la debida justificación para contratar a terceros.

- Establecer un procedimiento o guía para definir los *términos de referencia* que incluyan las especificaciones y requisitos o condiciones requeridos, así como para la evaluación de ofertas.
- Establecer, verificar y aprobar formalmente los criterios, términos y conjunto de pruebas de aceptación de lo contratado.
- Implementar un proceso de transferencia tecnológica que minimice la dependencia de la organización respecto de terceros contratados.

También es de suma importancia que la administración o el área encargada en la gestión de TI pueda analizar, estudiar y comprender de manera clara todos los componentes que envuelven la adquisición, puesta en marcha y el retorno de la inversión que la organización recibe por las TI. Esto con el fin de que en materia de servicios requeridos se entienda qué es lo idóneo con relación a lo que se tiene; qué responsabilidades son delegadas con la adquisición de ello y el seguimiento que debe darse para que se dé el cumplimiento de lo que se acuerda.

El control, mantenimiento y mejora continua de su plataforma tecnológica es esencial también. No es nada lógico que se coloquen millones de colones en un proyecto sin tener como retribución un desempeño óptimo, disponibilidad y uso maximizado, reducción de costos, entre otros más. Ahora bien, el riesgo de daños o pérdidas de información sensible es difícil de eliminar, pero puede ser minimizado con controles y un monitoreo periódico ajustado a lo que se tiene. Aspectos como la creación de *back up* o respaldos, manejo de incidentes, así como seguridad física y lógica son importantes. Adicional a la actualización de lo que se tiene en el presente, considerando el futuro.El jerarca y la función de TI deben acordar los servicios requeridos, los ofrecidos y sus atributos, lo cual deben documentar y considerar como un criterio de evaluación del desempeño. Para ello deben:

- Tener una comprensión común sobre: exactitud, oportunidad, confidencialidad, autenticidad, integridad y disponibilidad.
- Contar con una determinación clara y completa de los servicios y sus atributos, y analizar su costo y beneficio.
- Definir con claridad las responsabilidades de las partes.
- Establecer los procedimientos para la formalización de los acuerdos y la incorporación de cambios en ellos.
- Definir criterios de evaluación sobre el cumplimiento de los acuerdos.
- Revisar periódicamente los acuerdos de servicio, incluidos los contratos con terceros.

Para cumplir con lo establecido en las Normas técnicas de la CGR se debe mantener la plataforma tecnológica en óptimas condiciones y minimizar su riesgo de fallas. Para ello debe:

- Establecer y documentar los procedimientos y las responsabilidades asociados con la operación de la plataforma.
- Vigilar de manera constante la disponibilidad, capacidad, desempeño y uso de la plataforma, asegurar su correcta operación y mantener un registro de sus eventuales fallas.
- Identificar eventuales requerimientos presentes y futuros relacionados.
- Controlar la composición y cambios de la plataforma, mantener un registro actualizado de sus componentes (hardware y software), custodiar licencias de software y realizar verificaciones físicas periódicas.
- Controlar la ejecución de los trabajos mediante su programación, supervisión y registro.
- Mantener separados y controlados los ambientes de desarrollo y producción.
- Brindar el soporte requerido a los equipos principales y periféricos.

- Definir formalmente y efectuar rutinas de respaldo, custodiar los medios de respaldo en ambientes adecuados, controlar el acceso y establecer procedimientos de control para procesos de restauración.
- Controlar los servicios e instalaciones externos.

La organización debe asegurarse de que los datos que son procesados mediante TI corresponden a transacciones válidas y debidamente autorizadas, procesados en forma completa, exacta y oportuna, almacenados y desechados en forma íntegra y segura.

La organización debe hacerle fácil, eficaz, eficiente y oportuno al usuario el proceso para solicitar la atención de los requerimientos que surjan al utilizar las TI.

Además, debe identificar, analizar y resolver de manera oportuna los problemas, errores e incidentes significativos que se susciten con las TI. Dar el seguimiento pertinente, minimizar el riesgo de recurrencia y procurar el aprendizaje necesario.

Cuando la organización mantenga servicios con terceros debe:

- Establecer los roles y responsabilidades de terceros que le brinden servicios de TI.
- Establecer y documentar los procedimientos asociados con los servicios e instalaciones contratados a terceros.
- Vigilar que los servicios contratados sean congruentes con las políticas de calidad, seguridad establecidas por la organización.
- Minimizar la dependencia de la organización respecto de los servicios contratados a un tercero.
- Asignar a un responsable con las competencias necesarias que evalúe periódicamente la calidad y cumplimiento oportuno de los servicios contratados.

El monitoreo, la mejora continua y la retroalimentación son aspectos clave que se tomarán en este último capítulo. Todo esto se da luego del desarrollo y la ejecución del proyecto. Por lo es importante preguntarse ¿Cómo se valora esto?; pues es importante hacer la relación de los objetivos propuestos, si son cumplidos o no con respecto a lo obtenido con la implementación de las TI. Con esta interrogante se podrá establecer una medición del desempeño por parte del proyecto ejecutado en la organización.

Además, el papel del Control Interno, y en su caso del departamento de la auditoría interna en la gestión de TI es significativo; en donde la efectividad, el cumplimiento y las recomendaciones de mejora o corrección que puedan brindar por el bien de las TI y de la organización deben ser valorados en gran manera.

Los apartados de este último capítulo son claros; la revisión, la rendición de cuentas por parte de quienes tienen responsabilidades delegadas y el proceso de mejora continua deben prevalecer hasta el último día de vigencia de las TI en la organización.

La organización debe asegurar el logro de los objetivos propuestos como parte de la gestión de TI, para lo cual debe establecer un marco de referencia y seguimiento en los que defina alcance, metodología y mecanismos para vigilar la gestión de TI. Así como determinar responsabilidades del personal a cargo de dicho proceso.

El jerarca debe establecer y mantener el sistema de control interno asociado con la gestión de las TI, evaluar su efectividad, cumplimiento y mantener un registro de las excepciones que se presenten y de las medidas correctivas implementadas. Y debe velar porque el control interno en TI de la organización proporcione una garantía razonable del cumplimiento de los objetivos en esa materia.

Adicionalmente, en procura de la vigencia técnica y la mejora continua de la Seguridad de la información, se analizan las directrices existentes en materia de TI y comunicación, de manera que éstas se ajusten a las necesidades más actualizadas y a los

planteamientos estratégicos definidos institucionalmente. Es por ello que la Contraloría General de la República crea la directriz en el 2015 No. D-1-2015-DC-UTI y llamada: *Directrices sobre Seguridad y Buen Uso de las Tecnologías de Información y Comunicaciones***,** en donde en su capítulo 1: Aspectos Generales, cita el verdadero fin de ésta:

> "Incorporar dentro de las prácticas cotidianas de gestión institucional, un conjunto de acciones que permitan preservar las características de confiabilidad, integridad, confidencialidad, disponibilidad y privacidad de la información institucional; así como el buen uso de las Tecnologías de Información y Comunicaciones (TIC); dando así cumplimiento al numeral 1.4 de las Normas técnicas para la gestión y el control de las Tecnologías de Información…" (Contraloría General de la República, 2015)

Esta normativa fue creada bajo lineamientos que permitan fortalecer la administración de los recursos invertidos en Tecnologías de la Información por parte de las organizaciones, mediante el establecimiento de criterios básicos de control quobservados en la gestión institucional de esas tecnologías y que a su vez coadyuven en el control y supervisión que realice este órgano contralor. (Contraloría General de la República de Costa Rica, 2007).

La norma, aunque es obligatoria para aquellas a las que aplique, no debe verse como tal, sino más bien como una herramienta o manual colaborador que busca proteger los intereses de éstas bajo un lineamiento ordenado y con la claridad respectiva.

Para concluir, el sector al que va dirigida esta normativa maneja fondos públicos, es por eso que con ella se pretende que estos fondos sean usados en todo momento para los fines por los cuales son entregados (cumplimiento de objetivos organizacionales, misión y visión), teniendo como resultado la satisfacción de las necesidades y el logro del bienestar social deseado.

3.2.2. Análisis de la gestión de la seguridad y Tecnologías de la Información según el marco regulatorio aplicable por CONASSIF.

Normativa obligatoria y ejecutada por la Superintendencia General de Entidades Financieras (SUGEF) para todas las entidades sujetas a su supervisión.

En el sector regulado por CONASSIF se encuentra una única normativa sobre este tema, la cual abarca el sistema financiero en el que se desenvuelven bancos privados, financieras, casas de cambio, cooperativas de ahorro y crédito, y también bancos estatales.

El Reglamento sobre la gestión de las Tecnologías de Información es una normativa emitida por la Superintendencia General de Entidades Financieras y avalado por el Consejo Nacional de Supervisión del Sistema Financiero.

Esta normativa indica los procesos del Marco COBIT que la Superintendencia define como obligatorios, los cuales son:

PO9 Evaluar y Administrar los riesgos de TI.

PO10 Administrar proyectos.

AI6 Administrar Cambios.

DS2 Administrar los servicios de terceros.

DS4 Garantizar la Continuidad del Servicio.

DS5 Garantizar la seguridad de los sistemas.

DS11 Administrar los datos.

ME2 Monitorear y evaluar el control interno.

PO1 Definir un plan estratégico de TI.

PO3 Determinar la dirección tecnológica.

PO5 Administrar la inversión en TI.

AI3 Adquirir y mantener infraestructura tecnológica.

AI5 Adquirir recursos de TI.

DS3 Administrar el desempeño y la capacidad.

DS9 Administrar la configuración.

DS10 Administrar los problemas.

DS12 Administración del ambiente físico.

En dichos procesos se abordan diferentes puntos para abarcar una metodología de seguridad y control de la información que permita a estas entidades mejorar sus procesos en estos apartados. Estas son:

Punto 1: no serviría de nada tener una infraestructura e ideales estratégicos tecnológicos y adecuados a los objetivos de la organización sin contemplar aquellos factores que podrían crear imprevistos no deseados o en el peor de los casos impidan el cumplimiento de las metas por las que fueron creados. Estos factores se conocen como riesgos de TI.

Una gestión adecuada de riesgos de TI ayuda enormemente a prevenirlos, a actuar sobre ellos y retroalimentar al negocio para situaciones similares a futuro. La creación de controles sólidos en este tema, recurso humano capacitado y comprometido, así como una estructura tecnológica adecuada que permita monitorear y que tenga en todo momento la

capacidad de actuar sobre cualquier evento anormal que desee atentar contra las actividades operacionales o el desempeño de la organización.

Adicionalmente, la identificación de responsabilidades y roles, la claridad de las áreas críticas que tiene la organización, y el tema financiero, en especial con sus costos, son consideraciones adicionales en este tema.

La normativa estipula el siguiente proceso: *P09. Evaluar y Administrar los Riesgos de TI* en relación con dicho punto. Para ello son varias las actividades que se pueden citar y resumen de manera clara lo indicado:

1. Crear y dar mantenimiento a un marco de trabajo de administración de riesgos.
2. El marco de trabajo documenta un nivel común y acordado de riesgos de TI, estrategias de mitigación y riesgos residuales.
3. Cualquier impacto potencial sobre las metas de la organización, causado por algún evento no planeado se debe identificar, analizar y evaluar.
4. Se deben adoptar estrategias de mitigación de riesgos para minimizar los riesgos residuales a un nivel aceptable.
5. El resultado de la evaluación debe ser entendible para los interesados y se debe expresar en términos financieros, para permitirles alinear los riesgos a un nivel aceptable de tolerancia.

En sí, la entidad debe crear un marco de trabajo de administración de riesgos que puedan causar un impacto potencial sobre las metas de la organización, con estrategias de mitigación y riesgos residuales. Debe establecer un contexto de riesgo, y una evaluación recurrente de la probabilidad e impacto de los mismos para evitar que se vean amenazados los objetivos organizacionales establecidos. **Punto 2:** la administración de proyectos permite conocer en qué centrarse (priorizar), en qué destinar recurso físico, lógico, humano, entre otros; conocer los alcances que se tendrían, qué áreas del negocio se ven relacionadas

o beneficiadas con cada proyecto, qué consideración tienen en el presupuesto del negocio y el seguimiento que puede darse para observar en qué se invierte y qué resultados se logran con éste (resultados del proyecto), entre otros.

Otro aspecto importante que la administración de proyectos crea dentro de la organización es el grado de compromiso, responsabilidad, identificación y unión por parte de las áreas o responsables en cada uno de los proyectos que se desarrollan.

Finalmente, los controles son base fundamental, en especial para todos aquellos que tienen un tiempo de ejecución y culminación prolongado, pues puede crearse una desviación de los objetivos iniciales y no cumplir con las metas establecidas.

La normativa estipula el siguiente proceso: *P10. Administrar Proyectos* en relación con dicho punto. Para ello son varias las actividades que se pueden citar y resumen de manera clara lo indicado:

1. Establecer un marco de trabajo de administración de programas y proyectos para la administración de todos los proyectos de TI establecidos.

2. El marco de trabajo debe garantizar la correcta asignación de prioridades y la coordinación de todos los proyectos.

3. El marco de trabajo debe incluir un plan maestro, asignación de recursos, definición de entregables y aprobación de los usuarios.

4. El marco de trabajo debe tener un enfoque de entrega por fases, aseguramiento de la calidad, un plan formal de pruebas, revisión de pruebas y post-implantación después de la instalación para garantizar la administración de los riesgos del proyecto y la entrega de valor para el negocio.

Con respecto a la última actividad indicada, se hace mención a que un enfoque de este tipo reduce el riesgo de costos inesperados y de cancelación de proyectos, mejora la comunicación y el involucramiento del negocio y de los usuarios finales, asegura el valor y la calidad de los entregables de los proyectos, y maximiza la contribución a los programas de inversión facilitados por TI. **Punto 3:** a nivel de la administración de cambios en el área de TI, es clave señalar que todo debe ser archivado y documentado de manera clara y concisa. Todo esto apegado a los procedimientos de control relacionados con este tema y que debieron ser elaborados y creados por la organización.

La razón principal de esta administración de cambios es la consideración de eventos relacionados posteriormente que pueden surgir; claro está que con ello se permitiría entender eventos anteriores, temas de impacto en áreas, aspectos de priorización y respuestas ante posibles incidentes que puedan materializarse.

La normativa estipula el siguiente proceso: *AI6 Administrar Cambios* en relación con dicho punto. Para ello son varias las actividades que se pueden citar y resumen de manera clara lo indicado:

1. Todos los cambios, incluyendo el mantenimiento de emergencia y parches, relacionados con la infraestructura y las aplicaciones dentro del ambiente de producción, deben administrarse formalmente y controladamente.

2. Establecer un proceso para definir, plantear, evaluar y autorizar los cambios de emergencia que no sigan el proceso de cambio establecido.

3. Los cambios (incluyendo procedimientos, procesos, sistema y parámetros del servicio) se deben registrar, evaluar y autorizar previo a la implantación y revisar contra los resultados planeados después de la implantación. Esto garantiza la reducción de riesgos que impactan negativamente la estabilidad o integridad del ambiente de producción.

Esta normativa obliga a la entidad a establecer procedimientos para los cambios que permitan documentar y controlar formalmente las solicitudes para cambios a aplicaciones, procedimientos y procesos. **Punto 4:** ahora bien, si se contratan servicios de TI a terceros es básico tener presente por qué se delegan esas actividades y por qué no lo ejecuta el mismo recurso de la organización, además cómo se procede a seleccionar ese proveedor y considerar todas aquellas condiciones que el documento o contrato debe indicar para tener claridad de lo que se va a recibir por parte del proveedor y el resultado a obtener por parte de la organización que contrata.

Aspectos como el alcance, las responsabilidades, los tiempos de respuesta y entrega de servicios, entre otros, son los considerados en este tema. Otro asunto que debe recalcarse es la confidencialidad, la seriedad y cualquier otro aspecto de profesionalismo por parte del proveedor al momento de proceder con el manejo de datos de la organización a la que le presta el servicio, ya que la sensibilidad en mucha de ella puede provocar riesgos que no se desea que se materialice. La importancia de los acuerdos de nivel de servicio debe tocar todos estos puntos antes señalados.

La normativa estipula el siguiente proceso: *DS2 Administrar los Servicios de Terceros* en relación con dicho punto. Para ello son varias las actividades que se pueden citar y resumen de manera clara lo indicado:

1. La necesidad de asegurar que los servicios provistos por terceros cumplan con los requerimientos del negocio, requiere de un proceso efectivo de administración de terceros.

2. Claridad en la definición de roles, responsabilidades y expectativas en los acuerdos con los terceros.

3. Revisión y monitoreo de la efectividad y cumplimiento de dichos acuerdos.

4. Efectiva administración de los servicios de terceros minimiza los riesgos del negocio asociados con proveedores que no se desempeñan de forma adecuada.

Los servicios de terceros deben ser administrados apropiadamente para asegurar que cumplan con los requerimientos del negocio, las relaciones deben ser gestionadas para que la calidad de la misma se base en confianza y transparencia.

De igual forma se debe identificar y mitigar los riesgos relacionados con la entrega del servicio de los proveedores, se debe contemplar acuerdos de confidencialidad, contratos de garantía y demás requerimientos de seguridad que sean necesarios para mitigar los riesgos relacionados con la contratación de servicios de terceros. **Punto 5:** el garantizar la continuidad del servicio es muy importante, en especial para aquellas secciones consideradas como críticas o de sensibilidad dentro del negocio. Para ellas debe considerarse en todo momento lo que se conoce como un plan B, segunda opción, o plan de contingencia. Por ejemplo: en una empresa que labora de manera interrumpida brindando servicios de telefonía, sería inconcebible que se tenga un riesgo alto por no considerar diferentes alternativas en caso de que se interrumpa el servicio sea por unos segundos o minutos.

La consideración de aspectos como el seguimiento, la responsabilidad de labores, el control de licencias software, la estructura tecnológica y su deterioro, entre muchos otros, son esenciales para evitar lo señalado en el párrafo anterior. Una bitácora o portafolio de incidentes y soluciones de respuesta es clave en estos casos, así mismo, la ejecución de pruebas (simulacros) ante posibles eventos con el fin de conocer la reacción y capacidad de respuesta que se tiene. Posteriormente, la reanudación y reinicio luego de un evento de este tipo es clave para los intereses del negocio y la consecución de sus objetivos.

La normativa estipula el siguiente proceso: *DS4 Garantizar la Continuidad del Servicio* en relación con dicho punto. Para ello son varias las actividades que se pueden citar y resumen de manera clara lo indicado:

1. Brindar continuidad en los servicios de TI requiere desarrollar, mantener y probar planes de continuidad de TI.

2. Almacenar respaldos fuera de las instalaciones y entrenar de forma periódica sobre los planes de continuidad.

3. Realizar un proceso efectivo de continuidad de servicios, el cual minimiza la probabilidad y el impacto de interrupciones mayores en los servicios de TI, sobre funciones y procesos claves del negocio.

4. Centrar la atención en los puntos determinados como los más críticos en el plan de continuidad de TI, para construir resistencia y establecer prioridades en situaciones de recuperación.

Determinar que existe una estrategia de distribución definida y administrada para asegurar que los planes se distribuyan de manera apropiada y segura y que estén disponibles entre las partes involucradas y autorizadas cuando y donde se requiera. Se debe prestar atención en hacerlos accesibles bajo cualquier escenario de desastre.

La entidad debe establecer un plan de continuidad, que debe centrar la atención en los puntos más críticos de los procesos y establecer estos como prioridades en situaciones de recuperación. Las prioridades deben establecerse de acuerdo con niveles de prioridades.

Este plan de continuidad debe ponerse a prueba de forma regular para garantizar el funcionamiento del mismo y de igual forma entrenar apropiadamente al personal encargado de llevarlo a cabo. **Punto 6:** la seguridad física y lógica debe de ser considerada, la presencia y claridad en las responsabilidades de las personas, el apego a las políticas y

procedimientos organizacionales, la concientización y los buenos valores inculcados por parte de la administración a todo su equipo humano, el acceso y la aprobación a aplicaciones o lugares restringidos, entre otros, son claves para garantizar de manera constante la seguridad de los sistemas de TI. La sensibilidad de la información no es un tema que puede descuidarse, ya que es parte importante para lograr objetivos o metas establecidas por la organización.

La normativa estipula el siguiente proceso: *DS5 Garantizar la Seguridad de los Sistemas* en relación con dicho punto. Para ello son varias las actividades que se pueden citar y resumen de manera clara lo indicado:

1. Mantener la integridad de la información y proteger los activos de TI, requiere de un proceso de administración de la seguridad. Este proceso incluye el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI.

2. Realizar monitoreo de seguridad y pruebas periódicas así como realizar acciones correctivas sobre las debilidades o incidentes de seguridad identificados.

3. Una efectiva administración de la seguridad protege todos los activos de TI para minimizar el impacto en el negocio causado por vulnerabilidades o incidentes de seguridad.

Punto 7: los datos por si solos no indican o permiten conocer aspectos relevantes en un negocio. Sin embargo, el proceso de éstos es clave para que muchas áreas puedan cumplir a cabalidad con sus tareas. La administración de los datos en materia de su liberación, eliminación, recuperación y el mantenimiento que se les dé es importante. Ya que todo ello conlleva de manera conjunta con otras variables (equipo, recurso humano,

etc.) obtener información de calidad, oportuna y suficiente para satisfacer las necesidades de los usuarios.

La normativa estipula el siguiente proceso: *DS11 Administración de Datos* en relación con dicho punto. Para ello son varias las actividades que se pueden citar y resumen de manera clara lo indicado:

1. Una efectiva administración de datos requiere de la identificación de requerimientos de datos.

2. El proceso de administración de información también incluye el establecimiento de procedimientos efectivos para administrar la librería de medios, el respaldo y la recuperación de datos y la eliminación apropiada de medios.

3. Una efectiva administración de datos ayuda a garantizar la calidad, oportunidad y disponibilidad de la información del negocio.

4. Definir e implementar procedimientos de respaldo y restauración de los sistemas, aplicaciones, datos y documentación en línea con los requerimientos de negocio y el plan de continuidad.

La entidad debe administrar los datos apropiadamente de manera que se garantice la calidad, oportunidad y disponibilidad de la información del negocio. Debe tener procesos establecidos para el archivo, almacenamiento y retención de datos para conseguir los objetivos de negocio. Así mismo, debe implementar políticas para la seguridad aplicables al recibo, procesamiento, almacenamiento y salidas de los datos para conseguir los objetivos de negocio.

Punto 8: el monitoreo y la evaluación del control interno es un factor clave en el proceso efectivo de ejecución de TI y el logro de metas en las áreas relacionadas y la

organización como tal. La búsqueda por operaciones eficientes y eficaces, el procesamiento de datos suficientes y de calidad para los usuarios son otros de los logros que se pretenden con ello. Es por todo lo anterior que las revisiones constantes y no ocasionales son importantes.

La normativa estipula los siguientes procesos: *ME2 Monitorear y Evaluar el Control Interno* en relación con dicho punto. Para ello son varias las actividades que se pueden citar y resumen de manera clara lo indicado:

1. Establecer un programa de control interno efectivo para TI requiere un proceso bien definido de monitoreo.

2. Monitorear y crear reportes de las excepciones de control, resultados de auto-evaluaciones y revisiones por parte de terceros.

3. Proporcionar seguridad respecto a las operaciones eficientes y efectivas y el cumplimiento de las leyes y regulaciones aplicables.

Para cumplir con este proceso se debe cumplir con procedimientos anteriores donde se designe control interno a los proveedores, y se identifique la raíz de los problemas, los cuales deben ser retomados en este proceso para monitorear su avance o solución.

Todos estos procesos antes descritos son creados con la finalidad de que el sector regulado por esta institución cumpla a cabalidad con el proceso de gestión de las Tecnologías de Información. Dicha regulación permite la protección adecuada de su información y procesos relacionados con el fin de favorecer el cumplimiento de los objetivos de cada una de las instituciones y en apego a lo que la regulación del país así establece.

Punto 9: la puesta en marcha de un proceso de TI en un negocio es un tanto compleja; conlleva a realizar estudios a nivel de inversión y recursos versus resultados

esperados con la implementación, la consideración de temas operacionales, ambientales, legales y humanos. Así como la creación de elementos clave como son los planes y las tácticas estratégicas.

La normativa estipula el siguiente proceso: *P01 Definir un Plan Estratégico de TI* en relación con dicho punto. Para ello son varias las actividades que se pueden citar y resumen de manera clara lo indicado:

1. Definir una planeación estratégica de TI es necesario para gestionar y dirigir todos los recursos de TI en línea con la estrategia y prioridades del negocio. En resumen, generando y gestionando valor de TI para el negocio.

2. La función de TI y los interesados del negocio son responsables de asegurar que el valor óptimo se consigue desde los proyectos y el portafolio de servicios.

3. El plan estratégico mejora la comprensión de los interesados clave de las oportunidades y limitaciones de TI, evalúa el desempeño actual, identifica la capacidad y los requerimientos de recursos humanos, y clarifica el nivel de investigación requerido.

4. La estrategia de negocio y prioridades se reflejarán en portafolios y se ejecutarán por los planes estratégicos de TI, que especifican objetivos concisos, planes de acción y tareas que están comprendidas y aceptadas tanto por el negocio como por TI.

De acuerdo con lo estipulado anteriormente, las entidades supervisadas por la Superintendencia General de Entidades Financieras deben realizar un adecuado portafolio de inversiones de TI que le brinden valor a la entidad y permita a TI alinearse con los

objetivos organizacionales, y mediante un plan estratégico y un plan táctico cumplir con las medidas necesarias para llevar a cabo los proyectos de TI.

