MAESTRIA EN ADMINISTRACION DE TECNOLOGIAS DE INFORMACION

UNIVERSIDAD PARA LA COOPERACION INTERNACIONAL
(UCI)

ANALISIS FINANCIERO Y DE RIESGO AL TRASLADAR EL PROCESAMIENTO Y ALMACENAMIENTO DE LA INFORMACION CRITICA DE COOPEALIANZA R.L A UN CENTRO DE DATOS SUBCONTRATADO EN COSTA RICA

NORBERTO LEE RODRIGUEZ MADRIGAL

PROYECTO FINAL DE GRADUACION PRESENTADO COMO REQUISITO PARCIAL PARA OPTAR POR EL TITULO DE MÁSTER EN ADMINISTRACIÓN DE TECNOLOGIAS DE LA INFORMACION

San José, Costa Rica

Marzo 2016

UNIVERSIDAD PARA LA COOPERACION INTERNACIONAL
(UCI)

Este Proyecto Final de Graduación fue aprobado por la Universidad como Requisito parcial para optar al grado de Máster en Administración de Tecnologías de la Información

Marco Ugarte Ulate
PROFESOR TUTOR

_____
Melissa Vincenzi García
LECTOR No.1

_____
Jorge Trejos Gutiérrez
LECTOR No.2

_____
Norberto Rodríguez Madrigal
SUSTENTANTE

DEDICATORIA

Primero a Dios por ser mi guía y compañero de batallas. A mi madre Lorena Madrigal García por enseñarme lo importante de ayudar a los demás y a mi padre Alexis Rodríguez Madrigal por siempre inculcarme y servirme de ejemplo en no dejar de aprender y que el estudio es la respuesta a todo.

A mis dos hijos Ian y Ethan Rodríguez Sancho que son mi fuerza e inspiración para enfrentar los días que aún no han venido.

AGRADECIMIENTOS

A COOPEALIANZA R.L por creer e invertir constantemente en sus funcionarios, otorgando entrenamiento y capacitación de calidad.

A Víctor Julio Martínez Navarro Gerente de Operaciones y Francisco Montoya Mora Gerente General en COOPEALIANZA R.L; por darme la oportunidad de ser parte de esta gran cooperativa e invertir en mi formación profesional.

A mis compañeros en COOPEALIANZA R.L por todo el apoyo y contribución durante la realización de este trabajo.

INDICE

ÍNDICE DE FIGURAS

ÍNDICE DE CUADROS

ÍNDICE DE ABREVIATURAS

AI – Siglas del dominio COBIT Adquirir e Implementar

AYA – Siglas del Instituto Costarricense de Acueductos y Alcantarillados

ANSI – Siglas en inglés de *American National Standards Institute*

ATH – Siglas de la red de cajeros automáticos A toda Hora

COBIT – Siglas en inglés de *Control Objectives for Information and related Technology*

CCSS – Siglas de la Caja Costarricense del Seguro Social

CCTV – Siglas en inglés de *Closed Circuit Television*

ES – Siglas del dominio COBIT Entregar y Soportar

FODA – Siglas del análisis de fortalezas, oportunidades, debilidades y amenazas

ICE – Siglas del Instituto Costarricense de Electricidad

ISO – Siglas en inglés de *International Organization for Standardization*

ISP – Siglas en ingles de *Internet Service Provider*

ITIL – Siglas en inglés de *Information Technology Infraestructure Library*

ME – Siglas del dominio COBIT Monitorear y Evaluar

ROI – Siglas en ingles de *Return on investment* (retorno de inversión)

SINPE – Siglas del Sistema Nacional de Pagos Electrónicos en Costa Rica

SUGEF – Siglas de la Superintendencia General de Entidades Financieras

TI – Siglas de Tecnologías de Información

TIA – Siglas en inglés de *Telecomunications Industry Association*

TIER – Siglas de la clasificación de disponibilidad de centros de datos según el *Up Time Institute*

TIR – Siglas del método financiero Tasa Interna de Retorno

UPS – Siglas en inglés de *Uninterruptible Power Supply*

VAN – Siglas del método financiero Valor Actual Neto

WACC – Siglas en inglés de *Weighted Average Cost of Capital* (Costo Medio Ponderado de Capital)

RESUMEN EJECUTIVO

En el año 2004 la cooperativa de ahorro y crédito y servicios múltiples COOPEALIANZA R.L decide destinar recursos financieros al diseño y construcción de su propio centro de datos, con dicha decisión todo el personal de Tecnologías de Información debió involucrarse ya que al tener una estructura organizacional limitada cada miembro tendría que responsabilizarse por mantener en operación dicho centro de datos. Por otra parte la cooperativa tuvo que destinar en dicho periodo, recursos financieros por más de dos millones y medio de dólares, lo anterior sin considerar el costo total anual de propiedad en los que se incurre con un centro de datos de este tipo y que al estar en una zona alejada (Pérez Zeledón) con respecto a la concentración de proveedores que ofrecen soporte a este tipo de infraestructura, el costo se incrementó de manera considerable.