La planeación estratégica de TI debe estar en todo momento en línea y en total armonía con las metas de la organización. Que todos los componentes relacionados, llámese infraestructura TI, hardware, software o recurso humano, trabajen de manera conjunta y adecuada; en donde la eficiencia, eficacia, optimización de funciones y reducción de costos sean aspectos que los identifiquen. Todo lo anterior apegado a los factores internos y externos que de manera positiva o negativa interactúen con el negocio. Una planeación estratégica creada e implementada correctamente, así como un monitoreo continuo permite dar valor agregado a las funciones de la organización y cumplir con las metas establecidas.

Punto 10: es importante y clave que la administración tenga bien claro qué se desea obtener con la implementación de TI en su negocio (alcance de TI). Aspectos como un plan de infraestructura tecnológica, la claridad de los recursos con los que se cuenta para ello, así como el nivel de compromiso y aceptación influyen en gran manera con la dirección tecnológica.

Por otro lado, no solo debe verse esa dirección a corto plazo, es decir, considerando lo que se tiene y desea en el presente, sino más bien considerar factores externos (oportunidades de desarrollo y crecimiento, comportamiento de la industria, avances tecnológicos, entre otros) e internos (decisiones de la administración, fortalezas, objetivos anuales, entre otros) que pueden influir a futuro en esta implementación. Es por eso mismo, la importancia del proceso de monitoreo y seguimiento que debe darse para que la organización comprenda y esté en todo momento consciente de su posición en materia de TI.

La normativa estipula el siguiente proceso: *P03. Determinar la Dirección Tecnológica* en relación con dicho punto. Para ello son varias las actividades que se pueden citar y resumen de manera clara lo indicado:

1. La función de servicios de información debe determinar la dirección tecnológica para dar soporte al negocio.

2. Requiere de la creación de un plan de infraestructura tecnológica y de un comité de arquitectura que establezca y administre expectativas realistas y claras de lo que la tecnología puede ofrecer en términos de productos, servicios y mecanismos de aplicación.

3. El plan se debe actualizar de forma regular y abarca aspectos tales como arquitectura de sistemas, dirección tecnológica, planes de adquisición, estándares, estrategias de migración y contingencias. Esto permite contar con respuestas oportunas a cambios en el ambiente competitivo, economías de escala para consecución de personal de sistemas de información e inversiones, así como una interoperabilidad mejorada de las plataformas y de las aplicaciones.

Este proceso de COBIT establece que las entidades deben crear una planeación de la dirección tecnológica de TI para materializar la estrategia de TI, también sobre la creación de un plan de infraestructura para dicha área, y la importancia de establecer un comité de arquitectura de TI para proporcionar las directrices necesarias para el cumplimiento regulatorio y la estrategia del negocio.

Punto 11: los resultados de retorno para la organización a raíz de la implementación hecha en temas de TI varía debido a muchas variables que influyen. Una de ellas, y muy importante, viene a ser la inversión que se realice, otra es el mantenimiento, la adecuación a los cambios, entre otras. Todas ayudan a precisar mayormente, maximizar

las operaciones y recursos disponibles, así como lograr mejores resultados en temas de cumplimiento de objetivos y desempeño.

Ahora bien, la proyección que se tenga con las TI en el futuro de la organización y su presencia en el presupuesto anual va a hablar de lo que se quiere con ello; esto permite saber con qué se cuenta y evitar desembolsos no contemplados, proyectos inconclusos en el peor de los casos pérdidas para la empresa.

La normativa estipula el siguiente proceso: *P05. Administrar la Inversión en TI* el cual norma la administración de la inversión de Tecnologías de Información. Para ello son varias las actividades que se pueden citar y resumen de manera clara lo indicado:

1. Establecer y mantener un marco de trabajo para administrar los programas de inversión en TI que abarquen costos, beneficios, prioridades dentro del presupuesto, un proceso presupuestal formal y administración contra ese presupuesto.

2. Los interesados son consultados para identificar y controlar los costos y beneficios totales dentro del contexto de los planes estratégicos y tácticos de TI, y tomar medidas correctivas según sean necesarias.

3. El proceso fomenta la asociación entre TI y los interesados del negocio, facilita el uso efectivo y eficiente de recursos de TI, y brinda transparencia y responsabilidad dentro del costo total de la propiedad, la materialización de los beneficios del negocio y el retorno sobre las inversiones en TI.

Este proceso establece la necesidad de las entidades de administrar los programas de TI para una adecuada administración financiera de las inversiones realizadas. La entidad debe implementar un proceso para dar prioridad a la asignación de recursos del presupuesto

de TI así como un proceso de monitoreo de la contribución esperada de TI a los resultados de negocio.

Puntos 12 y 13: es fundamental que siempre las estrategias de TI vayan directamente en beneficio de los objetivos organizacionales. Que esas estrategias de TI puedan lograr con la maximización del uso de la infraestructura y los recursos con los que se cuenta. Clave es evitar la ociosidad de capacidades tecnológicas y humanas en el momento de implementación de las TI, pues ese no es el fin principal de su inclusión en las actividades del negocio.

Es importante crear una visión, a nivel de TI, con objetivos a largo plazo, considerando temas como la modificación o adecuación según así se requiera, sea por decisiones internas o propias del ambiente externo (flexibilidad tecnológica).

Tanto la infraestructura como los recursos de TI deben ser controlados de la manera correcta, los equipos deben funcionar correctamente y que procesen, en todo momento, los datos correspondientes de acuerdo con los requerimientos del usuario; por otro lado que el recurso humano responsable de TI esté en todo momento con la capacidad de resolver incidentes y busque la calidad de los servicios que se brindan a todas las áreas de la organización.

Los recursos de TI deben ser siempre de calidad, ajustados a lo que se desea obtener y apegado al presupuesto establecido para ello. Es aquí donde un estudio o planeación a nivel de selección de proveedores toma un papel clave, temas como responsabilidades, compromisos, calidad son de gran valor para ello.

Las organizaciones deben contar con procesos para adquirir, implementar y actualizar la infraestructura tecnológica. Esto requiere de un enfoque planeado para adquirir, mantener y proteger la infraestructura de acuerdo con las estrategias tecnológicas

convenidas y la disposición del ambiente de desarrollo y pruebas. Esto garantiza que exista un soporte tecnológico continuo para las aplicaciones del negocio.

La normativa estipula los siguientes procesos: *AI3 Adquirir y Mantener Infraestructura Tecnológica & AI5 Adquirir Recursos de TI* en relación con dicho punto. Para ello son varias las actividades que se pueden citar y resumen de manera clara lo indicado:

1. Generar un plan para adquirir, implementar y mantener la infraestructura tecnológica que satisfaga los requerimientos establecidos funcionales y técnicos del negocio, y que esté de acuerdo con la dirección tecnológica de la organización.

2. El plan debe considerar extensiones futuras para adiciones de capacidad, costos de transición, riesgos tecnológicos y vida útil de la inversión para actualizaciones de tecnología.

3. Evaluar los costos de complejidad y la viabilidad comercial del proveedor y el producto al añadir nueva capacidad técnica.

4. Suministrar recursos TI, incluyendo personas, hardware, software y servicios. Esto requiere de la definición y ejecución de los procedimientos de adquisición, la selección de proveedores, el ajuste de arreglos contractuales y la adquisición en sí. El hacerlo así garantiza que la organización tenga todos los recursos de TI que se requieren de una manera oportuna y rentable.

En este proceso se indica que las organizaciones deben contar con procesos para adquirir, implementar y actualizar la infraestructura tecnológica, el cual debe estar acorde

con la dirección tecnológica de la organización, también las entidades deben contar con revisiones periódicas para el mantenimiento de la infraestructura

Adicionalmente, la selección y control de los contratos con los proveedores son fundamentales para poder obtener los recursos que se necesitan en la organización, este proceso debe ser de acuerdo a una práctica justa, formal y de acuerdo con los requerimientos previamente especificados para la adquisición de los recursos que la administración indique.

Punto 14: no se puede poner en marcha las TI en un negocio y pretender que éstas actúen por sí solas, puesto que no es la clave para lograr el éxito y el cumplimiento de objetivos establecidos en un inicio. Es de allí que surge la importancia de administrar el desempeño y capacidad de éstas; la ejecución de revisiones periódicas en su ejecución, el cumplimiento de éstas para/con las necesidades del usuario, el logro de objetivos de TI establecidos (los cuales estarían ligados directamente con los objetivos organizacionales), así como el comportamiento ante cambios internos y externos en el negocio son factores que se deben considerar.

El seguimiento respectivo a todo lo anterior, la toma de decisiones justo a tiempo y el uso efectivo de la capacidad instalada son aspectos claves en este proceso.

La normativa estipula el siguiente proceso: *DS3 Administrar el desempeño y la capacidad* en relación con dicho punto. Para ello son varias las actividades que se pueden citar y resumen de manera clara lo indicado:

1. Administrar el desempeño y la capacidad de los recursos de TI requiere de un proceso para revisar periódicamente el desempeño actual y la capacidad de los recursos de TI.
2. Incluir el pronóstico de las necesidades futuras, basadas en los requerimientos de carga de trabajo, almacenamiento y contingencias.

3. Brindar la seguridad de que los recursos de información que soportan los requerimientos del negocio están disponibles de manera continua.
4. Monitorear continuamente el desempeño y la capacidad de los recursos de TI.

La información reunida sirve para dos propósitos:

- Mantener y poner a punto el desempeño actual dentro de TI y atender temas como elasticidad, contingencia, cargas de trabajo actuales y proyectadas, planes de almacenamiento y adquisición de recursos.
- Para reportar la disponibilidad hacia el negocio del servicio prestado como se requiere en los acuerdos de servicio. Acompañar todos los reportes de excepción con recomendaciones para acciones correctivas

El desempeño y la capacidad de los recursos de TI deben ser evaluados periódicamente mediante un proceso que brinde la seguridad de los recursos para garantizar que las inversiones realizadas en esta rama están dando los frutos deseados.

De igual forma se debe monitorear constantemente el desempeño para evaluar la necesidad de ajustes en los recursos de Tecnologías de Información.

Puntos 15 y 16: la bitácora o el portafolio en el proceso de configuración de TI y problemas de TI es clave. Sirve para tener un panorama y entender los eventos históricos relacionados versus la situación real.

Por otro lado, la categorización de los problemas permite conocer y saber cómo se puede responder a ellos. Variables como la causa, la consecuencia, el impacto, las soluciones, la prioridad, entre otros son importantes a considerar en este proceso.

La normativa estipula los siguientes procesos: *DS9 Administrar la Configuración & DS10 Administración de Problemas* en relación con dicho punto. Para ello son varias las actividades que se pueden citar y resumen de manera clara lo indicado:

1. Garantizar la integridad de las configuraciones de hardware y software requiere establecer y mantener un repositorio de configuraciones completo y preciso.
2. Incluir la recolección de información de la configuración inicial, el establecimiento de normas, la verificación y auditoría de la información de la configuración y la actualización del repositorio de configuración conforme se necesite.
3. Una efectiva administración de la configuración facilita una mayor disponibilidad, minimiza los problemas de producción y resuelve los problemas más rápido.
4. Una efectiva administración de problemas requiere la identificación y clasificación de problemas, el análisis de las causas desde su raíz, y la resolución de problemas.
5. El proceso de administración de problemas también incluye la identificación de recomendaciones para la mejora, el mantenimiento de registros de problemas y la revisión del estatus de las acciones correctivas. Un efectivo proceso de administración de problemas mejora los niveles de servicio, reduce costos y mejora la conveniencia y satisfacción del usuario

Esta normativa obliga a las entidades a mantener un repositorio de configuraciones completo y preciso, se deben establecer procesos de verificación y auditoría de la configuración y la actualización del repositorio de configuración con el fin de agilizar la solución a los problemas que se presenten. De igual forma, y a nivel de la administración de los problemas, debe conocer el esfuerzo y recursos necesarios en atenderlos para valorar las posibilidades de mejorar los procesos para minimizar los problemas.

Punto 17: no está de más indicar nuevamente la importancia que tiene la planeación, la dirección, la implementación, el uso y el seguimiento de manera adecuada que se le dé a las TI en una organización. Puesto que son muchos los aspectos del ambiente que pueden variar lo pensado en un inicio por la administración. El ambiente físico es clave en ello, desde la influencia de leyes o regulaciones, la protección y seguridad de la salud hasta el acceso al edificio, a las áreas relacionadas y los equipos de TI.

La normativa estipula el siguiente proceso: *DS12 Administración del Ambiente Físico* en relación con dicho punto. Para ello son varias las actividades que se pueden citar y resumen de manera clara lo indicado:

1. La protección del equipo de cómputo y del personal, requiere de instalaciones bien diseñadas y bien administradas.
2. Administrar el ambiente físico incluye la definición de los requerimientos físicos del centro de datos, la selección de instalaciones apropiadas y el diseño de procesos efectivos para monitorear factores ambientales y administrar el acceso físico.
3. La administración efectiva del ambiente físico reduce las interrupciones del negocio ocasionadas por daños al equipo de cómputo y al personal.

La entidad está obligada a mantener los equipos de cómputo en ambientes físicos apropiados, en instalaciones que cumplan con los requerimientos físicos del centro de datos con el objetivo de reducir la posibilidad de interrupciones causadas por daños a los recursos físicos de TI, el lugar donde se coloque el centro de datos físicos debe tomar en cuenta el riesgo de desastres naturales y causados por el hombre.

Este proceso obliga a la entidad a restringir el acceso físico al edificio y áreas de acuerdo con las necesidades del negocio, de igual forma la entidad debe mantener un registro de los accesos del personal, clientes, proveedores, visitantes o cualquier tercero.

Con lo anterior se da por concluido el conocimiento de la normativa que cubre al sector regulado por CONASSIF en Costa Rica.

3.3 Análisis comparativo de las normativas aplicables de la Contraloría General de la República y por el Consejo Nacional de Supervisión del Sistema Financiero.

Este análisis comparativo estará enfocado desde la óptica de control interno que valorará cuáles de las regulaciones podrían adaptarse a las fundaciones para realizar una gestión eficiente y suficiente de la seguridad y control de la información.

El análisis se realizará de acuerdo con los dominios que abarcan las actividades necesarias para gobernar efectivamente las Tecnologías de Información, los mismos se utilizan por instituciones internacionales como el ISACA para categorizar los procesos de acuerdo con las áreas que deben ser administradas por las organizaciones para garantizar una adecuada gestión de la información:

- Planear y Organizar
- Adquirir e Implementar
- Entregar y dar soporte
- Monitorear y Evaluar

Es importante tomar en cuenta que en este análisis se determinan ambas normativas de manera general con el fin de realizar una comparación equitativa, dado que ambas normas difieren en sus lineamientos y su análisis específico se realiza en los apartados 3.1 y 3.2 de este capítulo.

Planear y Organizar

La normativa aplicable por SUGEF estipula la ejecución, de carácter obligatorio, de los siguientes procesos en este dominio:

PO1 Definir un plan estratégico de TI

PO3 Determinar la dirección tecnológica

PO5 Administrar la inversión en TI

PO9 Evaluar y administrar los riesgos de TI

PO10 Administrar proyectos

Por otra parte, las normas técnicas de TI de la Contraloría General de la República de Costa Rica abarcan este dominio en dos capítulos: Cap. I Normas de aplicación general y Cap. II Planificación y Organización desarrollados en apartados anteriores.

Tanto la normativa de SUGEF como las Normas Técnicas de la CGR, a grandes rasgos explican que se debe gestionar y dirigir todos los recursos de TI en línea con la estrategia y prioridades del negocio para generar valor real de TI en el negocio. Se deben establecer prioridades evidenciadas en portafolios y que se ejecutarán de acuerdo con los planes estratégicos de TI.

La normativa SUGEF establece la creación de un plan de infraestructura tecnológica y de un comité de arquitectura que establezca y administre expectativas realistas de lo que se espera obtener. Y hace hincapié en la necesidad de actualizar de forma regular el plan para poder contar con respuestas oportunas a cambios en el ambiente competitivo.

También determina que la gestión adecuada de riesgos de TI ayuda enormemente a prevenir factores que puedan crear imprevistos no deseados que afecten el logro de los objetivos de la organización, por lo mismo se debe crear un marco de trabajo de administración de riesgos que indica la valoración de los riesgos, y las estrategias de mitigación de los mismos.

Otro aspecto importante que menciona la normativa SUGEF es que la administración de proyectos crea dentro de la organización una cultura de compromiso, responsabilidad, identificación y unión por parte de las áreas o responsables en cada uno de los proyectos que se desarrollan, dado que tienen un tiempo de ejecución y culminación definidos.

Por otra parte las Normas Técnicas de la CGR establecen que la organización debe lograr que las TI apoyen su misión, visión y objetivos estratégicos mediante procesos de planificación que logren el balance óptimo entre sus requerimientos, la estandarización de los sistemas de información de manera que los procesos de información se lleven a cabo de forma completa, exacta y oportuna. También determina que la organización debe optimizar el uso de los recursos financieros invertidos en la gestión de TI.

Asimismo, establece que la organización debe tener una perspectiva clara de su dirección y condiciones en materia tecnológica para lograr un uso óptimo de su infraestructura, y establece al jerarca como responsable de asegurar la independencia de la función de TI, respecto a las áreas usuarias.

De esta forma se concluye que para la planificación y organización de las Tecnologías de Información financiera, la normativa aplicable por la SUGEF para las entidades supervisadas comprende lineamientos más específicos que abarcan temas de riesgos, optimización de recursos, portafolio de inversiones, administración de proyectos y la necesidad de los diferentes controles para la correcta ejecución de la misma, mientras que el sector regulado por la Contraloría establece de manera más general lineamientos y

deja a la administración de las organizaciones su aplicación específica dado que no define un alcance explícito a sus entidades reguladas.

Adquirir e Implementar

Para el dominio de Adquirir e Implementar, la Superintendencia establece los siguientes procesos obligatorios que deben acatar las entidades reguladas:

AI3: Adquirir y mantener infraestructura tecnológica.
AI5: Adquirir recursos de TI.
AI6: Administrar cambios.

La entidad al implementar estos procesos, podrá establecer procedimientos, procesos, sistemas y parámetros que permitan administrar los cambios de la infraestructura de Tecnologías de Información.

Así mismo, establece criterios mínimos que se deben tomar en cuenta a la hora de adquirir servicios de TI de terceros, al cumplir con lo establecido por el marco de trabajo la entidad tendrá procesos adecuados para mitigar los riesgos asociados con la contratación de terceros y garantizar la confidencialidad de la información y una adecuada adquisición de los servicios necesarios.

Mientras tanto la Contraloría General de la República de Costa Rica define los procesos mencionados a continuación para la 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.

La Contraloría General de la República por su parte establece que las entidades deben tener claras las políticas sobre la justificación, autorización y documentación de las solicitudes de implementación o mantenimiento de TI, debe contar entre otros criterios con una definición clara y completa de los requerimiento y tomar las previsiones correspondientes para garantizar la disponibilidad de los recursos necesarios, también obliga a establecer estrategias para minimizar el riesgo de que lo adquirido no logre su objetivo.

Al igual que la Superintendencia, establece procesos para garantizar que al adquirir servicios de terceros se logre satisfacer las necesidades para lo cual fue contratado, mediante una estructura que defina políticas y permita controlar el proceso de adquisición e implementación de los recursos.

Entregar y dar soporte

En cuanto al dominio de Entregar y Dar Soporte del Marco de Trabajo de COBIT, la SUGEF 14-09 presenta como requerimiento obligatorio para las organizaciones reguladas ejecutar y adoptar los siguientes procesos:

DS2 Administrar los servicios de terceros.
DS3 Administrar el desempeño y la capacidad.
DS4 Garantizar la continuidad del servicio.
DS5 Garantizar la seguridad de los sistemas.
DS9 Administrar la configuración.
DS10 Administrar los problemas.
DS11 Administrar los datos.
DS12 Administración del ambiente físico.

Estos son enfocados a grandes rasgos en la Administración General de los recursos de TI, dentro de los cuales se enfatiza la correcta gestión para asegurar la continuidad del negocio y su operación.

Dentro de este dominio se abordan los temas relacionados con los servicios que necesitan las organizaciones para el uso óptimo de las Tecnologías de Información, dentro de éstas se encuentra la administración de la seguridad y de la continuidad, administración de datos y soporte de servicio a los usuarios.

Esto revela la importancia de dar soporte a los recursos que posea cada organización en cuanto a Tecnologías de Información, relacionado con las prioridades del negocio, optimización de costos de actualización, utilización de los recursos en cuanto a productividad, seguridad y confiabilidad, disposición e integridad de los datos.

Este proceso debe estar ligado a los dominios Planear y Organizar (PO) y Adquirir e Implementar (AI), pues es importante que sea considerado dentro de los mismos con el fin de mantener recursos económicos suficientes para su aplicación y desarrollo.

Por lo que en forma más específica el COBIT describe las requisiciones mínimas para una adecuada gestión al entregar y dar soporte detallando 13 procesos con los que se busca recibir los resultados de las diferentes soluciones que se presenten y hacerlas viables y utilizables por los usuarios finales.

Mientras tanto la Contraloría General de la República de Costa Rica define los procesos mencionados a continuación para la 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.

Estos están implícitos en el Manual de Normas Técnicas de TI de la Contraloría General de la República de Costa Rica. Y dentro de los mismos se abarca de forma muy general la claridad que deben poseer las distintas organizaciones bajo su regulación, con respecto a los servicios que son necesarios según la capacidad de las Tecnologías de Información.

También hace hincapié en el mantenimiento adecuado de estos recursos para la optimización de la operación con el fin mitigar el riesgo de fallas que se puedan presentar, así mismo, hace referencia a la importancia del procesamiento de datos, tanto a nivel de integridad y exactitud, como de niveles de jerarquización en cuanto a autorizaciones y seguridad de la información.

La Contraloría General de la República de Costa Rica tiene claro en este capítulo que es de suma importancia atender los requerimiento que surjan en el transcurso de la operación con el fin de minimizar costos y reconocer de manera oportuna cualquier error, problema o incidente que se pueda presentar, con el fin de que los servicios satisfagan las necesidades de los usuarios.

Monitorear y Evaluar

Este es el cuarto y último dominio que colabora para el logro de un gobierno eficiente de las Tecnologías de Información. Según COBIT se abarca la gestión del desempeño de TI, se mide el control interno asociado, se procura un apego a las normas regulatorias asociadas y finalmente una aplicación de Gobierno de TI en donde se busca la alineación de estrategias de TI con estrategias del negocio, implementación de nuevos

sistemas, la ejecución de procesos organizacionales y el logro de objetivos organizacionales.

Para el análisis comparativo de lo que dicta la normativa aplicable por SUGEF y las Normas Técnicas aplicables por la Contraloría en este apartado, se puede indicar que su enfoque para que sea ejecutado por el sector que le compete es muy similar.

Para el caso de la normativa 14-09 de la SUGEF, su centro de ejecución se basa, y es estipulado de carácter obligatorio para las entidades que les rige, en el proceso COBIT *ME2 Monitorear y Evaluar el Control Interno*. Este proceso dicta la creación de un programa específico en temas de control interno efectivo para TI y su respectivo monitoreo de manera continua, la ejecución de reportes asociados, revisiones por parte de terceros y que se brinde la seguridad en temas asociados con las operaciones y el cumplimiento de las leyes y regulaciones aplicables. Adicionalmente, indica el enfoque principal de dicho proceso, cómo se logra, cuáles son los objetivos de control asociados y cuál es su métrica de ejecución y cumplimiento. Para concluir y no menos importante se da una referencia de matriz RACI que puede ser ejecutada por la organización que implemente.

Así mismo, esta normativa hace mención a procesos ligados al dominio de Monitorear y Evaluar, los cuales son de carácter optativos y selectivos acordes al perfil del área de TI con el que cuenta cada organización. Dan ampliación importante en este campo para la consecución de los objetivos establecidos. Estos son ME1 Monitorear y Evaluar el desempeño de TI, ME3 Garantizar el cumplimiento regulatorio y ME4 Proporcionar Gobierno de TI.

Por otra parte, las Normas Técnicas de TI de la Contraloría General de la República C.R centran su atención en este dominio a partir del desarrollo de tres aspectos claves: 1. Monitoreo, 2. Mejora continua y 3. Retroalimentación.

A partir de lo anterior, se evidencia en las Normas Técnicas que la administración debe establecer y mantener el sistema de control interno asociado con la gestión de las TI, evaluar su efectividad, cumplimiento, mantener un registro de las excepciones que se presenten y de las medidas correctivas implementadas. Por otro lado, dar seguimiento técnico en materia de la mejora continua de la seguridad de la información (necesidades organizacionales, globalización, regulaciones vigentes) y finalmente la inclusión del departamento de auditoría interna en la gestión de TI es clave (evaluación de efectividad, cumplimiento y recomendaciones de mejora o corrección).

En resumen, se puede indicar que para ambas normativas el proceso de una implementación de Control Interno de TI adecuado es un aspecto predominante, esto debido a que es el tema en el que se hace mayor mención; así como el proceso de mejora continua.

No obstante, las Normas Técnicas de la Contraloría son criterios básicos de control y muy breves en términos de responsables, recursos y ejecución. Diferente de lo que puede verse en la normativa SUGEF puesto que su aplicación ligada de manera directa a un proceso de COBIT, permite conocer mejor los requerimientos y finalidades que se desean obtener; el contar con matrices de responsabilidad, métricas de desempeño y desarrollo la hace de gran interés.

Ahora bien, sí se denota que en ambas normativas no se realiza detalle suficiente de cómo ejecutar de manera clara y concisa dichos procesos, lo cual es importante para que las instituciones que deben implementarlo estén más claras y cuenten metodológicamente con una norma que así se los dicte.

Con lo anterior se evidencian las similitudes y diferencias que existen entre ambas normativas, y permite analizar la rigurosidad con que se aplica en el sector regulado tanto por la Contraloría General de la República como por el CONASSIF. De esta forma se determina que la SUGEF al aplicar los procesos que define como obligatorios de COBIT,

establece un marco más robusto que el de la Contraloría General de la República, dado que estás últimas dan un margen de interpretación que permitiría a las entidades aplicar y cumplir con lo estipulado de diversas formas.

Capítulo IV. Propuesta de una metodología para la evaluación y administración de la seguridad y control de la información en Tecnologías de Información.

4.1 Propósito de la metodología.

El propósito de esta propuesta es brindar una metodología para el control y seguridad de la información que las fundaciones o cualquier organización que no cuente con una regulación específica pueda acoger como una medida, con el fin de mejorar el control y la seguridad de la información y consecuentemente mejorar su gestión administrativa, minimizar los riesgos asociados a su operación y de rendición de cuentas.

Esta metodología proporcionará herramientas valiosas para la gestión de la seguridad y control de la información, agilizando la identificación, evaluación y gestión de los mismos en aquellas entidades que opten por aplicarla.

4.2. Bases normativas en las que se fundamenta de la metodología.

Las normativas que funcionarán como bases de la propuesta realizada son los marcos regulatorios aplicables a nivel nacional; primeramente se encuentra el Acuerdo SUGEF 14-09 *Normas técnicas para la gestión y el control de las Tecnologías de Información* una amplia guía basada en COBIT, específicamente en la aplicación de 17 procesos que el CONASSIF considera esenciales y obligatorios para la adecuada gestión de las Tecnologías de Información; y además se encuentran las *Normas técnicas para la gestión y el control de las Tecnologías de Información* donde se definen las diferentes características que deben tener los entes supervisados por la Contraloría General de la República para tener un adecuado control interno en esta área, dichas Normas han sido analizadas en el Capítulo III.

4.3. Propuesta de una metodología para la gestión de la seguridad y control de la información en Tecnologías de Información.

Metodología para la gestión de la seguridad y control de la información en Tecnologías de Información

PROCESO 1: Planificar y Organizar

Basado en:

COBIT PO.1, PO.2 y PO.3
Normas Técnicas CGR 1.1 y 2.1

La visión estratégica de TI permite a la entidad organizar el Departamento de Tecnologías de Información para que se alinee con las metas organizacionales y administración de riesgos, generando valor agregado en los procesos críticos mediante políticas organizacionales que el personal comprenda para gestionar y dirigir todos los recursos de TI en línea con la estrategia y prioridades de negocio.

Los sistemas deben estar enfocados en utilizar de manera eficiente y eficaz los recursos de las Tecnologías de Información, de esta forma la estrategia del negocio estaría apoyada por los sistemas de TI y se garantiza que la información necesaria para la toma de decisiones sea íntegra y segura.

Subproceso: PO-01 Visión estratégica de TI.

Para llevar a cabo una adecuada visión estratégica de TI es necesario elaborar un plan estratégico de TI, que debe contemplar como mínimo los siguientes puntos y contará con la aprobación del director ejecutivo:

Actividad: PO-01-01: Entendimiento de los riesgos, capacidades y necesidades actuales de TI.

PO-01-01.01 El departamento de TI con la supervisión del jefe informático debe realizar una identificación de los riesgos de TI. tanto por departamento y a nivel general del negocio, esto lo hará a partir de reuniones programadas con los directores correspondientes en donde se abarcará temas relacionados con su proceso, transacciones, autorizaciones, recursos, entre otros; se toman apuntes e información relacionada que pueda ser suministrada y con ello se tendrá cierta claridad de los riesgos relacionados con TI que pueden existir.

PO-01-01.02 El departamento de TI con la supervisión del jefe informático debe evaluar las capacidades y necesidades actuales de los recursos de TI por departamento y a nivel general del negocio, mediante un análisis de la eficiencia, efectividad, confiabilidad, disponibilidad e integridad de los sistemas actuales. Para ello se deben revisar los sistemas operativos, versiones, antivirus de los equipos con los que cuentan, además de reuniones con los directores y departamento respectivo para conocer su punto de vista en materia de necesidades en mejora de su desempeño actual.

PO-01-01.03 El departamento de TI con la supervisión del jefe informático debe reunirse y presentar un informe a las direcciones de los departamentos del negocio que incluya los riesgos, capacidades y necesidades actuales de TI identificadas en los dos puntos anteriores para la mejora de los recursos existentes.

Actividad: PO-01-02: Aplicación de esquemas de prioridades para que el plan estratégico de TI cubra los objetivos del negocio.

PO-01-02.01: El jefe de informática, en consulta con los directores de cada uno de los departamentos del negocio, debe realizar un listado y priorizar los componentes críticos o de mayor significancia para el desarrollo de sus funciones; los cuales deben ser cubiertos con los recursos requeridos para cubrir las necesidades expuestas en el punto anterior.

PO-01-02.02: El jefe de informática debe crear un esquema a partir de la tarea anterior, el cual sirva de herramienta para la toma de decisiones de la organización, visión estratégica y acorde al logro de los objetivos del negocio.

Actividad: PO-01-03: Establecimiento de un plan de trabajo y recursos tecnológicos de acuerdo con el presupuesto, los riesgos identificados y necesidades de la organización.

PO-01-03.01: El jefe de informática debe reunirse con el director financiero y el director ejecutivo para que a partir del informe presentado y esquema de priorización de componentes críticos por departamento, se establezca un rubro dentro del presupuesto que permita dar cobertura financiera en materia de la minimización de riesgos identificados y poder solventar necesidades indicadas.

PO-01-03.02: El departamento de TI con la supervisión del jefe informático debe crear un plan de trabajo y recursos tecnológicos que indique objetivos, responsables, necesidades a solventar, tiempos de ejecución, controles asociados, entre otros. Todo ello acorde con las actividades desarrolladas anteriormente y de acuerdo con el presupuesto aprobado para ello.

PO-01-03.03: El jefe de informática debe reunirse y presentar el plan de recursos tecnológicos a las direcciones de los departamentos del negocio. Los cuales analizarán, realizarán preguntas y procederán a dar su aprobación.

Para cumplir con lo anterior es necesario contar con lo siguiente:

- Apoyo de la administración en materia de acceso a la información requerida, recursos necesarios, directrices a los departamentos asociados, entre otros.

- Plan estratégico de la organización, esto para enfocar los esfuerzos de una manera eficiente y eficaz con el fin de no perder recursos por falta del mismo, que buscaría cumplir los objetivos de la organización.

- Plan anual operativo, debe estar alineado con el Plan estratégico de la organización. Este no puede ir separado de cada área de la entidad, incluido el departamento de TI, por lo que el encargado del departamento en conjunto con la administración, deben velar porque las actividades diarias, semanales, etc. vayan de la mano con las metas que se plantearon en el plan anual.

- Presupuesto anual de la organización, a partir del análisis de necesidades del departamento de TI y relacionados, y junto al área financiera hay que dedicar una parte del presupuesto anual para cobertura de las necesidades, sin dejar de lado otras áreas.

- Análisis de la valoración de riesgos organizacionales, es un punto de partida para futuros cambios, para mejorar la situación actual. También es con este que se dota el nivel de urgencia de los cambios que fuesen necesarios.

- Informe detallado del estatus de los recursos de TI, este informe iría de la mano con el análisis de necesidades y riesgos de TI, pues a partir de este se justifican cambios en la organización.

Subproceso: PO-02 Estructura organizacional y tecnológica

Basado en:

COBIT PO.4
Normas Técnicas CGR 1.4

La estructura organizacional de Tecnologías de Información debidamente planificada, permite a la entidad establecer funciones, roles y responsabilidades, para que el

personal lleve a cabo de la mejor manera los procedimientos establecidos de acuerdo con las políticas administrativas y alineados con la visión estratégica ya establecida.

Por otro lado, la estructura tecnológica es clave para la ejecución de las actividades; las herramientas necesarias para que el departamento de TI pueda ejecutar de manera eficaz y eficiente sus funciones. Aspectos como la calidad, el número, la especialidad, entre otros referentes a la adquisición y conformación de la estructura, van acorde con las demandas y necesidades por parte de la organización, es por ello que la toma de decisiones en conjunto con las direcciones departamentales es muy importante.

Para que la Junta Directiva, direcciones y departamentos de la organización cumplan un papel activo en esta etapa, deben tener claro los procesos asociados y la relación de las diferentes áreas con las Tecnologías de Información.

Para lograr una adecuada estructura organizacional y tecnológica es necesario contemplar como mínimo los siguientes puntos:

Actividad: PO-02-01: Procesos asociados a la Estructura organizacional y tecnológica.

PO-02-01.01: El jefe informático debe definir estructuras y relaciones organizacionales para TI tales como ¿a quién reporta?, objetivos y tamaño del departamento, roles y responsabilidades, ubicación en el organigrama y físicamente, entre otros; además de la independencia del departamento pero que sea flexible, objetiva y capaz de responder a las demandas que el negocio necesite. Todo ello debe quedar aprobado y documentado en las políticas organizacionales.

PO-02-01.02: El jefe informático debe contar con el personal adecuado en el departamento de TI, para ello y con apoyo del departamento de Recursos Humanos se establece un perfil de puestos acorde con lo que indican las políticas organizacionales

relacionadas y necesidades del negocio; quién cumpla a cabalidad y se ajuste al presupuesto destinado puede formar parte del departamento.

PO-02-01.03: El jefe informático debe definir de manera clara el diseño y la utilidad de la estructura tecnológica que el negocio necesita para optimizar el desempeño y ejecución de sus procesos críticos -considerar el actividad PO-01-01 y PO-01-02. Para ello debe elaborar una guía que defina objetivos, alcances, roles y responsabilidades, espacio físico, mediciones de desempeño, entre otros. El presupuesto con el que se cuenta es clave también que sea considerado –ver actividad PO-01-03-.

Actividad: PO-02-02: Procedimientos para todas las funciones con atención especial al control y aseguramiento de calidad.

PO-02-02.01: El director ejecutivo debe establecer un manual de procedimientos donde se defina explícitamente cómo llevar a cabo las funciones para cada puesto que integre el departamento de TI, incluyendo el puesto de jefe informático. Estos procedimientos deben estar enfocados a mitigar los riesgos mediante un control asociado y aseguramiento de la calidad acorde con la adecuada segregación de funciones. Todo ello debe quedar aprobado y documentado en las políticas organizacionales.

Actividad: PO-02-03: Políticas de administración

PO-02-03.01: El director ejecutivo debe implementar y mantener las políticas indicadas en las actividades anteriores, además debe realizar un análisis para tener certeza de que en todo momento dichas políticas se encuentran alineadas con su marco estratégico, planificación y modelos de TI.

PO-02-03.02: El director ejecutivo debe comunicar las políticas que dirigen los procesos de TI a todos los departamentos del negocio. Esto lo debe hacer vía digital o documental.

PO-02-03.03: El departamento de control debe asegurar que dichas políticas se encuentren debidamente documentadas, revisadas, mantenidas, aprobadas, almacenadas y comunicadas. Esto lo puede hacer de manera periódica acorde con su plan de trabajo y debe llevar una bitácora o control digital de hallazgos y conclusiones.

Actividad: PO-02-04: Administración de riesgos y seguridad de la información (a nivel de estructura organizacional)

PO-02-04.01: El jefe de informática debe formular y ejecutar estrategias de implementación que incluyan todas las medidas para minimizar el riesgo de que no se cumplan los objetivos previamente establecidos en la visión estratégica. Medidas como el monitoreo continuo, la medición del desempeño, porcentajes de avance a los objetivos establecidos, reuniones periódicas con las direcciones de los departamentos, entre otros.

PO-02-04.02: El jefe de informática debe presentar de manera periódica, según así se indique, un reporte de resultados a las direcciones del negocio.

PO-02-04.03: El director ejecutivo tomará las decisiones correspondientes, según así sean necesarias, ante el reporte presentado y comunicación con las direcciones.

PO-02-04.04: El director ejecutivo debe definir y asignar los roles y responsabilidades críticas para la administración de riesgos de TI y de la seguridad de la información.

Para poder realizar una apropiada estructura organizacional es necesario contar con los siguientes recursos.

- Marco de trabajo de procesos que dicte cómo se segregarán las funciones, y defina explícitamente cómo llevar a cabo las mismas para cada puesto que integre el departamento de TI. También que puntualice objetivos y responsabilidades, figuras superiores, es decir a quién se reporta, con su debido flujograma y organigrama.

- Manual de políticas (y procedimientos), estas son las que dictarían qué posición tiene la administración, el empleado, el usuario, etc en diferentes situaciones, como una sola organización. Por lo que es importante que toda la organización las conozca.
- Manual de procedimientos, es necesario tener un manual de procedimientos, bien detallado, de toda actividad para cada posición; no importa si es una posición con actividades complejas o simples. Siempre es importante tenerlo a la mano y actualizado, pues con este es que los diferentes roles no dejen de realizar las actividades que les compete o no realizarlas al 100% por desconocimiento de sus responsabilidades.
- Flujogramas de los procesos de la organización, los cuales servirán para observar el flujo de las diferentes y múltiples actividades de cada área dentro de la organización. También definirían junto al manual de procedimientos sobre quién recaen las actividades y hasta dónde llegan sus obligaciones.

Subproceso: PO-03 Gestión de proyectos

Basado en:

COBIT PO.6, PO.8 y PO.10
Normas Técnicas CGR 1.5 y 1.2

Dentro de las tareas de planificación es necesario que se realice un marco de trabajo sobre los proyectos de la entidad, con el fin de que se garantice la correcta administración de los proyectos. Lo anterior con el fin de definir de manera correcta la asignación de recursos, responsables, determinación de fases, una adecuada administración de los riesgos de los proyectos y por ende establecer una metodología que permita asegurar el valor y la calidad de los mismos.

Este enfoque permite minimizar los riesgos de cancelación de proyectos, así como un control estricto en la ejecución de estos, minimizando costos inesperados y mejorando la

comunicación, y de esta forma los resultados serían entregados en el tiempo, presupuesto y calidad definidos.

Para lograr una adecuada gestión de los proyectos de la organización es necesario cumplir con lo siguiente:

Actividad: PO-03-01: Realizar un marco de trabajo para la administración de proyectos:

El jefe de informática debe realizar un programa de los proyectos donde se definan los siguientes criterios:

PO-03-01.01. Conformación de la cartera de proyectos: se deben determinar los proyectos que se van a realizar, los cuales deben estar acordes con el programa de inversiones.

PO-03-01.02. Evaluación de los proyectos: se debe realizar una evaluación de cada uno de los proyectos en apoyo con el departamento de TI definidos en la identificación. Esto considerando el esquema de componentes críticos departamentales y el plan de recursos tecnológicos anteriormente elaborado; además de cualquier anotación que los directores por departamento deseen hacer.

PO-03-01.03. Priorización y selección: con base en la evaluación, se da prioridad y se seleccionan para su ejecución a partir de los criterios considerados y que son aquellos con mayor grado de criticidad para el logro de los objetivos organizacionales.

PO-03-01.04. Administración y control: En apoyo con el departamento de TI se debe determinar la metodología (según PMI) para administrar y controlar los proyectos. La cual será presentada a las direcciones del negocio para su aprobación.

PO-03-01.05. Establecer las fases del proyecto: En apoyo con el departamento de TI se debe indicar las fases definidas en las que estará conformado todo proyecto, esto es clave pues crea una herramienta para el control de los mismos.

Actividad: PO-03-02: Realizar un plan integrado del proyecto

PO-03-02.01: El jefe de informática debe realizar un plan para guiar la ejecución y control del proyecto. Este plan debe contener como mínimo objetivos, responsables, alcances, tiempos de ejecución, recursos asignados, controles asociados, entre otros.

PO-03-02.02: El departamento de TI debe documentar todas las actividades del mismo.

Actividad: PO-03-03: Administración de riesgos del proyecto

PO-03-03.01: El jefe de informática debe establecer una metodología que permita a la administración identificar, evaluar, administrar y monitorear los riesgos de cada proyecto.

Actividad: PO-03-04: Medición del desempeño, reporte y monitoreo de los proyectos.

PO-03-04.01: El director ejecutivo debe establecer una medición del desempeño de los proyectos. Esto debe estar basado en la planificación de los proyectos y sus fases, las cuales servirán como base de comparación durante la ejecución de los mismos. También se deben tomar en cuenta el alcance, el cronograma, los costos y riesgos del plan inicial y sus fases a la hora de realizar el monitoreo; el mismo debe ser oportuno para garantizar que las medidas correctivas sean aplicadas apropiadamente, en caso de ser necesario.

PO-03-04.02: El jefe de informática debe reportar de manera periódica a los directores del negocio el estatus de los proyectos activos, o en su caso, cuando así lo solicite alguno de ellos para consulta o toma de decisiones asociadas.

Actividad: PO-03-05: Cierre del proyecto.

PO-03-05.01: Al finalizar cada proyecto el jefe de informática debe realizar un análisis de los resultados y beneficios esperados en comparación con lo planificado.

PO-03-05.02: El jefe de informática debe preparar un informe de descargo y presentarlo de manera clara y breve a las direcciones del negocio, en este momento debe responder a cualquier consulta y rendirá cuentas por ello.

PO-03-05.03: El departamento de TI con la supervisión del jefe informático debe identificar, recabar y documentar todo aspecto de importancia desde el inicio y hasta al finalizar cada proyecto. Lo anterior servirá de retroalimentación para la ejecución de futuros proyectos.

Para cumplir con lo anterior es necesario contar con lo siguiente:

- Plan Anual Operativo, toda organización cuenta con objetivos a corto, mediano y largo plazo. En este PAO, se tiene que detallar muy bien qué corresponde a cada área, incluida el área de TI; y es aquí donde el área va a tener una visión organizacional de dónde se dirige la misma, de dónde se van a derivar los proyectos a realizar.
- Plan estratégico, esto pues si no se tiene una estrategia a seguir para cumplir los objetivos organizacionales, no se van a enfocar los esfuerzos de una manera eficiente y eficaz y se pueden perder valiosos recursos por falta del mismo.
- Presupuesto anual, esto es importante destacar, ya que hay que considerar con cuántos recursos se cuenta para trabajar en el año y utilizarlos de manera eficiente de acuerdo con los proyectos u objetivos establecidos; también dentro del mismo tiene que haber una parte para eventualidades dentro de los proyectos.
- Apoyo de las áreas involucradas, si bien el proceso va más enfocado al área de TI, hay que tener en cuenta que no solo se va a ver afectada la misma, sino también

toda la organización, por lo que el resto de las áreas deben estar igualmente enfocadas en los objetivos del PAO.

- Reporte anual de avance y cierre de proyectos, en donde debe contemplar tiempos-costos-alcances), en este apartado la administración podrá usar métricas de desempeño como los son: ROI (retorno sobre la inversión), VAN (valor actual neto) y TIR (tasa interna de retorno). Si bien cada proyecto tiene que ir de la mano con los objetivos previamente establecidos, es sumamente necesario tener un reporte de avance de proyectos pues es en el mismo en que se evidencia el grado de avance y porcentaje para su conclusión.

Subproceso: PO-04 Uso óptimo de los recursos.

Basado en:

COBIT PO.5 Y PO.7
Normas Técnicas CGR 1.4.2

Un marco de trabajo para el uso óptimo de los recursos permite a la organización ser eficiente en sus inversiones de Tecnologías de Información al identificar y controlar los costos definidos en los presupuestos. También brinda transparencia y responsabilidad dentro del costo total de las inversiones en TI.

Para garantizar un óptimo uso de los recursos es necesario que los programas de TI. abarquen los siguientes puntos:

Actividad: PO-04-01: Control financiero sobre las inversiones de Tecnologías de Información

PO-04-01.01: El director financiero debe crear un marco de trabajo para controlar inversiones realizadas y presupuestadas de Tecnologías de Información. Debe considerar desde el alcance y los objetivos de esta herramienta hasta aspectos como roles y

responsabilidades, cronograma de cumplimiento de proyectos, presentación de reportes de avance, controles de desembolsos, autorizaciones, costos de cada fase invertida en el área de TI (interna y a nivel de proyectos de apoyo), entre otros.

Actividad: PO-04-02: Priorización del presupuesto definido

PO-04-02.01: El jefe de informática debe asignar prioridades a las operaciones, proyectos y mantenimiento de Tecnologías de Información para maximizar la contribución de tecnologías a optimizar el retorno del portafolio empresarial de programas de inversión en TI. Ver actividad PO-03-01.

Actividad: PO-04-03: Control de la inversión presupuestada

PO-04-03.01: El departamento financiero con la supervisión de su dirección correspondiente debe establecer un proceso para comparar los costos reales con los presupuestados. Este proceso debe permitir identificar desviaciones oportunamente y pedir explicaciones a los responsables.

PO-04-03.02: El director financiero debe tomar medidas correctivas para asegurar la optimización de las inversiones de Tecnologías de Información esto bajo comunicación con el jefe de informática y la dirección relacionada al proyecto. Dicho análisis se dará en apoyo con el departamento de Control.

PO-04-03.03: El departamento financiero con la supervisión del departamento de control debe realizar revisiones periódicas desde la visión de cumplimiento. Aspectos como soporte documental necesario para realizar compras, aprobaciones para desembolsos, existencia de reportes de avance, entre otros.

Para cumplir con lo anterior es necesario contar con lo siguiente:

- Presupuesto anual, a partir de este es que se entrega una parte del mismo a cada área de la organización para que esta ayude con sus actividades a alcanzar las metas del año y de la organización.
- Presupuesto de TI, es la parte dedicada exclusivamente al departamento de TI, por lo que el mismo va a tener que maximizarlo mediante análisis y priorizaciones de actividades.
- Apoyo constante del departamento financiero, al estar mÁs enfocado en el área de TI, es fácil perder de vista el recurso monetario, por lo que el departamento financiero debe de ir dando una guía de cómo se ha ido invirtiendo y cómo controlar los gastos.
- Portafolio de proyectos de TI, el departamento no puede enfocarse solamente en un proyecto puesto que si este no funciona, sus esfuerzos serían en vano. También destacar que no puede tomar todos los proyectos que se presenten, pues hay que analizar si el mismo tiene un beneficio, retorno para el departamento, consecuentemente para la organización.
- Informes de avance y cierres de proyectos de la cartera de proyectos de TI, siempre se tiene que tener un control sobre las actividades a realizar y las realizadas dentro de cada proyecto, para así tener un soporte que indique el nivel de avance de cada proyecto. Estos informes pueden servir de base para futuros proyectos donde se puede demostrar en qué actividades o situaciones hay atrasos o dificultades, de igual manera hay que tener un control sobre qué proyectos ya fueron finiquitados. Dentro de estos informes tiene que detallarse si el cierre del proyecto fue por darse por finalizado al cien por ciento o por razones que imposibilitarán la continuación del mismo, así el departamento puede realizar un análisis para que determine si pudo haberse evitado el cierre de este.

Subproceso: PO-05 Conocimiento y Gestión de riesgos de TI

Basado en:

COBIT PO.9
Normas Técnicas CGR 1.3

La organización tiene que reconocer las posibles amenazas y contingencias que podrían generar problemas en administración de las Tecnologías de Información, por lo que es importante que tenga claro que la integración de las políticas y procedimientos con la cobertura, identificación y valoración de riesgos esté de acuerdo con los objetivos del negocio.

El riesgo en toda organización es inherente por lo que se debe considerar que es necesario un equilibrio en la valoración que no permita crear oportunidades a partir de su identificación, así como la creación de beneficios a través de una gestión adecuada del riesgo.

Se debe considerar que el entorno de los negocios se encuentra en un cambio constante y que genera incertidumbre, por lo que es importante identificar, valorar, asumir y mitigar los riesgos con el fin de lograr un crecimiento óptimo del negocio y tener un panorama completo de las amenazas y consecuencias que posee potencialmente la organización.

Para cubrir lo antes mencionado y que la organización este alineando sus objetivos cumpliendo con un adecuado conocimiento y gestión de riesgos, debe considerar varios puntos importantes los cuales se detallan a continuación:

Actividad: PO-05-01: Definición de un marco de trabajo de gestión de riesgos.

PO-05-01.01: El jefe de informática debe establecer un marco de trabajo que incluya la identificación y evaluación de riesgos, esto puede ser con base al juicio experto,

el cual debe tomar en consideración los riesgos inherentes y residuales, esto enfocado a los objetivos del negocio.

PO-05-01.02: El departamento de TI debe establecer que la identificación y evaluación de riesgos genere opciones adecuadas para responder a los riesgos identificados, enfocados en el impacto que pudiese generar la realización de los mismos. Ver actividad PO-01-01.01

PO-05-01.03: El departamento de TI con la supervisión del jefe informático debe establecer procedimientos para asegurar una vigilancia constante sobre desarrollo del negocio, lo que permitirá una actualización constante para definir acciones preventivas.

Actividad: PO-05-02: Identificación y evaluación de riesgos.

PO-05-02.01: La dirección ejecutiva debe ser consciente de que una oportuna identificación de riesgos puede mitigar un impacto negativo en los objetivos de la organización, por lo que debe ser primordial para asegurar la continuidad del negocio, esto se puede lograr mediante la aplicación de controles sobre los riesgos significativos que han sido identificados en la actividad PO-05-01.

PO-05-02.02: El jefe informático debe establecer procedimientos para la identificación de los riesgos mediante la visualización de eventos que amenacen de forma realista la continuidad y alineamiento de los objetivos del negocio.

PO-05-02.03: El departamento de control tendrá la tarea de realizar una evaluación continua sobre la probabilidad e impacto que puedan tener en la organización los riesgos identificados en los recursos de TI.

PO-05-02.04: El departamento de control debe llevar un registro adecuado de los riesgos inherentes que puedan generar un impacto negativo en la organización.

Actividad: PO-05-03: Plan de acción de respuesta y mantenimiento del monitoreo sobre los riesgos.

PO-05-03.01: El departamento de TI debe desarrollar un plan de acción como respuesta a los riesgos que garantice una mitigación adecuada sobre la exposición de la organización a los mismos.

PO-05-03.02: El departamento de TI con la supervisión de la dirección ejecutiva deben cualificar y cuantificar los impactos que generan los riesgos identificados, así como los efectos inherentes y residuales de cada uno de ellos.

PO-05-03.03: El departamento de TI con la supervisión del jefe de informática debe generar una priorización de actividades de control para cada uno de los niveles de la organización, con el fin de implementar respuestas para evitar, reducir, compartir o aceptar los riesgos, generando una asignación de responsabilidades a los empleados.

PO-05-03.04: La dirección ejecutiva debe estudiar y aprobar las acciones y recomendaciones del departamento de TI para mitigar y aceptar el riesgo residual que se puede generar, creando un nivel apropiado de tolerancia al riesgo.

PO-05-03.05: El departamento de control debe monitorear la implementación de los planes para reportar las posibles variaciones o desviaciones que se generen en las actividades del negocio.

Para cumplir con lo anterior es necesario contar con lo siguiente:

- Apoyo de la administración en materia de acceso a la información requerida, recursos necesarios, directrices a los departamentos asociados, entre otros.
- Participación activa de las áreas usuarias, el departamento de TI y su área de control no puede estar pendiente de todas las áreas todo el día, por lo que es necesario que cualquier usuario esté en constante comunicación, en especial si este nota algo

inusual; al igual que al estar más en contacto con sus actividades puede conocer, aún mejor que los mismos encargados del control, algunos riesgos.

- Establecer un marco de trabajo para la gestión de riesgos, pues es necesario tener una serie de actividades en caso de encontrarse con algún riesgo dentro de la organización, específicamente dentro de cada puesto de trabajo, pues estos pueden variar cómo actuar en los diferentes puestos. Este debe incluir la evaluación y registro de los mismos.
- Política y procedimientos para la identificación de riesgos, esto para detectar posibles riesgos. Si se detectan permite saber qué realizar con los mismos.
- Evaluación continua de probabilidad e impacto de los riesgos, es necesario estar midiendo los riesgos a los que está expuesta la organización, teniendo en cuenta todo aspecto que pueda amenazar o afectar a la misma.
- Registro de los riesgos inherentes, si bien la organización puede detallar algunos riesgos fácilmente, puede que otros aparezcan en el camino, por lo que habrá que registrarlos.
- Plan de acción como respuesta a los riesgos, a cada riesgo que se presente hay que tener una serie de acciones a seguir como respuesta al mismo, ya sea con acciones inmediatas o con acciones más detenidas (detalladas).
- Implementación de controles según la prioridad y requerimientos del negocio, cada organización es diferente por lo que dependerá de ella la priorización que le dé a cada riesgo. Dependiendo de esta prioridad, cada riesgo tendría su control preventivo y de monitoreo.
- Monitoreo constante del plan de acción para responder a los riesgos, este plan de acción no puede quedarse rezagado en relación con los diferentes riesgos que aparecen día a día; cada vez más impredecibles y más minuciosos.
- Infraestructura tecnológica actual, esto para ayudar a prevenir o lidiar según sea el caso, con los diferentes riesgos, más aún con lo que se refiere a T.I pues cada día más virus, software malignos y demás aparecen y son más difíciles de combatir, por

lo que hay que tener lo último en tecnología. También para ayudar al usuario a realizar de una manera más eficaz y eficiente sus tareas.

- Recurso tecnológico actual, es necesario contar con tecnologías adecuadas para lograr los diferentes objetivos organizacionales.
- Recurso humano técnico actual, es necesario que cada empleado entienda claramente cuáles son sus asignaciones para así reducir el riesgo, al igual que las acciones que debe tomar en caso de que el riesgo se haya materializado.

PROCESO 2: Adquirir e Implementar

Subproceso: AI-01 Identificar soluciones automatizadas

Basado en:

COBIT AI.1
Normas Técnicas CGR: 3.1

A partir del proceso de planeación estratégica, es importante que la administración se dé a la tarea de identificar, desarrollar o adquirir soluciones de TI que sean implementadas e integradas en los procesos del negocio. Que se cuente con las mejores y más eficientes aplicaciones tecnológicas que permitan satisfacer necesidades críticas y que vayan acorde con los objetivos y metas del negocio.

Claro está que aspectos como el análisis de factibilidad operativa y financiera, análisis de riesgos en el desarrollo o la compra de nuevas aplicaciones deben ser valoradas por el departamento respectivo, así como aprobadas obligatoriamente por la administración, pues el objetivo principal es el cumplimiento, en todo momento, de los requerimientos del negocio de una manera eficiente y efectiva.

Para lograr una correcta y satisfactoria identificación de soluciones automatizadas, es necesario contemplar como mínimo los siguientes puntos:

Actividad: AI-01-01: Conocimiento del dominio de Planeación y Organización.

AI-01-01.01: El director ejecutivo debe transmitir el entendimiento general de dicho dominio a todos los departamentos del negocio. Esto lo debe hacer comunicándolo vía digital o documental; así como a través de reuniones o inducciones.

Actividad: AI-01-02: Definir los requerimientos técnicos y del negocio.

AI-01-02.01: El departamento de TI con la supervisión del jefe informático debe recabar las necesidades y mejoras que los otros departamentos del negocio requieran. Para ello se debe programar reuniones con los directores de cada departamento.

AI-01-02.02: El jefe informático bajo supervisión del director ejecutivo debe priorizar y categorizar los requerimientos de las áreas de acuerdo con la importancia en el logro de los objetivos del negocio. Debe considerar el esquema de componentes críticos departamentales y el plan de recursos tecnológicos desarrollados anteriormente. Ver PO-01-02 y PO-01-03.02.

Actividad: AI-01-03: Definir y analizar los riesgos asociados.

AI-01-03.01: El jefe informático con la supervisión del director ejecutivo debe realizar una identificación de los riesgos asociados con los requerimientos del negocio e implementación de soluciones como parte de los procesos financieros y operativos del negocio. Ver actividad PO-05-01 y PO-05-02

AI-01-03.02: El departamento de TI con la supervisión del director ejecutivo debe realizar un análisis de los riesgos identificados con el fin de soportar la decisión si se desarrolla, se adquiere o si se rechaza el proyecto de implementación. Ver actividad PO-05-01 y PO-05-02

Actividad: AI-01-04: Realizar estudios de factibilidad como se define en los estándares de desarrollo.

AI-01-04.01: El jefe informático con la supervisión del director financiero, debe realizar estudios de factibilidad económica en donde se incluyan costos de oportunidad, tasa interna de retorno, maximización de recursos, entre otros; referente a la aceptación o no de proyectos relacionados con soluciones automatizadas en el negocio. El director financiero supervisa y da seguimiento de ello.

AI-01-04.02: El jefe informático con la supervisión del director financiero debe realizar estudios de factibilidad tecnológica en donde se incluya aumento en la eficiencia y eficacia de los procesos, mayor producción, menor mantenimiento, entre otros; referente a la aceptación o no de proyectos relacionados con soluciones automatizadas en el negocio. Tanto el director financiero como operativo supervisan y dan seguimiento de ello.

AI-01-04.03: El jefe informático debe preparar un informe con los resultados finales de los estudios de factibilidad realizados con el fin de ser presentados a las direcciones del negocio para que ellos tomen la decisión final si es factible o no realizar el proyecto.

- Apoyo de la administración en materia de acceso a la información requerida, recursos necesarios, directrices a los departamentos asociados, entre otros.
- Apoyo del departamento Financiero y de Operaciones, este apoyo viene a ser parte fundamental en el momento de la compra o desarrollo de la solución automatizada, ya que hay que velar por el costo-beneficio que traería la misma.
- Planeación estratégica, no puede hacerse un cambio sin un plan a seguir, por lo que es necesario tener una lista de actividades para la implementación del mismo.
- Presupuesto y políticas organizacionales, en lo que se refiere a políticas organizacionales, hay que tener en cuenta que no choquen estas con el nuevo formato automatizado, es decir que no vaya en contra a la posición que tiene la organización, ya sea interna o externamente.

- Participación activa de las áreas usuarias, al estar más relacionados con las actividades diarias, los usuarios deberían ser de los primeros en informar si es necesaria la automatización, al igual que participar en el análisis de qué herramienta es la más adecuada para la misma.

Subproceso: AI-02 Creación de aplicaciones acordes al negocio

Basado en:

COBIT AI.2
Normas Técnicas CGR 3.2

Posterior a la aprobación de la administración, y ya sea que se adquiera, se mantiene o se delega el software, es clave que las nuevas aplicaciones vayan dirigidas según los requerimientos del negocio y cumplan con condiciones de calidad, oportunidad, costo razonable y confiabilidad. Esto contribuye en el apoyo a los procesos operativos y financieros, la eficiencia y eficacia en la manipulación de datos y una mejor toma de decisiones tanto de las áreas usuarias como por parte de la administración.

La inclusión adecuada en el diseño y configuración de aplicaciones, controles y aspectos de seguridad, mantenimiento de software o seguimiento continuo en caso de contratación a terceros, así como un entrenamiento adecuado y retroalimentación son claves para que el proceso sea considerado en todo momento importante y satisfaga a cabalidad las necesidades del negocio y por el cual se optó su puesta en marcha.

Para lograr una adecuada creación de aplicaciones y acordes al negocio, debe contemplarse como mínimo los siguientes puntos:

Actividad: AI-02-01: Desarrollo de los requerimientos técnicos y del negocio a través de especificaciones en la creación del diseño e implementación de soluciones automatizadas.

AI-02-01.01: El departamento de TI con la supervisión del jefe informático debe preparar de manera detallada el diseño y los requerimientos técnicos de las aplicaciones solicitadas; este documento debe estar adecuado al 100% con las demandas del departamento del negocio que lo solicita, así como disposiciones de aspectos legales en caso de que lo amerite. Dicho diseño debe ser revisado por el jefe de informática y el director del departamento que solicita.

AI-02-01.02: El jefe informático con la supervisión del director ejecutivo debe elaborar una guía que permita dirigir todas las acciones a realizar, antes, durante y después de la implementación. En donde se detalle algunos aspectos como:

-Definición de requerimientos, alcances, roles y responsabilidades, estudios de factibilidad, elaboración de diseños.

-Período estimado para puesta en marcha, roles y responsabilidades, fase de programación y pruebas.

-Una vez implementado se debe contar con la satisfacción por parte del departamento solicitante, se debe evaluar posteriormente, en sus primeros días, el desempeño y eficiencia en pro del proceso crítico que la aplicación afecta, esto para conocer si es necesario ajustarlo.

-Dicho diseño debe ser revisado por el jefe de informática y el director del departamento que solicita.

Actividad: AI-02-02: Controles y seguridad en la creación de aplicaciones.

AI-02-02.01: El jefe informático con la supervisión del director ejecutivo debe crear un manual de seguridad que establezca aspectos como objetivos, estrategias, controles y asignación de funciones, indicadores de medición, responsabilidades y permisos de acceso que tendrá el personal a cargo de la implementación y del mantenimiento de las

aplicaciones instaladas. Este manual debe ser comunicado de manera digital o documental a los departamentos del negocio vinculados.

AI-02-02.02: El jefe informático con la supervisión del director ejecutivo debe supervisar de manera periódica que las áreas del negocio que estén relacionados con el proceso de implementación de la aplicación, funcionen acorde con las políticas organizacionales y en pro de los objetivos del negocio, para ello debe considerar aspectos como la guía usada para la implementación de la aplicación, el manual de seguridad respectivo, la visión estratégica y los objetivos organizacionales.

AI-02-02.03: El departamento de control con la supervisión del jefe informático debe implementar controles de negocio como listado de autorizados para acceso, controles de tipo físico, vistas y perfiles de usuario, entre otros; todo aquello que permita auditar las aplicaciones en materia de su procesamiento y cumpla con los requerimientos como la efectividad, eficiencia, integridad, oportunidad y confidencialidad.

Actividad: AI-02-03: Configuración y mantenimiento de la aplicación existente.

AI-02-03.01: El jefe informático con la supervisión del director ejecutivo debe crear una estrategia y plan de mantenimiento para la aplicación existente, que contenga aspectos como los objetivos, alcances, roles y responsabilidades, periodicidad de ejecución, tiempos de respuesta, controles asociados, entre otros. Dicha estrategia y plan deben ser revisados y autorizados por el jefe de informática.

AI-02-03.02: El departamento de TI con la supervisión del jefe informático debe elaborar una bitácora que contemple aspectos propios de la configuración de la aplicación, que defina los criterios para determinar la procedencia de cambios y accesos, también que indique procedimientos de autorización, registro, supervisión y evaluación técnica-operativa y administrativa de los resultados de esos cambios y accesos. Dicha bitácora

estará a disposición de consulta para la jefatura inmediata, direcciones del negocio y departamento de control cuando así lo necesiten.

Actividad: AI-02-04: Calidad de la aplicación.

AI-02-04.01: El jefe informático con la supervisión del director ejecutivo debe crear un plan de aseguramiento de calidad de la aplicación, que contenga los objetivos y el seguimiento a darse para tener claro que la aplicación implementada está apegada a los requerimientos del negocio y acorde con las políticas y procedimientos de calidad del negocio. Para ello debe considerarse la guía usada para la implementación de la aplicación, el manual de seguridad respectivo, la visión estratégica de TI desarrollados en actividades anteriores.

Actividad: AI-02-05: Contratación de terceros para la implementación y mantenimiento de software.

AI-02-05.01: Tomando como referencia el informe definitivo de los estudios de factibilidad (ver AI-01-04.03), el jefe de informática con la supervisión del director ejecutivo debe justificar a las direcciones del negocio por qué es más viable contratar a terceros para la implementación y mantenimiento de la aplicación solicitada.

AI-02-05.02: El jefe de informática con la supervisión del director ejecutivo debe establecer una guía para la contratación de productos de software a terceros, incluyendo aspectos como: ofertas por el servicio, términos de referencia que incluya la gestión de contratos y políticas, responsabilidades, obligaciones legales y financieros, documentación, cláusulas correspondientes, seguridad de propiedad intelectual, entre otros.

AI-02-05.03: El jefe informático con la supervisión del director ejecutivo debe establecer un proceso de transferencia tecnológica que minimice la dependencia de la

organización respecto de terceros contratados para la implementación y mantenimiento de la aplicación solicitada. Dicho proceso debe ser revisado y autorizado por el jefe de informática.

Para cumplir con lo anterior es necesario contar con lo siguiente:

- Participación activa de las áreas usuarias, al estar en contacto con las actividades del área, el usuario final conoce bien cuáles son sus necesidades para que el departamento de TI pueda tomar una decisión con base en el criterio técnico del departamento y las acotaciones que provea el usuario final. También se necesita de la participación activa del mismo para las pruebas de las aplicaciones.
- Listado de requerimientos críticos por áreas y del negocio, este listado puede ser elaborado por el usuario, la administración, el departamento de TI, o inclusive en conjunto, pero es indispensable que este listado no se quede solo papel, sino que se tome en consideración a la hora de crear las aplicaciones.
- Análisis de la valoración de riesgos organizacionales y de implementación o desarrollo de soluciones de TI, al ser algo nuevo para cualquier área, esta aplicación traería consigo otros riesgos que tal vez no fueron considerados en otros momentos, por lo que hay que valorar si esta aplicación viene a ayudar o más bien sería un problema por los riesgos que esta conlleva.
- Informe detallando los estudios de factibilidad para la implementación o el desarrollo de soluciones de TI, hay momentos en los cuales la organización debe optar por apoyo de terceros (*outsourcing*), a como hay momentos en los cuales la organización debe independizarse, por lo que hay que tener una constante revisión de qué es lo más conveniente para la organización, si desarrollar una solución propia o implementar soluciones de terceros.

Subproceso: AI-03 Adquirir infraestructura, recursos tecnológicos y humanos.

Basado en:

COBIT AI.3 y AI.5
Normas Técnicas CGR 3.2

Para que las aplicaciones implementadas en mejora de los procesos, la ejecución de tareas, la toma de decisiones y el logro de los objetivos del negocio puedan trabajar de manera eficaz y eficiente es importante que se cuente con la infraestructura, el recurso tecnológico a la medida, y el recurso humano adecuado. Todo lo anterior apegado a las estrategias convenidas, a la tendencia de TI, a los estándares de tecnología y a la disposición del ambiente de desarrollo y pruebas.

No se puede disponer en su máximo esplendor de las soluciones automatizadas si se cuenta con personal sin conocimiento técnico, una plataforma tecnológica obsoleta o/e insuficiente en sus capacidades (memoria, rapidez, versión) y una falta de disponibilidad cuando se requiere por parte de las áreas usuarias, la administración, externos autorizados, entre otros; de allí la importancia de la adquisición de lo adecuado, viable y eficiente en este apartado.

Para lograr una correcta adquisición de infraestructura, recurso tecnológico y humano, es importante contemplar como mínimo los siguientes puntos:

Actividad: AI-03-01: Creación de procesos para la adquisición, implementación y actualización de la infraestructura y recursos tecnológicos.

AI-03-01.01: El departamento operativo con la supervisión del director ejecutivo debe crear un procedimiento que permita indicar de manera explícita temas claros para la adquisición (incluye gestión de contratos y política en materia de selección de proveedores, responsabilidades, obligaciones legales y financieras, documentación, cláusulas correspondientes, seguridad de propiedad intelectual, entre otros), implementación y actualización de la infraestructura y recursos tecnológicos. Todo esto amparado en la visión estratégica de TI y los requerimientos técnicos y del negocio.

AI-03-01.02: El jefe informático con la supervisión del director ejecutivo debe dar aprobación a dicho procedimiento, con ello debe ser presentado al director ejecutivo para que pueda ser comunicado a toda la organización a partir de la fecha que se indique.

Actividad: AI-03-02: Adquisición o capacitación de recursos humano con conocimiento técnico y acorde a las capacidades del negocio.

AI-03-02.01: El departamento de TI con la supervisión del departamento de Recursos Humanos debe valorar la posibilidad de capacitación a personal existente en el negocio acorde a las necesidades de las nuevas implementaciones en los sistemas. Para ello debe considerarse lo indicado en el perfil de puestos elaborado en la actividad PO-02-01.02 y lo dictado en la guía usada para la implementación de la aplicación elaborada en la actividad AI-02-02.02. En tal caso, de no lograrse dicha opción se procede a contratar recurso humano con estas disposiciones.

AI-03-02.02: En caso de contratar, el departamento de Recursos Humano con la supervisión del jefe de informática deben evaluar el perfil de puestos existente (PO-02-01.02) para considerar si debe ajustarse a las necesidades requeridas y así contar con nuevo recurso humano capacitado. Ante cualquier ajuste el perfil debe tener autorización obligatoria del director ejecutivo.

Actividad: AI-03-03: Plan de mantenimiento y operatividad de la infraestructura tecnológica.

AI-03-03.01: El departamento de TI con la supervisión del jefe informático debe crear un plan de mantenimiento y operatividad para la infraestructura y recursos tecnológicos que contemple aspectos como actividades a realizar, procedimientos, roles y responsabilidades, recursos, y lapsos de ejecución por departamento; con ello se supervisa su optimización, su disponibilidad, su integridad y permite ajustarse a los cambios internos y externos de la organización. Dicho plan debe ser revisado y autorizado por el jefe de informática.

AI-03-03.02: El departamento de TI con la supervisión del jefe informático debe valorar en todo momento el informe relacionado con la administración de cambios (ver actividad AI-05-03.02) que le permitirá contemplar de una manera más clara el estatus y los aspectos a considerar en el mantenimiento de la infraestructura y los recursos tecnológicos. En caso de realizar ajustes al plan le debe comunicar al jefe de informática.

AI-03-03.03: El departamento de TI con la supervisión del jefe informático debe tener una comunicación continua en materia de necesidades del negocio; esto a través de reuniones periódicas con los jerarcas de cada departamento. La aprobación de dichas solicitudes será evaluada y tomada por parte del director ejecutivo.

AI-03-03.04: El jefe de informática con la supervisión el director ejecutivo debe incluir dentro del plan de trabajo (ver actividad PO-01-03) la revisión periódica en materia del mantenimiento y la operatividad de la infraestructura y los recursos tecnológicos, esto para prever posibles riesgos, evaluar vulnerabilidades y, de ser necesario, comunicar requerimientos adicionales de control y seguridad a la dirección ejecutiva.

Actividad: AI-03-04: Creación y ejecución de medidas de control, seguridad y auditabilidad.

AI-03-04.01: El jefe de informática con la supervisión del departamento de control debe crear un plan de medidas de control, seguridad y auditabilidad tanto para la infraestructura tecnológica como para el recurso tecnológico, estos deben contemplar aspectos como objetivos, estrategias, controles y asignación de funciones, indicadores de medición, responsabilidades, permisos de acceso, entre otros; con el fin de garantizar su disponibilidad e integridad en todo momento. Este plan debe ser comunicado de manera digital o documental a todas las direcciones y el departamento de control.

AI-03-04.02: El departamento de TI con la supervisión del jefe informático debe llevar una bitácora actualizada de todos los incidentes presentados, la composición y los

cambios en la configuración de hardware y software, pruebas de integración y desempeño, control de versiones y licencias, migración entre ambientes, etc. Esta bitácora debe permitir que se revise en cualquier momento la capacidad de requerimientos del negocio, acciones de mejora y revisiones por parte de las direcciones del negocio o el departamento de control.

Para cumplir con lo anterior es necesario contar con lo siguiente:

- Participación activa de las áreas usuarias, al ser los más involucrados en el uso de software y/o hardware, ellos son los que deben identificar las necesidades importantes y al mismo tiempo pueden tener las soluciones más sencillas para las mismas. Igualmente, al momento de realizar cualquier cambio, el usuario tiene que estar abierto al mismo, sino el cambio resultará inútil para la organización.
- Requerimientos técnicos del software de aplicación, siempre hay que estar actualizando tanto el talento humano como el hardware, pues de lo contrario la organización va a quedar rezagada en comparación con su competencia. A causa de esta actualización, los software también requieren de mayor capacidad; por lo que los requerimientos técnicos deben estar presentes en todo momento, pues en un futuro puede ser una limitante de actualización.
- Política y contratos en materia de la contratación de terceros para la implementación y mantenimiento de software, deben estar bien claros los alcances y límites que se vayan a contraer en cada uno de los contratos con terceros, pues si no se especifica bien, puede que haya un desfase en los mismos, ocasionando atrasos o conflictos entre ambas partes. Por ejemplo debe definirse si el proveedor dará la capacitación necesaria para el software, o quién hará las actualizaciones y revisiones del mismo, etc.
- Infraestructura tecnológica actual, de nada sirve tener la última tecnología en software y hardware, si no se tiene una correcta instalación tanto de redes como de

corriente, por lo que hay que conocer hasta dónde se puede llegar con lo que posee la organización.

- Recurso tecnológico actual, el usuario aprende a utilizar las nuevas tecnologías más rápido que antes, ya sea intuitivamente o por capacitaciones, por lo que el recurso tecnológico no debería quedarse atrás, desaprovechando el talento humano que posee la organización.
- Recurso humano técnico actual, hay que tener en cuenta que si se especializa mucho tanto el software como el hardware y el recurso humano no tiene la capacidad de procesarlos habrá problemas en el manejo de los mismos, siendo menos efectivos que con alguien que conozca cómo usarlos. Por lo tanto hay que analizar si este es el caso dentro de la organización.
- Comunicación continúa en materia de necesidades del negocio a través de reuniones periódicas con los jerarcas por departamento; éstas deberán ser revisadas por la administración.

Subproceso: AI-04 Facilidad en el uso y la operación.

Basado en:

COBIT AI.4
Normas Técnicas CGR

Se cuenta hasta este momento con las herramientas necesarias para lograr el cumplimiento de los requerimientos técnicos y del negocio, se trata de una plataforma tecnológica y aplicaciones automatizadas; pero es muy importante que el conocimiento de los nuevos sistemas, de su uso eficaz y eficiente sea entregado a los usuarios.

Este conocimiento debe procurarse que sea recibido y captado de la manera más clara y exacta posible, pues de ellos depende que el uso de los datos permita la optimización de los procesos, el cumplimiento y la confiabilidad en la generación de reportes, que la información visualizada o transmitida sea íntegra, que su ciclo de vida sea

útil y continuo, así como que la toma de decisiones, cuando así lo amerite, sea oportuna y correcta por parte de los puestos gerenciales de la organización.

Para lograr una adecuada y eficaz facilidad en el uso y la operación de las aplicaciones implementadas en el negocio, es necesario que se contemplen como mínimo los siguientes puntos:

Actividad: AI-04-01: Transferencia del conocimiento.

AI-04-01.01: La dirección del departamento solicitante con la supervisión de la dirección ejecutiva debe tomar posesión de la aplicación, ejercer la responsabilidad por la entrega y calidad del servicio obtenido, de la seguridad y control. Además, incluye la recepción de aspectos importantes como lo es el respaldo y la recuperación, la aprobación de accesos, controles automatizados del negocio, la administración de privilegios, entre otros.

AI-04-01.02: El departamento de Recursos Humanos con la supervisión de la dirección ejecutiva debe crear un plan para la programación de sesiones de capacitación para las áreas usuarias, con el fin de que se entienda, conozca y ejecute de la mejor manera las aplicaciones que recién son implementadas. La transferencia del conocimiento deberá incluir aplicaciones de ayuda en línea, asistencia a usuarios e identificación de usuario clave.

AI-04-01.03: El departamento de TI con la supervisión del jefe informático debe recibir por parte del equipo o encargado de la implementación de la aplicación (interno o externo) la inducción respectiva y necesaria para tener la capacidad de entregar, apoyar y mantener la aplicación y la plataforma tecnológica relacionada de manera eficaz y eficiente, acorde con los niveles de servicios que así se requieran. Además, el jefe de informática debe recibir la documentación de soporte técnico necesaria y cualquier otra información asociada.

AI-04-01.04: El departamento de Recursos Humanos con la supervisión del jefe informático debe realizar una evaluación que permita tener una visión sobre si el mensaje e información impartida fue captada de la mejor manera por parte del departamento usuario. Un breve cuestionario puede ser una opción para ello.

AI-04-01.05: El departamento de Recursos Humanos con la supervisión del jefe informático debe realizar el levantamiento de un informe con los resultados, recomendaciones y conclusiones en el tema de la transferencia del conocimiento, el cual será comunicado a la jefatura de informática y a la dirección del departamento solicitante.

Actividad: AI-04-02: Generación de manuales para usuarios y departamento de TI.

AI-04-02.01: El departamento de Recursos Humanos con la supervisión del jefe informático debe entregar manuales o materiales de información necesarios que sirvan de referencia o guía para una mejor comprensión por parte del o los departamentos del negocio vinculados a la aplicación.

Para cumplir con lo anterior es necesario contar con lo siguiente:

- Apoyo de la administración en materia de acceso a la información requerida, recursos necesarios, directrices a los departamentos asociados, entre otros
- Participación activa de las áreas usuarias, al ser los más involucrados en el uso de software y/o hardware, ellos son los que deben identificar formas en que se podría facilitar el uso del software o hardware y reportar cualquier mal uso que se le pueda a dar a los mismos. Igualmente, al momento de realizar cualquier cambio, el usuario tiene que estar abierto al mismo, si no el cambio resultará inútil para la organización.
- Planeación estratégica esto si no se tiene una estrategia a seguir para cumplir los objetivos organizacionales, los esfuerzos no se van a enfocar de una manera eficiente y eficaz y se pueden perder valiosos recursos por falta de la misma.

- Políticas organizacionales, dentro de estas debe haber un apartado donde se indique la transferencia de conocimiento; también debe haber un manual que guíe a los usuarios en sus labores, facilitando su inclusión en la organización.
- Infraestructura tecnológica, el usuario puede tener la actitud de aprender a usar un nuevo software o de manejar un nuevo hardware, pero si la infraestructura tecnológica no es la óptima, el aprendizaje va a ser más lento de lo esperado, por lo que hay que tener una buena infraestructura en la cual pueda el usuario basarse, por ejemplo ayudas en línea o manuales electrónicos, para el uso de cada software o hardware.
- Recursos tecnológicos, al igual que con la infraestructura tecnológica, es necesario contar con bases de apoyo para cualquier duda que se pueda presentar en el usuario, independientemente si es de hardware o software.

Subproceso: AI-05 Administración de cambios.

Basado en:

COBIT AI.6
Normas Técnicas CGR 4.2

Son muchos los aspectos en los que puede influir la realización de modificaciones, ya sean programadas o no programadas, en las aplicaciones, en los recursos tecnológicos, en la infraestructura tecnológica y en el recurso humano técnico ligado directamente en dicho proceso. Claro está que los cambios siempre buscarán la minimización de errores, la optimización de especificaciones realizadas por la administración, entre otros; pero no puede obviarse que se puede generar un impacto negativo con ello que provoque una desviación en la visión estratégica de TI elaborada desde un inicio, la falta de eficiencia en la ejecución de los procesos del negocio y por consiguiente la pérdida en la búsqueda del logro de los requerimientos establecidos por parte de la administración.

La administración de cambios permite reducir los riesgos asociados y la incertidumbre de que la información obtenida posterior a los cambios permanecerá siendo íntegra y confiable a la vista de los usuarios y para la toma de decisiones. Desde la variación en un procedimiento, un proceso, hasta cambios directos en los servicios son ejemplos de ello.

Para lograr, y mantener una correcta administración de cambios que permita la optimización de las aplicaciones, es necesario que se contemplen como mínimo los siguientes puntos:

Actividad: AI-05-01: Definición y comunicación de procedimientos de cambios.

AI-05-01.01: El jefe de informática con la supervisión del director ejecutivo debe elaborar un procedimiento de cambios formales -incluyendo mantenimiento y parches-, el cual debe estar aprobado por el jefe de informática con el propósito de tratar de manera ordenada todas las solicitudes que así le sean indicadas. Este procedimiento debe abarcar aspectos claves como la justificación clara a la solicitud del cambio, la persona que solicita y la autorización por parte de la jefatura correspondiente.

AI-05-01.02: El jefe de informática con la supervisión del director ejecutivo debe elaborar un procedimiento de cambios no programados o de emergencia, el cual estará aprobado por el jefe informático, con el propósito de indicar de manera clara cuál cambio es considerado bajo ese nivel y cuál es el manejo que debe dársele a estos. Este procedimiento debe abarcar aspectos como la autorización del director respectivo o encargado inmediato, documentación del cambio ejecutado y pruebas posteriores, resumen del incidente y comunicación a interesados.

AI-05-01.03: El director ejecutivo debe hacer un comunicado oficial de dichos procedimientos a todos los departamentos del negocio, además el departamento de TI o jefe de informática debe aclarar dudas en caso de ser necesario.

Actividad: AI-05-02: Evaluación del impacto, prioridades y autorización de los cambios programados.

AI-05-02.01: El jefe de informática con la supervisión del director ejecutivo debe analizar y evaluar el impacto que el cambio realizado puede ocasionar en el sistema operacional actual y su funcionalidad. Para ello debe considerarse la guía usada para la implementación de la aplicación, el manual de seguridad respectivo, la visión estratégica de TI desarrollados en actividades anteriores, así como el ambiente de prueba que permita conocer la manera en que funciona y la creación de planes *vuelta atrás*, lo cual permite que al momento de ejecutarse se presenta alguna anomalía, sea posible regresar al estado anterior para volver a ejecutar posterior a la modificación o variación.

AI-05-02.02: El jefe de informática con la supervisión del director ejecutivo debe crear un informe, de manera periódica, o en el momento que alguna dirección departamental lo solicite, con todas las solicitudes de cambios que fueron recibidas en determinado lapso, estableciendo prioridades por categoría con el fin de mitigar el riesgo que exista si no se aplican los cambios, ya sean programados o no.

AI-05-02.03: El jefe de informática con la supervisión del director ejecutivo debe tomar la decisión final si se aprueban o no las solicitudes. Posteriormente es comunicado al departamento solicitante de la decisión, en caso de que hubiese sido una negativa para que proceda a realizar una nueva solicitud si es necesario.

AI-05-02.04: El jefe de informática con la supervisión del director ejecutivo debe evaluar ante cambios significativos en las aplicaciones, la necesidad de actualizar cualquier documento o información vinculada a la ejecución de nuevas aplicaciones en un proceso (ver proceso AI-02). Esto bajo la aprobación del jefe de informática.

Actividad: AI-05-03: Seguimiento, aceptación y reporte de los cambios realizados.

AI-05-03.01: El jefe de informática con la supervisión del director ejecutivo debe establecer un sistema de seguimiento a los cambios solicitados y ejecutados para conocer la implantación correcta y total de éstos. En este sistema se puede abarcar información general, solicitante, estatus del cambio, grado de avance, conclusiones, indicaciones especiales, entre otros. Este será presentado y supervisado de manera periódica por el jefe de informático.

AI-05-03.02: El departamento de TI con la supervisión del jefe de informática debe elaborar un documento de conformidad, el cual será firmado por el responsable solicitante del cambio al momento de la conclusión y entrega; con ello acepta y se cierra la gestión en la que se trabajó. En caso de no conformidad, el solicitante podrá presentar razones fundamentadas al jefe de informática, o de ser necesario a la dirección ejecutiva, para que puedan ser solventadas sus necesidades de la manera indicada.

AI-05-03.03: El jefe de informática con la supervisión del director ejecutivo debe entregar un reporte, de manera periódica al director ejecutivo o cuando las direcciones del negocio y departamento de control así lo requieran. De ser necesario debe responder a consultas o en tal caso se está dando por concluido y cerrado el proceso de dicho cambio.

Para cumplir con lo anterior es necesario contar con lo siguiente:

- Participación activa de las áreas usuarias, al ser los más involucrados en el uso de software y/o hardware, ellos son los que deben estar abiertos al mismo, si no el cambio resultará inútil para la organización. De igual manera ellos son los que deben decir si hay algún problema con el mismo.
- Infraestructura tecnológica, es importante que al momento del cambio haya un respaldo, en caso de que el cambio no se haga tan fluido como se esperaba y no hayan inconvenientes al momento del mismo.

- Recursos tecnológicos, como se mencionó anteriormente, es necesario contar con los recursos tecnológicos que el software al cual se va a cambiar ocupe, es decir si se planea una actualización mayor, lo más probable es que el hardware y demás recursos tecnológicos también tengan que ser cambiados por algo más actual, por lo tanto es necesario tener presente las necesidades que conlleva el cambio.
- Manuales para usuarios y departamento de TI. como se ha mencionado, es necesario contar con manuales, no solo digitales, en caso de cualquier inconveniente, para tener una base sobre qué acciones se deben realizar para las diferentes situaciones que se puedan presentar, al igual que manuales por cada puesto para así ayudar al usuario con sus tareas cotidianas.

Subproceso: AI-06 Instalación y Acreditación de soluciones y cambios

Basado en:

COBIT AI.7
Normas Técnicas CGR 3.3

Una vez concluido el proceso de planeación, adquisición y desarrollo se debe proceder con la implementación de las nuevas aplicaciones en el proceso del negocio. Es importante saber con antelación qué actividades críticas pueden verse afectadas y si se cumple a cabalidad con las expectativas y demandas. En resumen, que no se materialicen riesgos indicados previamente.

Son varios los aspectos que deben ser realizados previamente, entre ellos: la ejecución de pruebas, en especial en procesos críticos y de manera repetitiva, la definición clara de las instrucciones a seguir para migrar a las nuevas aplicaciones, así como la implementación y revisiones posteriores.

Todo lo anterior permite que los procesos de implementación y ejecución sean realizados de una manera confiable, íntegra y consecuentemente permitan lograr con

eficiencia los requerimientos técnicos y de negocio que fueron indicados en el proceso de planeación.

Para lograr y mantener una adecuada Instalación y Acreditación de soluciones y cambios, es necesario que se contemplen como mínimo los siguientes puntos:

Actividad: AI-06-01: Creación de una metodología de pruebas

AI-06-01.01: El jefe de informática con la supervisión del director ejecutivo debe elaborar un plan de pruebas que permita indicar roles, responsabilidades, periodos de ejecución, áreas vinculadas, definición de ambientes de prueba, respaldos, aprobaciones, entre otros.

AI-06-01.02: El jefe de informática con la supervisión del director ejecutivo tiene la tarea de revisar y aprobar dicho plan de pruebas. Posteriormente, lo presenta y comunica a todas las direcciones del negocio para su debido conocimiento y que ellos transmitan la información prudente a los departamentos correspondientes.

Actividad: AI-06-02: Planificar el proceso de migración de sistemas y datos a las nuevas aplicaciones.

AI-06-02.01: El jefe de informática con la supervisión del director ejecutivo debe elaborar un plan para realizar el proceso de migración de sistemas y datos a las nuevas aplicaciones; que permita indicar roles, responsabilidades, periodos de ejecución, respaldos, pistas de auditoría, aprobaciones, entre otros. Este será presentado y aprobado por el jefe informático.

Actividad: AI-06-03: Evaluación y aprobación de los resultados de las pruebas por parte de la dirección ejecutiva.

AI-06-03.01: Cada departamento debe evaluar conjuntamente con la supervisión del jefe informático, la necesidad de realizar cambios en la aplicación, si posterior a los resultados de las pruebas es necesario.

Actividad: AI-06-04: Ejecución de revisiones posteriores a la implementación

AI-06-04.01: El jefe de informática con la supervisión del departamento de control deben revisar de manera periódica el proceso de la implementación que fue realizado. Tomar en cuenta el proceso AI-05 para ello. El fin viene a ser tener claro el conocimiento de la optimización de los procesos, opciones de mejora, recomendaciones de cambio, etc.

AI-06-04.02: El jefe de informática con la supervisión del departamento de control debe llevar una bitácora que contenga todos los aspectos asociados a estas revisiones posteriores, esto con el fin de que cuando así lo solicite la jefatura de informática, direcciones del negocio, departamento de control o cualquier personal autorizado se pueda revisar, analizar y tomar cualquier decisión asociada a este asunto.

Para cumplir con lo anterior es necesario contar con lo siguiente:

- Manuales para usuarios y departamento de TI luego de instaladas (implementadas) las diferentes soluciones, es necesario capacitar a los usuarios, son parte importante los manuales para los mismos, que servirán como base de consulta en caso de haber una duda. Igualmente estos manuales deben demostrar cada proceso detalladamente.
- Plan para el entrenamiento en la transferencia del conocimiento, el cual va de la mano con los manuales de usuarios, ya que el usuario por si solo puede no conocer al 100% el cómo utilizar la nueva implementación; por lo que es necesario establecer un plan a seguir para entrenarlo y capacitarlo.
- Recurso humano técnico capacitado, de nada serviría un cambio si el personal no está capacitado para hacer uso del mismo, por lo que este punto debe estar bien

claro dentro del plan de la administración, si no fuese así se corre el riesgo de que la solución implementada quede sin uso por falta de personal capacitado.

- Infraestructura tecnológica y recursos tecnológicos, es necesario contar con bases de apoyo para cualquier duda que se pueda presentar en el usuario, independientemente si es de hardware o software. También es importante destacar que estos deben estar actualizándose continuamente, pues así los recursos pueden desempeñarse de una manera más óptima, al igual que los usuarios de estos.

PROCESO 3 Entregar y Dar Soporte

Basado en:

COBIT DS.1, DS.2 y DS.6
Normas Técnicas CGR 4.1

Posterior a la adquisición e implementación de las Tecnologías de Información es necesario que la organización tome en consideración que se deben establecer procedimientos en la entrega y las evaluaciones posteriores, con el fin de dar soporte de una forma ágil y apropiada.

Lo antes mencionado se da por la constante actualización de las Tecnologías de Información y para dar respuesta a los cambios que se vayan desarrollando con el paso del tiempo, así como tener la capacidad de solventar los problemas e inconvenientes que se vayan presentando en el transcurso del giro del negocio.

Para conseguir lo antes mencionado la organización debe tomar en consideración que hay procesos fundamentales que se deben cumplir:

Subproceso: ES-01 Prestación de servicios

Es importante que la organización cuente con un acuerdo documentado de servicios de Tecnologías de Información, con el fin de que exista un alineamiento de servicios con

los objetivos de la entidad, así mismo para mantener una adecuada comunicación entre el departamento de TI y la administración.

La identificación de requerimientos de servicios, acuerdos de niveles y monitoreo del cumplimiento de los mismos, así como la formación de acuerdos internos y externos son fundamentales en la prestación de servicios para mantener una actualización sobre las necesidades que surjan durante el desarrollo del negocio.

Este paso va de la mano con la adecuada administración de servicios, ya sean internos o externos, por lo que se debe tomar en consideración la asignación de costos en el presupuesto planteado en los procesos de Planificación y Organización, con el fin de asegurar que los servicios cumplan con los requerimientos que el negocio requiera para satisfacer la optimización y transparencia en el consumo de recursos.

Para cumplir lo antes mencionado es necesario establecer los siguientes puntos críticos para el desarrollo de la administración de servicios, la identificación y asignación de costos:

Actividad: ES-01-01: Identificación y definición de los servicios y de un marco de trabajo para los diferentes niveles requeridos.

ES-01-01.01: El jefe de informática debe establecer un marco de trabajo el cual contenga procedimientos para la creación de requerimientos de servicios enfocados a cumplir con los objetivos de negocio, así como la definición de los mismos, crear acuerdos entre departamentos, o bien, con terceros y presupuesto, esto para su desarrollo y mantenimiento. Este marco de trabajo debe establecer la prioridad de importancia de servicios, roles, tareas y responsabilidades, tanto de los proveedores como de los clientes para cada uno.

ES-01-01.02: El jefe de informática debe realizar la centralización de servicios establecidos mediante un portafolio en el cual se puedan identificar los requerimientos para cada uno de los mismos. El portafolio se puede generar vía digital al cual tengan acceso los diferentes departamentos

ES-01-01.03: El jefe de informática debe establecer convenios para los niveles de servicios críticos que se brindan, estos tienen que contener el compromiso con los usuarios o clientes, requerimientos de soporte, métricas para la medición del desempeño de los servicios, roles y responsabilidades en la ejecución de los mismos, también se debe considerar que estos acuerdos hagan mención sobre el desempeño, capacidad de crecimiento de la entidad, seguridad, restricciones y niveles de soporte. Estos acuerdos se deberán revisar periódicamente por parte del director ejecutivo para evaluar su cumplimiento y establecer la continuidad de los mismos.

Actividad: ES-01-02: Monitoreo de los servicios y cumplimiento de requerimientos.

ES-01-02.01: El departamento de control debe monitorear constantemente los criterios de desempeño específicos de cada servicio, esto mediante la elaboración de reportes sobre el cumplimiento de los convenios establecidos en ES-01-1.03, esta evaluación debe ser ejecutada de forma periódica, ya que permite el análisis de las tendencias positivas y negativas de los servicios en general.

ES-01-02.02: El departamento de control debe revisar periódicamente los convenios establecidos con los proveedores internos y externos que prestan los distintos niveles de servicios para asegurar la efectividad y calidad de los servicios.

Actividad: ES-01-03: Identificación y asignación de costos

ES-01-03.01: El departamento financiero con la supervisión del director del área debe establecer un modelo de costos (puede considerarse el ABC o costeo basado en

actividades) para las Tecnologías de Información que pueda soportar los servicios requeridos y alineados con los procesos del negocio. Este modelo debe permitir expresar el costo del objeto de la inversión y ayudar en la toma de decisiones.

ES-01-03.02: El departamento financiero con la supervisión del director del área debe registrar y asignar los costos de los servicios, así como periódicamente deben realizar un análisis de las variaciones presentadas entre el presupuesto y los cargos reales, tomando en consideración los costos directos, indirectos y fijos de los servicios.

ES-01-03.03: El jefe de informática debe realizar reportes sobre los resultados del modelo de costos y el soporte de los servicios requeridos; esté deberá ser presentado a todas las direcciones del negocio.

Para cumplir con lo anterior es necesario contar con lo siguiente:

- Coordinación entre departamentos, es necesario definir un marco de trabajo entre departamentos, dentro del cual debe existir una lista de requerimientos y necesidades y cómo se planea cubrir los mismos, en conjunto.
- Formalización de acuerdos internos y externos en línea con los requerimientos y la capacidad de entrega, esto para saber cuáles son los máximos que se pueden manejar dentro de la organización, sin afectar las demás operaciones. De igual manera es necesario establecer los requerimientos mínimos que se ocupan para poder empezar relaciones con externos, para así no atrasar procesos.
- Informes del cumplimiento de los niveles de servicio (reportes y reuniones), dentro del marco de trabajo entre departamentos, hay tareas que corresponden a diferentes partes de la organización, por lo que es importante tener un control sobre el desarrollo y/o cumplimiento de las mismas.
- Identificación y comunicación de requerimientos de servicios actualizados y nuevos para planeación estratégica, como se mencionó anteriormente es necesaria la

coordinación entre departamentos, por lo que la comunicación entre estos, es necesaria para tener un plan estratégico que beneficie a toda la organización.

- Elaboración y aplicación de un modelo de costos adecuado, continuando con el apoyo entre departamentos, un departamento que debe estar muy involucrado en la prestación de servicios sería el departamento financiero, ya que ellos son los que manejan y controlan mayormente las finanzas de cada servicio, ya sea mediante análisis de costos de los servicios al igual que las variaciones de los mismos.
- Realizar reportes sobre los resultados del modelo de costos, al inicio se plantea la idea de un modelo de costos, para poder determinar si una actividad va a estar fuera del presupuesto inicial, de igual manera hay que mantener un modelo de costos para así poder determinar los precios que se deberían alcanzar para cubrir los costos y dejar un margen operativo para las demás operaciones de la organización.

Subproceso: ES-02 Administración del desempeño, la seguridad y la continuidad

Basado en:

COBIT DS.3, DS.4 y DS.5
Normas Técnicas CGR 4.2

Uno de los puntos críticos en el uso de Tecnologías de Información en la organización es la evaluación y administración del desempeño, la seguridad y continuidad de los servicios, esto debido a que la organización podría tener problemas si el funcionamiento de sus sistemas no es el adecuado y generaría que se alejen de los objetivos previamente establecidos.

Una adecuada administración del desempeño de las Tecnologías de Información es importante porque permite evaluar el funcionamiento, así como encontrar y evaluar las deficiencias de seguridad de la información que se puedan tener en el día a día y permite que la organización mantenga la continuidad del negocio.

La exactitud de los datos y un buen desempeño de las Tecnologías de Información permiten que la organización cumpla con sus objetivos de corto y largo plazo, de una forma eficiente y eficaz. Por lo que se debe hacer el esfuerzo para mantener una administración del desempeño, seguridad y continuidad de los servicios adecuado, lo cual se puede lograr mediante el cumplimiento de los siguientes puntos:

Actividad: ES-02-01: Administrar el desempeño de las Tecnologías de Información.

ES-02-01.01: El jefe de informática debe establecer una planificación que contenga procedimientos para la revisión del desempeño de los servicios enfocados en las capacidades, costos y cargas de trabajo para cada colaborador y sistema, estos procedimientos deben establecerse tomando en consideración la ejecución de los servicios, así como resultados pronosticados con base en las tendencias del trabajo.

ES-02-01.02: El departamento de control debe revisar la aplicación de los procedimientos establecidos en la tarea ES-02-01.01 durante la ejecución de los servicios enfocado a verificar la capacidad y desempeño de los recursos periódicamente, para mitigar el riesgo de una posible interrupción de los servicios.

ES-02-01.03: El departamento de control debe revisar la ejecución de los procedimientos establecidos en la tarea ES-02-01.01 para el pronóstico de necesidades futuras de actualizaciones de recursos, con el fin de que no afecte el desempeño de la organización.

ES-02-01.04: El departamento de control debe generar un reporte que describa los resultados de las revisiones de los procedimientos realizadas en las tareas ES-02-01.02 y ES-02-01.03, con el fin de evaluar si los recursos brindan una capacidad y desempeño adecuado para cubrir con los objetivos actuales y futuros propuestos para los recursos de TI.

ES-02-01.05: El departamento de control debe establecer un plan de monitoreo y pronóstico, el cual genere reportes de desempeño de los servicios. Este plan debe abarcar desde responsables, propósitos, momentos de ejecución, medios para recolección de datos, indicadores, entre otros; hasta su inclusión en el presupuesto del departamento de TI y la necesidad de recursos.

Actividad: ES-02-02: Aseguramiento de la seguridad de los sistemas de información.

ES-02-02.01: El director ejecutivo debe realizar un plan de seguridad que comprenda responsables de su ejecución, objetivos y alcances, diagnóstico de la situación actual, los requerimientos del negocio y riesgos asociados (Ver PO-01-03 y PO-05) y considerando la infraestructura de TI (ver AI-03-01 y AI-03-04) .

ES-02-02.02: El director ejecutivo debe asegurar que exista acceso y comunicación de las políticas y procedimientos de seguridad a todos los departamentos del negocio.

ES-02-02.03: El departamento de TI debe asegurar que se puedan identificar los usuarios y sus acciones con los recursos de TI, esto mediante la implementación de una bitácora electrónica que permita su consulta en el momento que se requiera.

ES-02-02.04: El departamento de TI debe establecer controles periódicos para que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas, así como los privilegios de los usuarios sean aplicados con los movimientos de personal (promociones, traslados o despidos).

ES-02-02.05: El departamento de TI debe realizar monitoreos constantes sobre los accesos y privilegios de los usuarios para identificar actividades inusuales o anormales. Estos deben ser informados mediante reportes de incidencias, con el fin de que quede documentado y aplicar procedimientos para prevenir y detectar estas situaciones en el futuro.

Actividad: ES-02-03: Aseguramiento de la continuidad del servicio.

ES-02-03.01: El jefe de informática debe desarrollar un marco de trabajo para garantizar la continuidad, este debe contener la determinación de resistencia de infraestructura y guías de desarrollo de planes de recuperación para desastres y contingencias.

ES-02-03.02: El departamento de TI con la supervisión del jefe de informática debe realizar planes de continuidad basados en el marco de trabajo antes mencionado en la tarea ES-02-03.01, que debe considerar los requerimientos de resistencia, procesamiento alternativo y capacidad de recuperación de servicios, por lo que debe estar enfocado en los puntos más críticos, con el fin de establecer prioridades de respuesta y recuperación de información, alineado con los objetivos del negocio.

ES-02-03.03: El departamento de TI con la supervisión del jefe de informática debe definir y ejecutar procedimientos para el control de cambios, con el fin de que el plan de continuidad se mantenga actualizado y refleje los requerimientos actuales, así mismo probar el plan de continuidad regularmente para identificar las deficiencias y alcance de la recuperación de datos y reanudación de los sistemas. Estos procedimientos deben ser aprobados previamente por la administración.

ES-02-03.05: El departamento de TI con la supervisión del jefe de informática, deben coordinar pruebas del plan de continuidad haciendo simulacro de alguna contingencia, posterior a la reanudación de las funciones de los sistemas (ya sea por prueba o por desastre), debe determinar si los procedimientos establecidos son adecuados para asegurar una eficiente continuidad, esto mediante la realización de un informe de aplicación del plan de continuidad.

Actividad: ES-02-04: Entrenamiento de personal y administración de configuraciones de los servicios.

ES-02-04.01: El jefe de informática debe identificar las necesidades de entrenamiento con el fin de establecer estrategias y requerimientos de actualización para negocios futuros, conocimiento de valores corporativos, implementación de nuevos recursos de TI, credenciales necesarias, entre otras. Esto se logra mediante una evaluación de aptitudes y conocimientos de los empleados, y generar un reporte sobre los resultados con el fin de identificar la necesidad de entrenamiento.

ES-02-04.02: Una vez establecidas las necesidades de entrenamiento producto de la evaluación realizada en la tarea ES-02-04-.01, el jefe de informática debe asignar personal capacitado con tiempo suficiente para impartir los entrenamientos, así como considerar en conjunto con el departamento de Recursos Humanos, una evaluación posterior al personal que recibió la capacitación, con el fin de tabular los resultados y obtener un informe con los criterios de relevancia, calidad, efectividad y retención de conocimiento.

ES-02-04.03: El departamento de TI debe establecer procedimientos de configuración sobre la gestión y control de cambios, con el fin de lograr integrar los cambios con la gestión de incidentes y gestión de problemas.

ES-02-04.04: El departamento de control debe realizar revisiones según se considere necesario sobre los datos de configuración y software instalados para validar la integridad de los mismos, así como para reportar, actualizar y corregir errores y desviaciones.

Actividad: ES-02-05: Administración de incidentes.

ES-02-05.01: El jefe de informática debe establecer procedimientos para identificar mediante un análisis de las causas y clasificar los incidentes de manera que los incidentes puedan resolverse con la mayor brevedad posible. Este análisis debe contemplar una categoría, impacto, urgencia y prioridad de solución.

ES-02-05.02: El jefe de informática debe realizar un listado que establezca un escalonamiento de las prioridades para atender los incidentes y monitorear adecuadamente el ciclo de vida de los servicios de forma permanente.

ES-02-05.03: El departamento de control debe formar procedimientos para el monitoreo puntual de la resolución de los incidentes desde la raíz, así como confirmar que existan las autorizaciones mínimas (jefatura de cada departamento en el que se van a aplicar) para su aplicación.

Para cumplir con lo anterior es necesario contar con lo siguiente:

- Coordinación entre departamentos, siempre que se habla de desempeño, la coordinación y cooperación entre departamentos es indispensable, por ejemplo el departamento de TI puede dotar a cada departamento de alguna herramienta para la evaluación de alguna tarea en particular o viceversa, donde el departamento evalúa las posibles deficiencias que encuentre en los sistemas de TI.
- Planeación adecuada entre la capacidad y disponibilidad de sistemas, es necesario que siempre existan recursos disponibles para así no retrasar las operaciones de la organización, afectando los objetivos de la misma. De igual manera hay que tener un marco que indique cuáles serían los máximos que pueden manejar los sistemas, para así no sobrecargar las capacidades de las instalaciones y sistemas.
- Reportes de monitoreo y pronóstico del desempeño de los recursos, esto para observar si los pronósticos se están cumpliendo o el desempeño de los mismos está por debajo de los mismos, para así corregir o indagar qué es lo que afecta el desempeño de los recursos de la organización.
- Elaboración de un marco de trabajo de continuidad, así como un plan de continuidad de TI, ya que los avances de la tecnología son cada vez más acelerados, dando espacio a rezagarse si no se tiene un plan de acción que permita actualizarse,

pero sin dejar de lado las tareas habituales para no atrasar en la consecución de los objetivos organizacionales.

- Entrenamiento de personal, este debe ser constante, por la razón de la velocidad con lo que se vuelven obsoletas las tecnologías. De igual manera es necesario que el personal nuevo tenga una capacitación introductoria para que no afecte tanto la continuidad de las tareas.
- Crear procedimientos de resolución de incidentes, dependiendo de la gravedad de cada incidente debe haber un plan a seguir, que inicie desde un nivel básico, donde el colaborador (empleado) pueda resolverlo solo, hasta un incidente donde tengan que intervenir varios departamentos, esto para no afectar la continuidad de las operaciones de la organización.

Subproceso: ES-03 Administración de datos

Basado en:

COBIT DS.11
Normas Técnicas CGR 4.3

La administración de datos juega un papel muy importante en el manejo adecuado de las TI, esto debido a que debe estar enfocada a optimizar el uso y garantizar la disponibilidad de la información cuando se requiera, esto con el fin de mantener un adecuado alineamiento de los objetivos de las Tecnologías de Información con el giro del negocio.

Una administración de datos eficiente y efectiva necesita que los departamentos internos de la organización puedan identificar su necesidad diaria de datos para garantizar la calidad de los servicios e información que se requiera tanto interna como externa.

La administración de datos debe estar enfocada principalmente en obtener un adecuado almacenamiento de datos, respaldos oportunos y seguridad de la misma, estos

puntos están contemplados en los requerimientos de cumplimiento expuestos a continuación:

Actividad: ES03-01: Necesidad de requerimientos para una adecuada administración de datos.

ES-03-01.01: El jefe de informática debe establecer procedimientos para que todos los datos que se esperan procesar sean recibidos por el departamento correspondiente y establecer controles para verificar que el proceso se complete.

ES-03-01.02: El departamento de TI debe realizar un reporte en el cual se verifique que los resultados de los requerimientos de datos cubran las necesidades emergentes.

ES-03-01.03: El jefe de informática debe crear procedimientos para el archivo, almacenamiento y retención de datos.

Actividad: ES-03-02: Respaldo, restauración y eliminación de datos.

ES-03-02.01: El jefe de informática debe definir los procedimientos para asegurar la protección de datos sensibles cuando se eliminen o transfieran los datos a algún software o hardware nuevos.

ES-03-02.02: El jefe de informática tiene que crear procesos adecuados para el respaldo y restauración de sistemas, aplicaciones y datos, esto establecido en el plan de continuidad. Dichos procesos deben contar con la aprobación previa de la administración.

Actividad: ES-03-03: Necesidad de seguridad para la administración de datos.

ES-03-03.01: El jefe de informática debe establecer políticas y procedimientos para aplicar los requerimientos necesarios para la seguridad de los sistemas de información. Los procedimientos de seguridad establecidos deben cubrir el recibo, procesamiento,

almacenamiento y salida de datos y que estén de acuerdo con los objetivos del negocio. Las direcciones del negocio deben dar visto bueno y previo a dichos procedimientos.

Para cumplir con lo anterior es necesario contar con lo siguiente:

- Coordinación entre departamentos, ya que habrá casos donde dos o más departamentos utilicen la misma hoja de información, lo que podría alterar la misma y afectar los datos almacenados. Para solucionar esto entre departamentos debe haber cierta comunicación y coordinación, donde se indique qué departamento tiene prioridad o ventaja sobre el otro, o si es el caso trabajar en conjunto.
- Planeación adecuada entre la capacidad y disponibilidad de sistemas; tener un control del almacenamiento para los datos es clave, puesto que todos los días será mayor, se debe contemplar espacio necesario para evitar que por falta de almacenamiento se tengan que paralizar las tareas de la organización hasta que sea solucionado el problema.
- Respaldo de datos y restauración, es indispensable, ya que siempre existe el riesgo de que se pierdan datos, ya sea adrede o por error, por lo que se requiere un respaldo que permita recuperar los datos perdidos.
- Establecimiento de políticas y procedimientos de seguridad, la seguridad de los datos es sumamente importante, ya que si esta fuese violentada, podrían perderse datos valiosos, información privada, etc. Por lo que hay que tener bien establecido cuáles serán las políticas a seguir, tanto por usuario, como por departamento y organización en conjunto.

Subproceso: ES-04 Administración de procesos operativos y ambiente físico

Basado en:

COBIT DS.10, DS.12 y DS.13
Normas Técnicas CGR 4.5

Como parte de una adecuada implementación y administración de las TI se debe tener en consideración que es necesario un seguimiento adecuado a los procesos operativos y el establecimiento y mantenimiento de un ambiente físico que ayude a cumplir con los objetivos de los sistemas de información.

En esta parte se debe tener en consideración que es esencial realizar una adecuada gestión a los problemas que se presenten para satisfacer los requerimientos del negocio, satisfaciendo a los usuarios finales con un servicio de calidad.

Con el fin de cumplir con requerimientos del negocio y generar servicios de calidad la administración debe considerar los siguientes puntos:

Actividad: ES-04-01: Administración operativa y monitoreo de la infraestructura de TI.

ES-04-01.01: El jefe de informática debe establecer, implementar y dar seguimiento a procedimientos para las operaciones de TI, con el fin de velar por que el personal esté llevando a cabo las tareas adecuadamente.

ES-04-01.02: El jefe de informática debe establecer una programación de tareas para que el personal trabaje por objetivos, realizando las tareas en una secuencia preestablecida que permita resultados más eficientes y mejore el desempeño y la aplicación de los recursos.

ES-04-01.03: El jefe de informática tiene que realizar un plan de monitoreo para identificar si las funciones de los sistemas así como de los registros permiten la reconstrucción, análisis y revisión de las operaciones.

ES-04-01.04: El departamento de TI debe realizar un programa de mantenimiento preventivo para los recursos de Tecnologías de Información, esto para reducir la frecuencia e impacto de las fallas que podrían afectar el desempeño.

Actividad: ES-04-02: Identificación, clasificación y cierre de problemas.

ES-04-02.01: El departamento de TI debe establecer procesos para reportes de problemas identificados en el día a día de trabajo.

ES-04-02.02: El departamento de TI tiene que centralizar los problemas reportados y clasificarlos según incidente para determinar el impacto, urgencia y prioridad.

ES-04-02.03: El departamento de TI tiene que generar un procedimiento adecuado, que registre los problemas solucionados y documentando la eliminación del error que procede a ser un error conocido. Se debe realizar una integración de la administración de cambios, configuración y los problemas conocidos para mejorar los servicios brindados y la calidad del negocio.

Actividad: ES-04-03: Administrar el ambiente físico.

ES-04-03.01: El jefe de informática debe definir claramente y seleccionar los centros de datos físicos en los que se encontrarán los recursos de TI de acuerdo con la necesidad y naturaleza del negocio.

ES-04-03.02: El jefe de informática debe diseñar el esquema de centro de servicios tomando en consideración los riesgos latentes como lo son desastres naturales y los causados por el hombre.

ES-04-03.03: El jefe de informática debe establecer medidas de seguridad físicas como procedimientos que comprendan perímetros de seguridad, zonas de seguridad, ubicación de equipo crítico y áreas de transferencia de datos. El director ejecutivo debe ser consciente sobre los riesgos existentes y la importancia de delimitar el acceso a personas físicas a ciertas áreas de la entidad, a solo el personal autorizado para asegurar el funcionamiento de los recursos de TI.

Para cumplir con lo anterior es necesario contar con lo siguiente:

- Coordinación entre departamentos, ya que habrá casos donde dos o más departamentos utilicen la misma hoja de información, lo que podría alterar la misma y afectar los datos almacenados. Para solucionar esto entre departamentos debe haber cierta comunicación y coordinación, donde se indique qué departamento tiene prioridad o ventaja sobre el otro, o si es el caso trabajar en conjunto.
- Establecimiento de procedimientos para identificación, clasificación y resolución de problemas. Establecimiento de políticas y procedimientos de seguridad, la seguridad de los datos es sumamente importante, ya que si esta fuese violentada, podrían perderse datos valiosos, información privada, etc. Por lo que hay que tener bien establecido cuáles serán las políticas a seguir, tanto por usuario, como por departamento y organización en conjunto.
- Establecimiento de políticas de acceso a instalaciones físicas, esto para limitar el acceso de terceros, e inclusive propios colaboradores, a diferentes lugares dentro de la organización. Controlando así el acceso a ubicaciones que contengan componentes delicados para la seguridad de la información.

PROCESO 4: Monitorear y evaluar

Subproceso: ME-01 Aplicación del Gobierno de TI

Basado en:
COBIT ME.4

Las estrategias de TI deben ir siempre alineadas con las estrategias del negocio, y qué mejor manera que con la aplicación de un Gobierno de TI en la organización. Su influencia además abarca áreas como la planificación y organización, la implementación de nuevos sistemas, la ejecución de procesos organizacionales y su continuidad; por todo lo anterior su creación, implementación y control de manera permanente es clave en toda organización.

La aparición de un sistema efectivo en área de las TI que permita, a partir de estructuras, procesos, liderazgo, roles y responsabilidades garantizar la optimización de los recursos tecnológicos, crear una alineación estratégica, entregar valor, administrar los riesgos y el medir el desempeño.

Para lograr la creación, implementación y permanencia de un Gobierno de TI en la organización es importante que se cumpla como mínimo los siguientes puntos:

Actividad: ME-01-01: Marco de trabajo de gobierno efectivo.

ME-01-01.01: El director ejecutivo debe crear un marco o guía que defina, establezca y alinee de manera clara y completa la visión estratégica de TI (ver proceso PO-01) con los objetivos organizacionales. Así mismo, debe revisar y dar seguimiento de que dicha alineación esté siempre acorde.

ME-01-01.02: El jefe de informática debe crear un marco o guía que cumpla a cabalidad con la ética y cultura organizacional, con las leyes o regulaciones que le rigen de conformidad con las TI del negocio. Para ello debe apoyarse en el proceso ME-04 y las políticas organizacionales ligadas a este tema.

ME-01-01.03: Posterior a la creación del marco de trabajo de Gobierno de TI es fundamental que el jefe de informática comunique de manera formal, y a través de un informe, a la dirección ejecutiva y demás direcciones del negocio para su respectiva aprobación. Clave que se indique de manera puntual la entrega de valor que genera, la capitalización de oportunidades y la obtención de ventajas competitivas que da este elemento a la organización.

Actividad: ME-01-02: Logro de resultados y reportes a la administración.

ME-01-02.01: El jefe de informática debe de manera periódica o como así lo indique la dirección ejecutiva, generar reportes en donde se haga mención de aspectos críticos asociados, hallazgos, puntos de mejora, entre otros.

ME-01-02.02: La dirección ejecutiva tomando en cuenta el grado de tolerancia que la organización considere a nivel de riesgo, debe tomar las acciones necesarias en temas propios de los procesos de TI, de su influencia con el negocio, o que así lo ameriten y hayan sido indicados. Dichas acciones deben ser indicadas y puestas en ejecución por parte del director del departamento correspondiente.

ME-01-02.03: La dirección ejecutiva debe tomar en todo momento las medidas correctivas o de mejora para que el marco de trabajo de Gobierno de TI efectivo permita medir el desempeño y entregar valor a la organización.

Para cumplir con lo anterior es necesario contar con lo siguiente:

- Apoyo de la administración en materia de acceso a la información requerida, recursos necesarios, directrices a los departamentos asociados, entre otros
- Apoyo de todos los departamentos del negocio, ya que cada parte de la organización debe cuidar de sus actividades en cuanto a regulaciones internas y externas, al mismo tiempo que deben estar dispuestos a rendiciones de cuentas cuando se necesite de ellos en cuanto a TI se refiere. al igual que aportar a la consecución de los objetivos organizacionales.
- Visión estratégica de TI, todos los departamentos de la organización están dirigidos a cumplir con ciertos objetivos, estos tienen que ir de la mano con la visión estratégica que tiene el departamento de TI para el cumplimiento de los mismos.
- Administración de los riesgos y recursos de TI, ya que no todo lo puede resolver la administración, es necesario tener una organización y procesos a seguir, dependiendo de la tolerancia al nivel de riesgo, así deberán ser tomadas las medidas. En cuanto a la administración de recursos es necesario que vayan de la mano con la

visión estratégica, para poder organizar mejor el uso de los mismos para una mayor eficacia y eficiencia.

Subproceso: ME-02 Administración del Desempeño de TI

Basado en:

COBIT ME.1
Normas Técnicas CGR 4.2

Es clave que se cuente con las herramientas necesarias para que los recursos de TI ya implementados puedan perdurar por mucho tiempo y muestre la eficiencia y eficacia con la que se ponen a funcionar desde un inicio.

Para lo anterior, la administración –como principal responsable- debe velar porque los sistemas de TI sean monitoreados, gestionados y se les pueda medir su desempeño de manera constante. Claro está que los objetivos de desempeño deben ser establecidos previamente.

En fin, son muchos los beneficios que se obtienen al administrar y valorar el desempeño de las TI; pues permite tomar decisiones de mejora, de corrección o mantenimiento en los sistemas implementados. En resumen, lograr la consecución de objetivos y requerimientos técnicos y del negocio es lo primordial.

Para tener una buena administración del desempeño de TI, y basado en los intereses de la organización, es necesario que se contemplen como mínimo los siguientes puntos:

Actividad: ME-02-01: Plan para la Administración del desempeño de TI.

ME-02-01.01: El jefe de informática con la supervisión de la dirección ejecutiva y basados con la visión estratégica de TI (ver proceso PO-01) debe crear un plan que establezca objetivos, procesos asociados, roles y responsabilidades, alcances, logro de

metas, inversión versus beneficios operativos y de desarrollo, solicitud de reportes y su debida presentación a las direcciones del negocio, entre otros. Todo lo anterior que permita gestionar el desempeño de los sistemas tecnológicos para el logro de los objetivos establecidos.

ME-02-01.02: De manera periódica, el director ejecutivo en apoyo con el jefe de informática deben realizar una revisión de este plan – esto a partir de los reportes entregados, cambios operativos o tecnológicos en el negocio, administración de cambios (ver proceso AI-05), desempeño en la gestión de proyectos (ver actividad PO-03-04), entre otros - con el fin de ajustarlo, modificarlo o mejorarlo acorde con los nuevos requerimientos que el negocio.

Actividad: ME-02-02: Definición de indicadores de Desempeño de TI.

ME-02-02.01: El departamento de TI con la supervisión de la dirección ejecutiva debe establecer las métricas necesarias para valorar de manera cualitativa y cuantitativa si el desempeño de TI es acorde con los requerimientos del negocio; aspectos en materia financiera como porcentaje de costos versus inversiones en materia de TI y según presupuesto; en materia de proyecto como porcentaje de proyectos concluidos exitosamente, tiempos de respuesta y ejecución; en materia de seguridad de la información como porcentaje de incidentes en los sistemas o parches de seguridad implementados en un periodo determinado, entre otros. Dichas métricas deben tener un alcance ligado al nivel de tolerancia de riesgo que la administración haya asignado previamente. Se recomienda implementar un *Balanced Scorecard* o Cuadro de Mando Integral para la medición del desempeño.

ME-02-02.02: De manera periódica, la dirección ejecutiva debe realizar una revisión de estos indicadores con el fin de ajustarlos, modificarlos o establecer mejoras acorde con los nuevos requerimientos que el negocio disponga.

Actividad: ME-02-03: Reportes sistemáticos y oportunos

ME-02-03.01: A partir de la información recabada con los indicadores antes señalados, el departamento de control debe elaborar un reporte de manera periódica a las direcciones del negocio o cuando así le soliciten. Que este reporte ayude a analizar, evaluar y tomar las decisiones prudentes en materia de los procesos y recursos vinculados a las Tecnologías de Información del negocio.

Actividad: ME-02-04: Creación, ejecución y seguimiento de acciones correctivas o de mejora.

ME-02-04.01: La dirección ejecutiva debe dar respuesta a las desviaciones que hayan sido señaladas en los reportes presentados, o así mismo a cualquier aspecto de mejora que se pudiese identificar. Debe asignar roles y responsables, periodos de ejecución, entre otros para el cumplimiento de las tareas indicadas como acción correctiva o de mejora.

ME-02-04.02: La dirección ejecutiva debe dar seguimiento de que todo lo indicado sea cumplido de conformidad en tiempo y eficiencia.

Para cumplir con lo anterior es necesario contar con lo siguiente:

- Apoyo del Departamento de TI, si bien el que tiene que medir el desempeño de sus propias actividades debería de ser el departamento de TI, es necesario contar con el apoyo del mismo para lo que respecta a la administración, ya que ella debe velar porque todo departamento vaya acorde con el resto de departamentos.
- Visión estratégica de TI, como el punto anterior, es necesario que la administración tenga bien claras las metas, para así poder medir el desempeño de cada área, específicamente el del departamento de TI, para así tomar medidas al respecto.

- Administración de recursos y riesgos, siguiendo con el plan de trabajo es necesario monitorear los riesgos inherentes que vengan con cada actividad, de igual manera hay que monitorear el uso y desempeño de los recursos, esto para tomar acciones en caso de desviaciones en los objetivos organizacionales.

Subproceso: ME-03 Implementación y evaluación del Control interno de TI

Basado en:

COBIT ME.2
Normas Técnicas CGR 5.2

La administración debe garantizar la ejecución eficaz y eficiente del sistema de control interno para que la gestión y el proceso de TI estén siempre acorde con los requerimientos del negocio y puedan prevenirse riesgos asociados.

Además, la auditoría interna o externa debe ser un área de apoyo para la organización, pues de conformidad con sus capacidades y competencias, da seguimiento, monitoreo y evalúa la eficiencia y eficacia del Control interno en el área de TI y que los procesos asociados estén alineados de acuerdo con los procedimientos y el cumplimiento de las metas establecidas.

Para contar con un control adecuado en el negocio y su evaluación respectiva, es necesario que se contemplen como mínimo los siguientes puntos:

Actividad: ME-03-01: Definición y elaboración de un sistema de control interno integrado con el marco de trabajo de los procesos de TI

ME-03-01.01: La dirección ejecutiva debe establecer un sistema de control interno dinámico e integral, el cual puede crearse sobre la base de lo que indica el informe COSO, guía importante en la creación de sistemas fundamentados en la planificación, el diseño y la ejecución de controles de acuerdo con las necesidades de la entidad.

ME-03-01.01: La dirección ejecutiva debe considerar que el sistema incluya y se enriquezca con aspectos importantes como:

- Establecer procedimientos para garantizar el compromiso y colaboración de todos los departamentos del negocio en el logro de los objetivos del sistema, refiérase a integridad organizacional, valores éticos y cultura corporativa.

- Formulación de un diagnóstico e identificación de riesgos asociados.

- Desarrollo de acciones de control previstas a nivel de procesos como por ejemplo el estudio de factibilidad, la aprobación previa a la ejecución de un proyecto determinado o la existencia y cumplimiento de políticas y procedimientos de TI por parte de los departamentos del negocio (visto en dominios PO, AI y ES).

- Desarrollo de acciones de control en materia de procesos críticos del negocio como por ejemplo la continuidad y seguridad de los sistemas de información, específicamente en el caso de los servidores (visto en dominios PO, AI y ES).

- Acciones orientadas a su revisión y monitoreo.

Actividad: ME-03-02: Monitoreo y reporte de la efectividad de los controles internos.

ME-03-02.01: La dirección ejecutiva debe establecer un enfoque de monitoreo, en el cual se integra el alcance, metodología, procesos, responsables, métodos para la recolección de datos, entre otros.

ME-03-02.02: El departamento de control es responsable de ejecutar y dar cuentas por la puesta en marcha de dicho enfoque de monitoreo. Debe reportar a las direcciones del negocio, de manera periódica, el estatus o cualquier aspecto de importancia –basado en los componentes críticos, riesgos asociados que se detallan en el proceso P0-01- relacionado con el impacto de TI en el negocio.

ME-03-02.03: La dirección ejecutiva debe encargarse, a partir de dicho reporte, de tomar las decisiones necesarias y oportunas que así lo requieran por el cumplimiento de los objetivos del negocio.

ME-03-02.04: La dirección ejecutiva en apoyo del jefe informático, debe asegurarse de que el proveedor cumpla a cabalidad con lo estipulado de manera contractual cuando los servicios de *outsourcing* de sistemas de información sean necesarios. Es por ello que debe crear, en apoyo con el departamento de TI, una guía de control (cumplimiento de todo lo indicado contractualmente) que dé respuesta a lo anteriormente indicado. Debe tomar decisiones y comunicar de ser necesario.

Actividad: ME-03-03: Revisión del Control interno por parte de terceros.

ME-03-03.01: La dirección ejecutiva debe adquirir de los servicios auditables de terceros, estableciendo con éstos el alcance, precios del servicio, tiempo de ejecución y conclusión, así como cualquier otra consideración que deba ser indicada. Estos servicios deben adquirirse de manera periódica, y que permitan corroborar la adecuada implantación, ejecución y obtención de logros en materia de los requerimientos del negocio a nivel de controles internos.

ME-03-03.02: El equipo de auditoría que sea contratado debe reportar hallazgos de la revisión hecha a la dirección ejecutiva para que sea ésta quien tome las decisiones correspondientes.

Actividad: ME-03-04: Revisiones de auditoría y reporte de la efectividad de dichos controles.

ME-03-04.01: El departamento de control debe reportar de manera periódica a la dirección ejecutiva el estatus o cualquier aspecto de importancia relacionado con los

controles internos implantados a las TI del negocio. Para ello puede basarse en el proceso P0-01- y las actividades ME-02-01, ME-02-02 y ME-02-03.

ME-03-04.02: La dirección ejecutiva debe encargarse, a partir de dicho reporte, de tomar las decisiones necesarias y oportunas que así lo requieran por el cumplimiento de los objetivos del negocio.

Para cumplir con lo anterior es necesario contar con lo siguiente:

- Apoyo del Departamento de TI, en cuanto a la evaluación se refiere, quién puede medir de mejor forma el desempeño de cada sistema es el departamento de TI, por lo que la auditoría interna y/o áreas usuarias deben estar apoyadas en este para futuras evaluaciones y establecer qué tan eficientes y eficaces son estos, y no solo con respecto al control interno. En caso de ser por *outsourcing*, es necesario que la comunicación entre la organización y el proveedor del servicio sea abierta, en el sentido que siempre el proveedor esté disponible para resolver cualquier aspecto que la organización le solicite.
- Visión estratégica de TI, al ser el departamento con mejor conocimiento del control interno de la parte de TI, siempre es bueno ver qué detalles se pueden mejorar y cómo se haría para realizar dicha mejora.
- Administración de recursos y riesgos, es importante monitorear los riesgos inherentes que vengan con cada operación dentro de la organización, también hay que monitorear el uso y desempeño de los recursos, para así tomar acciones en caso de que los mismos no estén cumpliendo las expectativas esperadas de los recursos.
- Plan para la administración del desempeño de TI, como se mencionó anteriormente, la auditoría (o ente controlador) debería dar reportes, ojalá con el apoyo del departamento de TI.

Subproceso: ME-04 Cumplimiento regulatorio asociado a las TI

Basado en:

COBIT ME.3 y ME.4
Normas Técnicas CGR 1.7 y 4.1

Existen legislaciones nacionales e internacionales que se relacionan e influyen de una manera estrecha en la implementación de nuevos sistemas, su ejecución en los procesos organizacionales y su continuidad. Es por ello que es importante que sean identificados, conocidos, entendidos, cumplidos y controlados en todo momento.

En este caso, cabe indicar la obligación por parte de la organización en el cumplimiento de la legislación que le aplica y es pertinente al tema de Tecnologías de Información, a las regulaciones y requerimientos contractuales asociados. El cumplimiento de todo lo anterior, ya sea incluyendo o ajustando las políticas y procedimientos de la organización, viene a reducir el riesgo de posibles incumplimientos, retrasos en los procesos organizacionales e inclusive arreglos y multas que afectan a la organización en la consecución de sus objetivos ya establecidos.

Para cumplir a cabalidad con la legislación, regulaciones y requerimientos correspondientes, es necesario que se contemplen como mínimo los siguientes puntos:

Actividad: ME-04-01: Identificación de requisitos legales y regulatorios ligados con TI

ME-04-01.01: El director ejecutivo debe contar con el entendimiento continuo y actualizado de la legislación que le rija en materia de TI al negocio. Para ello debe considerar las políticas organizacionales y políticas ambientales del negocio, adicional puede pedir asesoría a terceros de ser necesario para la comprensión de aquellos reglamentos locales, de industria o mercado que le competen al negocio, entre otros.

ME-04-01.02: El director ejecutivo debe llevar una bitácora actualizada de toda la información asociada, la cual estará a disposición de las direcciones del negocio, departamento de control o terceros autorizados que la soliciten para la toma de decisiones.

ME-04-01.03: El director ejecutivo en apoyo con el jefe informático debe comunicar con correos, inducciones, boletines informativos, entre otros, a todos los departamentos del negocio aquella legislación en materia de TI que deba ser de acatamiento obligatorio.

Actividad: ME-04-02: Evaluación del impacto de los requisitos regulatorios

ME-04-02.01: El director ejecutivo debe evaluar si el acatamiento de los requisitos regulatorios ligados con TI en el negocio, requiere de modificaciones a lo interno, esto comprendiendo temas como políticas, procedimientos, procesos, administración de riesgos, infraestructura, entre otros.

ME-04-02.02: El director ejecutivo debe tomar en todo momento las medidas necesarias para ajustarse a los requerimientos legales y regulatorios que así le competan al negocio. Para ello debe tener reuniones programadas con las direcciones del negocio, jefe informático y departamento de control que le deben estar comunicando y recomendando según corresponda.

Actividad: ME-04-03: Monitoreo y reporte del cumplimiento regulatorio

ME-04-03.01: El director ejecutivo debe elaborar un plan de cumplimiento que permita establecer el acato de lo considerado en el proceso ME-03-01. Este plan debe contemplar aspectos como el establecimiento de objetivos, procesos asociados, roles y responsabilidades, alcances, entre otros. Todo lo anterior que permita controlar el cumplimiento, según la legislación o regulaciones lo dicten, en materia de TI dentro del negocio.

ME-04-03.02: El director ejecutivo, de manera periódica debe coordinar reuniones y presentar reportes a las direcciones del negocio; todo ello que permita dar a conocer el estatus en materia de cumplimiento de TI

ME-04-03.03: Con lo reportado en la actividad ME-03-03.02, es responsabilidad del director ejecutivo tomar las acciones correspondientes para corrección o ajuste. Debe abarcar planes de acción, roles y responsabilidades, requerimientos para el logro de objetivos, entre otros.

Para cumplir con lo anterior es necesario contar con lo siguiente:

- Conocimiento de la legislación (requisitos legales y regulatorios) ligada con TI y aplicable al negocio. Es indispensable tener muy claro los límites de las leyes, ya que no se quiere caer en ilegalidades, de igual manera si se sabe que hay ciertos requerimientos legales estos pueden llegar a ser una demora, afectando la consecución de los objetivos.
- Visión estratégica de TI al tener objetivos por cumplir, hay que determinar si hay obligaciones legales que se deban cumplir antes de continuar con el cumplimiento de los objetivos organizacionales.
- De ser necesario, asesoría en temas relacionados, si no se posee un departamento legal dentro de la organización, es recomendable que se asesoren en dichos temas, ya que por desconocimiento de la misma puede caer en ilegalidades y eventualmente tener contratiempos por ponerse en regla.

Conclusiones y recomendaciones

5.1 Conclusiones

La necesidad de las organizaciones por contar de manera oportuna con la información necesaria, adecuada, relevante y exacta para el desarrollo de sus actividades operativas, la toma de decisiones y la consecución de sus objetivos departamentales a nivel general del negocio es clave. Claro está que para lograrlo es importante que se puedan tener, implementar y controlar herramientas relacionadas con una adecuada gestión de la seguridad y protección de la información en los sistemas de información.

El auge de la documentación digitalizada y el crecimiento de las organizaciones traen consigo el aumento en el volumen de la información que se procesa. Por lo anterior, se cree que la metodología elaborada y propuesta en este proyecto de graduación viene a convertirse en un instrumento esencial y de interés, puesto que las instituciones van a requerir de procedimientos, planes de acción para así responder con mayores y mejores controles y evitar que la información sea manipulada de manera no autorizada, sea errónea o se genere de manera incompleta para la toma de decisiones.

Ahora bien, en este proyecto ya se han desarrollado cuatro de los cinco capítulos que lo componen. Se realizó desde un estudio y análisis del sector –háblese de fundaciones-, hasta llegar a conocer aspectos propios y vinculantes de FUNDEVI, así como la creación de una metodología aplicable en materia de seguridad y control de la información. A partir de ello son diversos los puntos que se pueden concluir y se detallan a continuación:

- Durante el desarrollo de la investigación se identificó que las fundaciones han mantenido su objetivo primordial desde sus inicios como institución de bienestar social; si bien ya no mantienen una relación estricta con la iglesia, se establecen

como organizaciones asociadas a un fin determinado, sin socios ni miembros, y su duración dependerá de la existencia de este.

Así mismo, en el presente se han establecido leyes y regulaciones debido a su importancia en el desarrollo social, y fue a partir del cambio de la Ley de Reforma Fiscal de 1970 de los EEUU que las fundaciones se consolidaron como organizaciones fundamentales para la sociedad al ser catalogadas como instituciones de beneficencia pública.

Propiamente en Costa Rica las fundaciones se establecieron como instituciones jurídicas privadas con bienestar público a partir de 1973, mediante la aprobación de la Ley No.5338, Ley de Fundaciones, la cual marcó la pauta para la evolución y crecimiento de las fundaciones en el país.

A partir de lo anterior se concluye que las fundaciones tienen un rol muy importante en la sociedad dado que son organizaciones sin fines de lucro que asisten las diferentes acciones del gobierno para socavar la necesidad presentada en la sociedad.

- La administración de la seguridad y el control de la información de las Tecnologías de Información en Costa Rica se inicia desde la década de los 80 hasta el periodo actual, las compañías se han enfocado en realizar una inversión importante en las Tecnologías de Información con el fin de agilizar los procesos de sus negocios, lo cual se evidencia con la creación de la Asociación Nacional de Informática en el año 1982, ante la necesidad de agrupar a los profesionales de esta rama, debido a la alta demanda de las computadoras para los trabajos realizados en las diferentes entidades, esto produjo que los desarrolladores intenten día a día mejorar los sistemas para el manejo de la información, incrementando los estándares de seguridad y control de la misma. Sin embargo, su regulación formal comienza con la supervisión por parte de los órganos gubernamentales, tales como el CONASSIF y la Contraloría General de la República, dichas regulaciones tuvieron sus inicios en 2009 con la creación del Acuerdo SUGEF 2007 y con la publicación de las Normas

técnicas para la gestión y el control de las Tecnologías de Información respectivamente.

Se concluye que a pesar de que existen normativas formales y estrictamente definidas para entidades reguladas, existe otro gran sector fundamental para la sociedad que no tiene regulación en este apartado, tal como las organizaciones sin fines de lucro y sociedades no sujetas a la supervisión que no abarcan las fundaciones.

- Durante el análisis realizado de la estructura se determinó que FUNDEVI contiene una estructura administrativa establecida formalmente, ya que cuenta con políticas tales como políticas de calidad, de transparencia y de responsabilidad social y ambiental por mencionar algunas. También cuenta con una Asamblea General establecida en su acta constitutiva, una junta administrativa, delegado ejecutivo fiscalía, auditoría, auditoría de calidad, dirección de fomento y administración de proyectos, con el fin de garantizar que su operación se encuentre alineada con los objetivos estratégicos incorporados en el plan de la fundación para apoyar a la Universidad de Costa Rica agilizando sus actividades de vínculo remunerado.

  Se concluye que a pesar de contar con una estructura administrativa formal, el departamento de Tecnologías de Información es relativamente nuevo, y se encuentra en un proceso de reestructuración total, lo que genera una oportunidad para implementar regulaciones de seguridad y control de la información para garantizar que esta sea fiable, íntegra y oportuna.

- La normativa realizada por el Consejo Nacional de Supervisión del Sistema Financiero es más rigurosa que la que establece la Contraloría General de la República, dado que la SUGEF 14 09 se basa en el marco COBIT 4.1 y obliga a estas entidades a realizar 17 de sus 34 procesos, lo cual genera que las entidades supervisadas deban contar con un departamento de Tecnologías de Información bastante robusto, así mismo genera un mayor costo operativo debido a su rigidez.

Por otra parte la Contraloría establece mediante sus Normas Técnicas para la gestión y el control de las Tecnologías de Información, una serie de criterios de control que deben acatar las entidades supervisadas como parte de la gestión institucional de las Tecnologías de Información.

Como conclusión estos criterios de control se establecen para diferentes entidades y es por esta razón que los criterios establecidos por la Contraloría General de la República son más generales, debido a que se adaptan a una gran diversidad de instituciones, mientras que las establecidas en la SUGEF 14-09 son más específicas, debido a que se dirigen a un sector más limitado y homogéneo, como lo son las entidades financieras.

- De acuerdo con la encuesta realizada a las cuatro fundaciones de las universidades públicas, se determina que las mismas cuentan con departamentos de Tecnologías de Información establecidos, que valoran el aporte que las Tecnologías de Información realizan al logro de los objetivos organizacionales establecidos en cada plan, asimismo estas organizaciones establecen controles físicos para el resguardo de la información, tienen procedimientos establecidos para el mantenimiento y además obtienen servicios de *outsourcing* para gran parte de sus procedimientos menos críticos. Sin embargo, se identifican diferencias significativas en el manejo de la seguridad y control de la información de las organizaciones.

  A pesar de contar con algunas buenas prácticas del manejo de la gestión de seguridad y control de la información, las organizaciones contestaron con un resultado promedio de 58.10% en todos los criterios fundamentales que se evaluaron en las encuestas. Sin embargo, estos criterios podrían homologarse y mejorar con un marco regulatorio que les aplique.

- La propuesta metodológica contempla criterios de seguridad y control de información con base en los marcos regulatorios del país, en la misma se establecen buenas prácticas mediante una serie de procesos que se deben establecer, los

mismos son rigurosos pero a la vez permiten ser ajustados a las necesidades y características de cada entidad de acuerdo con su entorno.

Los procesos definidos permiten a las diferentes entidades estandarizar sus controles de TI, de igual forma la lista de verificación de cumplimiento de seguridad y control de la información en las tecnologías de información suministrado sirve a las entidades como herramienta para realizar valoraciones iniciales y periódicas sobre su gestión de la seguridad y control de la información, y así tener un panorama más claro de la posición en que se encuentran respecto a este tema, con la finalidad de poder alinear los objetivos de TI con los objetivos organizacionales definidos en los planes estratégicos de cada una.

Se concluye que una adecuada gestión de la información permite a la entidad contar de manera oportuna con la información necesaria, adecuada, relevante y exacta para el desarrollo de sus actividades operativas, la toma de decisiones y la consecución de sus fines para lo cual fue establecida; de esta forma las fundaciones y demás organizaciones sin fines de lucro pueden lograr eficazmente el cumplimento de los objetivos establecidos, del presupuesto, de las expectativas de las direcciones del negocio y en especial desarrollando un crecimiento en materia económica, investigativa y de bienestar social, ejes centrales de las fundaciones.

5.2 Recomendaciones

Posterior a la elaboración de la propuesta metodológica para la gestión de la seguridad y control de la información en Tecnologías de Información de fundaciones, con base en un análisis de la normativa vigente aplicable por la Contraloría General de la República y por el Consejo Nacional de Supervisión del Sistema Financiero para el sector regulado, y con base en las conclusiones establecidas anteriormente, se realizan las recomendaciones descritas a continuación a la Fundación de la Universidad de Costa Rica para la Investigación:

- Se recomienda realizar exámenes periódicos de la seguridad y el control de la información, con el fin de obtener un claro panorama del manejo de la información que se presenta en la organización y el control existente, así como identificar oportunamente los riesgos que puedan afectar la seguridad y control de la información de la misma, esto enfocado en el cumplimiento de mejores prácticas presentado por las entidades reguladas.

- Se recomienda establecer canales de comunicación que permitan la difusión de políticas de control interno, con el fin de mantener las mejores prácticas enfocadas en el manejo de la información, así como los lineamientos con los objetivos organizacionales.

- Se recomienda a la administración de la empresa implementar la propuesta de este trabajo de investigación, con la que se pretende adoptar una cultura de control de la información que abarque toda la organización y que promueva una serie de iniciativas tales como las que se exponen a continuación:

  1. Crear conciencia en los diferentes departamentos para incentivar procesos administrativos y operativos que sean eficientes y eficaces.
  2. Protección de la información contra pérdidas por mala gestión, errores, fraudes o irregularidades en el manejo de las Tecnologías de Información.
  3. Determinar el impacto que podría generar una aplicación obligatoria de las normativas aplicables tanto internas (reglamentos, directrices, políticas y procedimientos) como externas (leyes y normativa técnica).
  4. Generar reportes financieros y operativos completos, confiables y oportunos que permitan detectar las deficiencias de seguridad de la información.

- Se recomienda a las organizaciones ejecutar todos los procesos propuestos que sean aplicables a su entidad, para poder hacer el mejor uso de la metodología propuesta

es necesario que contemplen todos los procesos posibles de la herramienta que se brinda.

ANEXOS

ANEXO #1: Cuestionario para las fundaciones basado en las Normas Técnicas de Gestión y Control de la Contraloría General de la República.

Referencia Capítulo 1 Normas de aplicación

1.3 Gestión de riesgos:

1. ¿Qué riesgos considera la organización a nivel de seguridad y control de la información? Ejemplificar por separado (seguridad y control)

2. ¿La organización mantiene un sistema específico de valorización de riesgos? (Si su respuesta es positiva omitir la pregunta 3)

3. ¿Cómo se lleva a cabo la gestión de los riesgos que considera la organización con respecto a la seguridad y control de la información? Ejemplificar puntualmente.

4. ¿Cuentan con un equipo de trabajo establecido, así como marcos de planificación y ejecución en aspectos de control y seguridad de la información?

5. ¿Qué marco(s) normativo(s) considera la organización para establecer sus criterios de calificación de riesgos de seguridad y control?

1.4 Gestión de la seguridad de la información:

6. ¿Posee la organización políticas de seguridad de la información, así como manual de procedimientos? ¿Si es así, es posible adjuntarla? (si la respuesta es negativa, omitir la pregunta 7).

7. ¿Bajo qué marco normativo se desarrolló la política?

8. ¿Existe algún acuerdo (contrato) de confidencialidad y compromiso con los empleados sobre la seguridad de la información? ¿Si es así, es posible adjuntarla?

9. ¿Existen controles de acceso a las instalaciones? Si la respuesta es sí, indicar cuáles.

10. ¿Existen controles para la ubicación de servidores y otros recursos de Tecnologías de Información claves que contienen la información?

11. ¿Se mantienen requisiciones físicas para las entradas y salidas de equipo? Si hay, indicar quién es el encargado de su custodia.

12. ¿Quién realiza el mantenimiento del equipo de TI y con qué periodicidad?

13. ¿Se mantiene un protocolo para el desecho y reutilización de los recursos de TI? Si hay, describirlo.

14. ¿Cuáles son las condiciones de seguridad y control para los suministros de energía eléctrica, cableado de datos y comunicaciones inalámbricas?

15. ¿Quién en la organización está a cargo de la seguridad y control de la información, así como de la comunicación del estado de la misma? ¿Cuáles son sus funciones y actividades para la valoración y documentación de la misma?

16. Con respecto a nivel de seguridad física y ambiental de los recursos de TI, ¿cuál considera como principal logro o fortalecimiento en los últimos tres años?

17. ¿Cómo cree que ha ayudado a cumplir con los objetivos organizacionales?

18. ¿Cómo realizan la actividad del desecho de documentación física?

19. ¿El departamento encargado de la gestión de TI lleva controles o bitácoras de manera continua con respecto al mantenimiento, actualizaciones o cambios adicionales que se le den a los equipos de la institución?

1.7 Cumplimiento de obligaciones relacionadas con la gestión de TI:

20. ¿Conoce acerca de la existencia de un marco jurídico que deba aplicarse a nivel de Tecnologías de Información en su entidad?

Referencia Capítulo 2 Planificación y Organización

2.1 Planificación de las Tecnologías de Información:

21. ¿Qué papel desempeñan las Tecnologías de Información en la organización?

22. ¿Las funciones de las Tecnologías de Información apoyan la misión, visión y objetivos estratégicos de la organización? (Ejemplifique).

23. ¿Se incluye dentro del presupuesto de la compañía rubros afines con el propósito de las TI? Cite las metas que mantienen dentro del presupuesto actual para las mismas.

2.4 Independencia y Recurso Humano de la Función de TI:

24. ¿El personal de TI mantiene independencia de las áreas usuarias?

25. El departamento de TI, según el organigrama (por favor adjuntar si es posible), ¿dónde se coloca?, ¿a quién reporta o rinde cuentas?, ¿existe algún aspecto en particular que consideran (con respecto a otros departamentos) cuando ingresa personal nuevo en TI?

Referencia Capítulo 4 Prestación de servicios y mantenimiento

4.6 Administración de servicios prestados por terceros:

26. ¿Existe servicio *outsourcing* de los sistemas de información? (si la respuesta es negativa, omitir pregunta 27)

27. ¿Qué contratos de *outsourcing* se tienen y qué alcance tiene cada uno?

28. ¿Quién custodia aquellos contratos con terceros en materia de servicios de software o hardware?

29. ¿Cada cuánto y qué criterios se utilizan si se renuevan aquellos contratos en estado activo o a los que deben ser renovados? ¿Hay responsabilidad y compromiso por parte de estos terceros?

4.3 Administración de los datos:

30. ¿Qué controles existen a nivel de aplicaciones para asegurar que la información sea válida y que sea debidamente procesada y autorizada?

4.5 Manejo de incidentes:

31. ¿Quién y cómo se lleva a cabo la identificación, análisis y resolución de problemas, errores e incidentes significativos en el procesamiento de la información, así como en el sistema?

32. ¿Qué procedimientos realizan para mitigar el riesgo de pérdida de la información?

ANEXO #2: Entrevista a Abonos del Pacífico S.A referente a los servicios recibidos por FUNDEVI.

Entrevista realizada a terceros que reciben servicios de FUNDEVI.

Empresa: Abonos del Pacifico S.A (ABOPAC). Productora y Distribuidora de Fertilizantes, Agroquímicos, entre otros.
Entrevistada: Ing. Bertalicia Arguedas, Representante Técnico, Depto. Ventas ABOPAC.
Entrevistador: José María Vargas Guillén
Fecha: 18 de Mayo del 2015.

1- ¿Qué servicios recibe por parte de FUNDEVI?

Servicio Prestado	Si	No	Información Adicional
Investigac. y Desarrollo Tecnológico	X		Emisiones N2O Piña
Productos Cientificos y Tecnológicos		X	
Capacitaciones, Actualizaciones, etc.	X		Suelos, Fisiología, medición GEI, etc.
Asesorías Especializadas		X	
Servicios de Laboratorio	X		Suelos, foliares, gases.
Servicios Técnicos		X	
Servicios de Certificación		X	
Intercambio Académico		X	
Otros, Indicar cuál		X	

2- ¿Desde hace cuánto recibe servicios por parte de FUNDEVI?

5 AÑOS

3- ¿Cómo cataloga el trabajo de FUNDEVI, y por qué?

El trabajo de las diferentes entidades que nos brindan el servicio son excelentes, por ejemplo: CICA, CIA, sin embargo el servicio posventa es deficiente; lo relacionado con facturación posterior al pago.

4- A nivel de beneficio empresarial, ¿En cuánto favorece el servicio que FUNDEVI les brinda para el cumplimiento de sus objetivos organizacionales?

Es una alianza estratégica entre ABOPAC, como empresa privada y Fudevi como un ente estatal. Realmente nos beneficia mucho

Firma de la Entrevistada: Bertalicia Arguedas M

Abopac

Firma del Entrevistador: José Mª Vargas G.

ANEXO #3: Entrevista a FUNDEVI.

TRANSCRIPCIÓN ENTREVISTA REALIZADA A LOS PERSONALES DEL DEPARTAMENTO DE T.I. DE FUNDEVI EL DÍA 22 MAYO DEL 2015.

Fundevi (F). Ahorita el otro plan está en proceso, pero está demasiado crudo, estamos apenas estructurando, y tenemos algo demasiado básico pero si se pretende que aquí a un par de meses ya esté listo el nuevo.

Grupo (G). Si entonces seria montarlo con el nuevo ya que la idea es que sea útil, por eso nosotros pensábamos el que está ahora y como plan de mejoramiento el que tienen pensado.

F. Rafa, ellos son del proyecto que nos había hablado don Erick, que don Mario cuando en su momento nos había contactado y ellos vienen a saber un poco de la estructura las funciones y cómo funciona el departamento, para que nos ayudes. Entonces lo hacemos con la que estaba antes, porque la que tenemos ahorita no hay mucho.

G. Si, entonces la primera pregunta es cómo ha sido el proceso de evolución de las TI dentro de la organización, ósea como se ha desarrollado, como ha crecido a través de los años, como era cuando FUNDEVI se empezó a crear, como trabajó este departamento, y como fue creciendo ahora que usted me está indicando ahora va a crecer aún más.

F. Bueno, hace seis años, seis años y medio era solo una persona, y el 80% de los servicios eran subcontratados. El tipo de servicio era 100% reactivo, no había planificación ni había algún tipo de servicio proactivo, se empezó a trabajar y a invertir capital en el departamento, no se hacía desarrollo de software en ese entonces. Se contrató a otra persona, y en ese momento ya se empezaron a dividir funciones. Se empezó a hacer planificación e hubo un cambio de personal, aun no se hacía desarrollo dentro de la organización, se compraba todo el software, y ya se empezó a trabajar en los planes que se empezaron a crear 6 meses antes, se invirtió en infraestructura, hubieron varios ataques, bueno, hubo un ataque a la página que nos obligó a cambiar un poco lo que era la dirección en la íbamos a trabajar... íbamos a trabajar primero en lo que era sistemas pero este ataque nos obligó a trabajar primero en lo que fueron las redes, se empezó a invertir en lo que es infraestructura de la seguridad.

G. ¿Cuándo fue este ataque?

F. fue en el 2011

g. ¿Y qué fue lo que pretendía este ataque?

F. Fue de esos robots que anda buscando vulnerabilidades y lo que hace es cargar una página de ha sido hackeado por... de estos grupos que solo andan buscando popularidad.
En ese entonces éramos 2 compañeros uno se iba a especializar en el área de seguridad, en ese caso fui yo, yo me fui especializando en lo que era seguridad y mi compañero en lo que era software, entonces, invertimos en equipo, invertimos en capacitación, se reestructuró completamente la red. Ah bueno una etapa anterior, en el 2010 se hizo toda la red de la Fundación, cableado y estructurado y se certificó la red para poder aplicar a la plataforma de pagos en línea del banco. Este ataque nos hizo cambiar lo que era la visión del departamento que en aquel entonces era optimizar sistemas y cambiamos la visión a que fueran sistemas disponibles y confiables 24/7 entonces empezamos a trabajar lo que era seguridad de las redes y alta disponibilidad...se hizo un departamento completamente nuevo, de desarrollo, se separaron, se crearon dos departamentos. Uno de desarrollo y otro de infraestructura.

G. ¿En qué año fue está separación?

F. Esto fue en el 2011. Entonces el ataque fue en el 2010.
Esa restructuración, después del ataque se creó como la parte de seguridad y el que estaba siguió en la parte del software.

F. Correcto, tuvimos el ataque entonces tuvimos que cambiar completamente el objetivo de la organización, bueno del departamento, y no podíamos dejar de lado lo que ya traíamos. Entonces lo que hicimos fue no tener los dos recursos en la misma sino dejar un recurso encargado en la parte de infraestructura, pero todavía no estaba estructurado que iba a ser un área de TI, o infraestructura y otra área de desarrollo de software. Esto se dio hasta en el 2011 que ya se hizo la propuesta d ya crear 2 subprocesos, uno de desarrollo de TI y en ese entonces se empezó a contratar programadores. Esto fue otro cuestionamiento, íbamos a tener programadores de planilla, o íbamos a contratar freelancers, o si se iba a comprar software.

G. ¿en este momento todavía seguían subcontratando?

F. sí, estaba de hecho en planes el desarrollo del sistema financiero/contable o administración de proyectos, se cotizo con una empresa y salió cómo en 800.000 dólares y lo entregaban hasta 5 años después. Entonces se optó por desarrollar y e ir entregando de forma modular, modulo que se necesita modulo que se desarrolla. La siguiente pregunta fue si se hacía con programadores de planilla o se contratan freelancers. Costos, disponibilidad de recursos, etc. se optó por freelancers y también como para dar una opción a los estudiantes de la U. El asunto de los programadores fue creciendo poco a poco era 1 luego 2...hasta llegar el momento que se contrató, porque los proyectos fueron creciendo se contrató otro analista, en un principio éramos el encargado de tecnología y el encargado de análisis y desarrollo de software. Contrataron otro analista de sistemas porque ya habían

muchos proyectos y se contrató a un técnico para infraestructura, entonces el departamento ya en planilla éramos 4 personas, esto en el 2012.

G. ¿Y actualmente cuantos son?

F. actualmente somos 4 en planilla la estructura en cuanto a personal sigue igual, es hasta hace un mes que se presentó la nueva propuesta. Como lo que era infraestructura ha ido evolucionando, ósea se ha buscado la optimización de procesos, ya no sentimos nosotros que sea tan necesario tener tanto personal para mantener infraestructura que ya está trabajando de una manera muy proactiva y no reactiva... entonces hemos estado orientando los recursos hacia un solo departamento de informática, en donde todos vemos lo que es análisis bueno lo que es software e infraestructura.
G. ¿Igual los cuatro sin aumentar?

F. Exacto, ahí es donde empieza la nueva propuesta, donde lo que buscamos es que todos estemos capacitados para trabajar en todas las áreas, pero con especialidades, ósea habría una persona que va ser como tier 2 o tier 3 en seguridad otra persona que va a estar en nivel superior en análisis o diseño, otra en base de datos, otra persona en infraestructura y redes por ejemplo.

G. Lo único que harían serian reestructurar las funciones, pasarlas a un solo departamento pero con las mismas funciones

F. Exacto, más que nada es por eso, ya una de las áreas evoluciono, prácticamente es muy autómata lo que es infraestructura es algo muy estable muy automatizado y lo que hay que hacer es darle seguimiento y control ya estamos en la etapa de seguimiento y control si vemos el ciclo de tenemos que entrar en una nueva etapa de planificación pero está nueva etapa de planificación requiere de cambios estructurales y es en lo que estamos ahorita, viendo cual es una estructura que se adapte a las necesidades de la organización. Y pensamos que como la organización es tan variable, no sé, hoy puede que decidan hacer un nuevo edificio o crear una sucursal en otro lugar. Entonces se va requerir más recursos para infraestructura. Pero puede que mañana digan que tienen desarrollar un sistema nuevo para alguno de los 700 proyectos entonces se van a requerir más recursos en desarrollo. Entonces lo que queremos es no tener que estar entrando en capacitación... La curva para análisis y desarrollo es casi 6 meses la curva de conocimiento para TI es parecida entonces que nosotros podamos tener un solo "pull" de recursos y que podamos asignar o distribuir según necesidades. La idea es que sea más integral, que no sea tan aislado, sino un solo "pull" de recursos y un solo "pull" de necesidades para informática.

G. ¿El software ya se desarrolló?

F. Ok, eso también fueron varias etapas. El departamento de desarrollo que estuvo anteriormente creó, habían muchas urgencias, entonces se le dio más prioridad a desarrollar

la herramienta que cumpliera con las necesidades básicas, a la parte de calidad de software, entonces el sistema tiene algunas deficiencias en lo que es calidad de software en bases de datos, diseño, documentación. Ahora lo que queremos es entrar en lo que es calidad de software, entonces esas herramientas que ya están funcionando empezar a crear versiones 2 donde estén optimizadas, que sea el mismo fin pero que funcione de una manera más óptima entonces esas son las 2 etapas que han habido en lo que es desarrollo de software y coincidió con lo que fue el cambio del personal, las 2 personas que estaban anteriormente dejaron los sistemas en esta etapa, funcionando con las deficiencias de las que hablamos, pero como la urgencia era que hubiera alguna herramienta para utilizar El departamento cambio en cuestión de 6 meses, salieron las que estaban anteriormente y entraron 2 personas nuevas y desde ese momento se ha venido dando mantenimiento a las herramientas que estaban funcionando, y nos dimos cuenta que se estaba gastando mucho tiempo en mantenimiento en solucionar una herramienta que no debería de estar siendo solucionada, digo estar siendo tan manipulada. Entonces se empezó a trabajar lo que fueron las nuevas propuestas del sistema.
g. ¿Con lo del cambio del edificio se van a ver afectados para la parte del ordenamiento?

f. ¿físicamente?

g. sí

f. Todavía no se sabe. De hecho eso que está ahí fue el primer plano bueno el plano que se anunció con todos estos cambios del edificio estaba pensado con la estructura que les comente de estos cuatro años... entonces los muchachos de desarrollo iban a estar en la última oficina, y nosotros nos íbamos a mantener acá, pero ese mismo día nosotros le presentamos la propuesta de la restructuración a don Roberto, entonces él dijo esto queda cancelado, entonces en el primer piso va a estar todo lo que es la parte operativa, ahí van a estar gestores de proyectos, ejecutivos de proyectos, directores; nosotros nos vamos a quedar aquí en el segundo piso, no les aseguro que sea así, pero si nos vamos a quedar juntos los cuatro y en la segunda planta.

g. ¿Cuáles son las principales responsabilidades y funciones del departamento de T.I aquí?

f. ¿de lo que tenemos actualmente?

g. sí.

f. OK básicamente habían 3 puestos, que eran analista de sistemas de estos hay 2 personas profesional de T.I y técnico especializado en TI.
Es que aquí se llamaba informática el conjunto de desarrollo software e infraestructura.... en lo que es infraestructura y yéndonos directamente a lo que dice el proceso... habían 3 macro-actividades, que eran: nuevas necesidades, mantenimiento correctivo y mantenimiento preventivo. Esto en todo a lo que se refiere infraestructura desde redes,

equipo de cómputo, telefonía, servidores hasta aires acondicionados, alarmas todo lo que tenga que ver con infraestructura en esas 3 áreas.
En esta macro-actividad (nuevas necesidades) lo que se busca es la manera de recuperar o de obtener las necesidades en el área de infraestructura que tenga la organización y se hacía de varias formas, una era por medio de entrevistas con los directores a principio de año, todo esto era para crear un plan de adquisiciones, entrevistas con analistas, encuestas de satisfacción y de clima organizacional. Básicamente esos eran los 3 insumos para capturar lo que eran las necesidades de infraestructura, porque los directores? porque la idea es que los planes que ellos están haciendo nosotros ver si ocupan el apoyo de infraestructura en algún área.

g. adicional a los objetivos.

f. Exactamente. Por qué analistas, para saber cuáles van a ser los recursos que ellos van a requerir en cuanto a básicamente redes y servidores y porque las encuestas de clima organizacional y de satisfacción al cliente? para ver qué es lo que la gente opina que es lo que la gente piensa algo tan básico como la iluminación, es que las oficinas son muy oscuras, entonces hay que ver como solucionamos ese problema. Posterior a esto, una vez que tenemos está información, Primero se hace un análisis de viabilidad, si lo que ellos están pidiendo de alguna manera solventar con lo que ya se tiene en la organización, sin tener que requerir adquisiciones, si se requiere una adquisición, cuánto va costar, si nosotros podemos darle mantenimiento, si no se le puede dar mantenimiento, cuánto va costar ese mantenimiento o si requiere capacitación, por ejemplo. Si pasa todas estas etapas entran en lo que es el plan de adquisiciones. El plan de adquisiciones se presenta junto con el plan anual a la delegación para que le asigne un presupuesto de acuerdo a lo que está dentro de las adquisiciones.
Después entra lo que es el plan de mantenimiento preventivo, el cual también se hace anual, que considera desde el teléfono que tienen los usuarios en la maquina hasta las redes y servidores. cada uno con una periodicidad y actividades diferentes algunas inclusive son diarias, dentro del mantenimiento preventivo se consideran los respaldos de información, igual que dependen del impacto que tengan en la organización, están categorizados, por impacto por tiempo de recuperación, y de acuerdo a está prioridad, al final de cuentas es una sola prioridad, se asigna el nivel de respaldo, hay tres niveles de respaldo, uno es local, todo lo que se trabaja acá está replicado localmente, el segundo nivel es un sitio remoto, no es un sitio alterno porque no levanta, si aquí cae allá no levanta, hay que levantarlo manualmente, todas las máquinas virtuales, ósea este es el segundo nivel, lo que nosotros definimos se replica en el sitio remoto, son máquinas virtuales todo está... tal cual ahí se asigna si se replica una vez al día, dos veces por semana, etc. depende del análisis previo. El segundo nivel es en la nube se contrata un servicio de almacenamiento en la nube para replicar los servicios más críticos bases de datos, sistemas Web se respaldan en la nube como un nivel adicional y el ultimo son medios de almacenamiento magnéticos, y se guardan en una bóveda de seguridad especializada para este tipo de dispositivos.

g. ¿Está bóveda está dentro de la misma organización?

f. No. está fuera de la organización, en cuanto a geolocalización, el primer nivel es en el mismo edificio, el segundo nivel está en la misma área de hecho está en la universidad, el tercer nivel es en la nube y el cuarto nivel, está un poco más lejos pero si es una bóveda contra inundaciones, contra terremotos con piso especial para pisos magnéticos, etc.

G. ¿Eso sería solo para la parte de mantenimiento preventivo. Y la tercera?

f. el mantenimiento correctivo, según como lo veníamos trabajando, aclaro que no se va trabajar de la misma manera, las solicitudes de mantenimiento correctivo se hacían a través de un sistema si no había sistema se hacían por teléfono, llegaban al profesional de T.I, el profesional de T.I asignaba la solicitud dependiendo del área, inclusive como a veces llegaban de software y las pasaba a desarrollo de software, si el problema se le pasaba al técnico, esa era la idea, y no se podía solucionar, se iba escalando y se llegaba al momento que se tenía que subcontratar algún especializado en el área. Estaban categorizadas, las solicitudes, y de acuerdo al tipo de solicitud tenían un SLA. Desde un día hasta 30 días en algunos casos que dependían de adquisición o de apoyo por parte de la Universidad que es tiempo Universidades de Costa Rica y es un poco más lento entonces desde 1 día de respuesta hasta 30 días de respuesta dependiendo de la categoría de la solicitud o del evento, esto en lo que es infraestructura.
En lo que es desarrollo de software, funciones se tiene lo que es análisis, que se hace solicitud de algún sistema que se requiera, se toman todos los requerimientos de ese sistema, se analiza si se va a hacer o en la fundación o si lo vamos a subcontratar, y si se subcontrata se hacen todas las averiguaciones sobre quien lo puede hacer los costos, y si se hace en la fundación, los dos compañeros de análisis hacemos todo el análisis o lo empezamos nosotros y se lo pasamos a los programadores o los programadores con nosotros. Y entonces así se desarrollaría, eso sería para el desarrollo y para las preventivas más que todo las reparaciones, igual pasaba así, el profesional de T.I las detectaba por que le llegaba un problema si ellos no lo podían resolver ellos la elevaban y nosotros nos encargábamos de distribuir el trabajo dependiendo del área que fuera a los compañeros.

g. ¿Ustedes le brindan también soporte de software a los proyectos?

f. sí

G. ¿Los recursos humanos son solo ustedes cuatro?

F. Sí, solo nosotros cuatro.

G. ¿Y recursos físicos?

F. Los servidores y nuestros equipos de trabajo.

G. ¿Existe alguna comisión de T.I?

F. No, pero cualquier reunión que soliciten siempre es con alguno de nosotros, pero no hay ningún comité.

G. ¿Pero con los directivos de la fundación en sí, no existe alguna comisión periódica para ver necesidades?

F. no.

G. ¿El plan anual se le presenta a quién?

F. Al delegado, don Roberto.

G. ¿Recursos humanos son ustedes cuatro, pero siguen subcontratando cuando es necesario o como se decide pasar al nivel de outsourcing?

F. Se hace un análisis por tiempos y por costos y lo que sea más viable, ahí se toma la decisión de si se hace outsourcing o se hace en casa.

(FIN DE LA ENTREVISTA).

ANEXO #4: Tabulación de respuestas.

(VER CD ADJUNTO)

ANEXO #5: Lista de verificación de cumplimiento de seguridad y control de la información.

(VER CD ADJUNTO)

ANEXO #6: Normas técnicas para la gestión y el control de las tecnologías de la información (N-2-2007-CO-DFOE).

(VER CD ADJUNTO).

ANEXO #7: SUGEF 14-09: Reglamento sobre la gestión de la tecnología de información.

(VER CD ADJUNTO)

ANEXO #08: COBIT 4.1: Objetivos de Control para Información y Tecnologías Relacionadas.

(VER CD ADJUNTO)

ANEXO #09: Carta certificada de revisión total del trabajo por parte de Bachiller en Filología Española.

(VER CD ADJUNTO)

Referencias bibliográficas

Ackoff, R. (1962). "Scientific Method: Optimizing applied research decisions" (1ra Ed.). Nueva York: Wiley.

Aguilar, I., Brenes, P., León, I., & Mora, E. (1995). "Asignación y administración de fondos públicos a través de fundaciones". (Memoria de Seminario de Graduación de Licenciatura en Administración Pública). Universidad de Costa Rica, San José, Costa Rica.

Alonso, J. (2003). "Metodología" (11va ed.). México: Limusa.

Calvo, M., Chinchilla, M., Coto, G., & Pacheco, E. (1993). "Las organizaciones no gubernamentales y su participación en la gestión de la política social costarricense". (Seminario de Graduación presentado para optar al título de Licenciatura en Trabajo Social). Universidad de Costa Rica, San José, Costa Rica.

De la Mora, M. (2006). "Metodología de la investigación; Desarrollo de la Inteligencia" Quinta Edición. México: Cengage Learning

González, J. (2001). "Metodologías de Control Interno, Seguridad y Auditoria Informática". En M.G Piattini & E. Del Peso (Ed.). Auditoría Informática un enfoque práctico. Madrid, España: Ra-Ma Editorial.

Hernández, G. (1992). "Un sistema de Información Gerencial para las fundaciones". (Memoria de Seminario de Graduación de Licenciatura en Administración de Negocios). Universidad de Costa Rica, San José, Costa Rica.

Laudon, J. & Laudon. K (2012). "Sistema de información gerencial", decima segunda edición. México, Pearson Educación.

Quesada, J.; Masis, D.; Barahona, M; Meza, T.; Cuevas, R. & Rhenán, J. (1999). "Costa Rica Contemporánea- Raíces del estado de la nación" .Editorial de la Universidad de Costa Rica- Costa Rica.

Ramírez, X., & Umaña, R. (2007) "Propuesta teórica metodológica para el diseño de un sistema de gestión de planos: estudio de caso: la Oficina Ejecutora del Programa de Inversiones de la Universidad de Costa Rica" (Proyecto de graduación (licenciatura en archivística). Universidad de Costa Rica, San José, Costa Rica.

Rodríguez, E. (2004). "Costa Rica en el siglo XX". Universidad Estatal a Distancia, San José, Costa Rica.

Stromberg, A. (1956). "Philanthropic foundations in Latin America". Nueva York: Russell Sage Foundation.

Valero, U. (1969). *"La Fundación como forma de Empresa"*. Universidad de Valladolid. España. Secretariado de Publicaciones - Valladolid.

Sitios web:

Asamblea Legislativa (1973, act.2001). Ley No.5338 "Ley de Fundaciones". Art. No.1. Recuperado de: http://www.asamblea.go.cr/Centro_de_informacion/biblioteca/Centro_Dudas/Lists/Formule%20su%20pregunta/Attachments/626/Ley%205338.pdf.

Asociación Española para la Calidad. (2013). "Centro de Conocimiento: Seguridad de la Información". Recuperado de: http://www.aec.es/web/guest/centro-conocimiento/seguridad-de-la-informacion.

Autoridad Reguladora de los Servicios Públicos (2014), "Diccionario de Términos Regulatorios utilizados en Costa Rica". Recuperado de: http://www.aresep.go.cr/index.php/inicio/diccionario.

Agudo, A. (2015). "Nace un sello para acreditar el buen funcionamiento de las ONG". Diario El País. España. Recuperado de: http://elpais.com/elpais/2015/02/16/planeta_futuro/1424088950_955465.html

Aguirre, L. (2012). "Entrevista para el periódico El País al embajador de EEUU en España". Recuperado de: http://sociedad.elpais.com/sociedad/2012/03/24/actualidad/1332611241_867697.html.

Balbis, J. (2001). "ONGs, Gobernancia y Desarrollo en América Latina y el Caribe. UNESCO". Recuperado de: http://www.unesco.org/most/dsp53_sp.pdf

Berciano, J. (2014). "La importancia y la necesidad de proteger la información sensible". Recuperado de: http://www.redseguridad.com/opinion/articulos/la-importancia-y-la-necesidad-de-proteger-la-informacion-sensible.

Bill and Melinda Gates Foundation (2014). "Who We Are, Foundation Fact Sheet". Recuperado de: http://www.gatesfoundation.org/Who-We-Are/General-Information/Foundation-Factsheet/.

Carmona, A. (1974). "Reseña histórica Hospital San Juan de Dios". Recuperado de: de: http://www.binasss.sa.cr/revistas/hospitales/art72.pdf

Centro de información jurídica. (2007) "Informe de investigación CIJUL con tema las fundaciones, Asesores y Consultores de Centro América". Recuperado de: http://aslegalcr.com/blog/wp-content/uploads/2007/09/1248_fundaciones_10-06.pdf.

Charry, C. & López, S. (2004). "Las fundaciones comunitarias en México y el mundo; Polis: Investigación y Análisis Sociopolítico y Psicosocial". Recuperado de: http://www.redalyc.org/articulo.oa?id=72620402

Comin, M. (2005). "*Gobernar las TI: obtener el máximo valor de la tecnología*." Recuperado de http://www.iese.edu/es/files/Art_ED_Cabre_Microcommerce_ESP_tcm5-7281.pdf

Contraloría General de la República (1994). Ley No.7428 "Ley Orgánica de la Contraloría General de la República". Recuperado de: http://www.tse.go.cr/pdf/normativa/leyorganicaContraloria.pdf.

Contraloría General de la República (2007). "Normas técnicas para la gestión y el control de las Tecnologías de Información". Recuperado de: http://cgrw01.cgr.go.cr/portal/page?_pageid=434,1869313&_dad=portal&_schema=PORTAL.

Contraloría General de la República (2009). "Resolución: R-CO-14-2009". Recuperado de: https://cgrfiles.cgr.go.cr/publico/jaguar/sad_docs/.../R-CO-14-2009(FUNDEVI).doc

Cornell University Law School, (2001), "Organizaciones Sin Fines de Lucro: Una Visión General". Recuperado de: http://www.law.cornell.edu/wex/non-profit_organizations.

Cruz Roja Costarricense (2015). "Quiénes somos: Historia". Recuperado de: http://www.cruzroja.or.cr/index.php?option=com_content&view=article&id=283&Itemid=57

Ernst & Young (2011). "Seguridad de la Información en un mundo sin fronteras". Recuperado de: http://www.ey.com/Publication/vwLUAssets/Seguridad_de_la_informacion_en_un_mundo_sin_fronteras/$FILE/Seguridad_de_la_informacion_en_un_mundo_sin_fronteras.pdf.

Fundación Ana Ross (2015). “Inicio e Historia”. Recuperado de: http://ross.or.cr/web2015/fundacion-anna-rossFundación Costa Rica- Canadá (2015). *Inicio e Historia*. Recuperado de: http://www.fundacioncostaricacanada.org/quienessomos/historia

Fundación de la Universidad de Costa Rica para la Investigación (2011). Recuperado de: http://www.fundevi.ucr.ac.cr/

Fundación para el Desarrollo Académico de la Universidad Nacional (FUNDAUNA). (2014). Recuperado de: http://www.fundauna.org/

Fundación Tecnológica de Costa Rica (FUNDATEC). (2016). Recuperado de: https://www.fundatec.ac.cr/

Fundación de la Universidad Estatal a Distancia para el Desarrollo y Promoción de la Educación a Distancia (FUNDEPREDI). (2015). Recuperado de: http://www.fundepredi.org/

Fondo de Naciones Unidas para la Infancia (UNICEF). (2014). *UNICEF, Costa Rica*. Recuperado de: http://www.unicef.org/costarica/overview_12319.htm

Fondo de Naciones Unidas para la Infancia (UNICEF). (2015). ¿Quiénes somos?. Recuperado de: http://www.unicef.org/spanish/

Foundation Center (2014). “Aportes filantrópicos de fundaciones estadounidenses: América Latina”. *2010–2012*. Recuperado de: http://foundationcenter.org/gainknowledge/research/pdf/latinamerica_20102012_espanol.pdf

Gonzáles, C. (2007). “La Importancia de la digitalización de archivos para la biblioteca” Recuperado de

http://eprints.rclis.org/10647/1/La_importancia_de_la_digitalizaci%C3%B3n_de_archivos_para_la_bi%E2%80%A6.pdf

IT GOVERNANCE INSTITUTE, (2007). "COBIT 4.1 Controls Objectives for Information and related Technology". Cuarta Edición. Recuperado de: http://www.isaca.org/Knowledge-Center/cobit/Documents/COBIT4.pdf.

Pérez, F. (2014). "Ciber-seguridad: Un reto cargado de desafíos y también un campo lleno de oportunidades". Recuperado de: http://www.cantabriatic.com/ciberseguridad-desafios_y_oportunidades/

Pérez, R. (2002). ¿Qué es una Fundación?, *su origen*. Recuperado de: http://www.abogadodefundaciones.com/que-es-una-fundacion/

Portal de la Investigación-Universidad de Costa Rica (2015). *FUNDEVI*. Recuperado de: http://www.vinv.ucr.ac.cr/index.php?option=com_content&task=view&id=79

Sabino, C. (1996). "Proceso de Investigación". Recuperado de: https://metodoinvestigacion.files.wordpress.com/2008/02/el-proceso-de-investigacion_carlos-sabino.pdf.

Scott, S. (2004). "Fundaciones Filantrópicas y Cooperación al Desarrollo". Traducción de extracto del diario del Comité de Ayuda al Desarrollo (CAD). Recuperado de: http://www.oecd.org/investment/stats/31670558.pdf

Superintendencia General de Entidades Financieras. (2016). "Listado de entidades sujetas a fiscalización al 02 de setiembre del 2016". Recuperado de: https://www.sugef.fi.cr/publicaciones/listado_entidades_sujetas_fiscalizacion/2016/09-%20Lista%20de%20entidades%20al%2002-09-2016.pdf

Superintendencia General de Entidades Financieras. (2016). “Reglamento sobre Administración Integral de Riesgos, Acuerdo 2-10”. Recuperado de: http://www.sugef.fi.cr/servicios/documentos/Normativa/NormativaPrudencial%5CReglamento%202-10%5CSUGEF%202-10.pdf.Superintendencia General de Entidades Financieras. (2016).

Superintendencia General de Entidades Financieras. (2016). “Acuerdo SUGEF 24-00 Reglamento para juzgar la situación económica-financiera de las entidades fiscalizadas”. Recuperado de: https://www.sugef.fi.cr/normativa/normativa_vigente/documentos/SUGEF%2024-00%20(v18%20setiembre%202014).pdf

Superintendencia General de Valores. (2010). Mercado de Valores. Recuperado de: http://www.sugeval.fi.cr/mercadovalores/Paginas/SistemaFinanciero.aspx.

Universidad de Costa Rica, (2008) Oficio en Respuesta al Informe No-DFOE-SOC-1-2008 de fecha 01 de febrero del 2008, denominado “Informe sobre los mecanismos de control establecidos por la Universidad de Costa Rica en la actividad de vinculación externa realizada con la coadyuvancia de la Fundación de la Universidad de Costa Rica para la Investigación (FUNDEVI). Recuperado de: http://wvw.nacion.com/ln_ee/2008/febrero/18/_MMedia/0000002991.doc.