Es importante indicar además que en el año 2016 el centro de datos principal de COOPEALIANZA R.L ubicado en Pérez Zeledón, cumplió más de diez años de haber entrado en operación, es así como todos los principales componentes de infraestructura, eléctricos, mecánicos, físicos y de seguridad, deberán ser renovados y por otra parte la cooperativa requiere analizar si en lugar de construir un nuevo centro de datos, más bien aprovecha las oportunidades que ofrecen los centros de datos subcontratados que cumplen con certificaciones tales como *COBIT*, *ITIL*, ISO 27000 y certificaciones *TIER* del *Up Time Institute*, por mencionar algunas. Es por lo anterior que con este proyecto se pretende realizar un análisis financiero y de riesgo al trasladar el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica; con lo anterior obtener una justificación o sustento a la hora de decidir diseñar y construir un nuevo centro de datos o bien subcontratar dicho servicio.

El objetivo general de este proyecto consistió en realizar un análisis financiero y de riesgo al trasladar el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica; ya que para una entidad financiera como COOPEALIANZA R.L, donde su principal negocio es la colocación de crédito, el ahorro y los servicios financieros múltiples, se convierte en una importante decisión estratégica no sólo redirigir recursos financieros hacia su principal negocio sino que además se vuelve relevante que el personal de Tecnologías de Información se enfoque más al giro de negocio principal y se justifique el traslado de la operativa actual de mantener el centro de datos hacia una empresa especializada en dicho campo, con lo anterior contribuir con el negocio de la cooperativa en gestionar de una manera eficiente y razonable los recursos de Tecnologías de Información.

En este proyecto y como parte de los objetivos específicos, se elaboró un análisis financiero del costo inicial y de mantenimiento anual estimado de construir un

nuevo centro de datos para COOPEALIANZA R.L que soporte el procesamiento y almacenamiento de la información crítica para los próximos 10 años; se desarrolló un análisis financiero de los costos anuales de arrendamiento y servicios complementarios de centros de datos subcontratados para soportar el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L para los próximos 10 años; se ejecutó el proceso de gestión de riesgos de acuerdo al marco ISO 31000 a la actividad de trasladar el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica y finalmente se proporcionó a la alta administración de COOPEALIANZA R.L de recomendaciones para contribuir con la decisión estratégica en función de la operación del nuevo centro de datos.

La metodología que se utilizó para satisfacer los objetivos antes mencionados consistió en la obtención de datos con el objetivo de realizar el análisis financiero al construir un nuevo centro de datos y además la alternativa de subcontratarlo, para lo anterior se obtuvieron datos de proveedores sobre los principales costos de los componentes y/o servicios que formen parte según la modalidad. Para la obtención de datos con el objetivo de realizar el análisis de riesgo al subcontratar un centro de datos a una empresa dedicada a este tipo de servicios, se realizaron encuestas a un grupo interdisciplinario de funcionarios de COOPEALIANZA R.L, a fin de obtener calificaciones de probabilidad e impacto sobre los riesgos identificados tanto para el riesgo inherente como para el riesgo residual.

Una vez recolectados los datos sobre los principales costos alrededor de construir un nuevo centro de datos y/o de subcontratarlo, dichos datos se procesaron utilizando la técnica financiera del flujo de caja para el proyecto con capital propio como para el flujo de caja para el proyecto de subcontratación del centro de datos; además se aplicaron técnicas financieras como el valor actual neto (VAN) y la tasa interna de retorno (TIR), lo anterior con el objetivo de obtener un resultado financiero que permitiera a la cooperativa tomar decisiones adecuadas con respecto a la gestión de los recursos. Por otra parte y con respecto al análisis de riesgo, una vez realizadas las respectivas encuestas, los resultados de las mismas se incorporaron en un informe de evaluación de riesgo y se mostraron en un mapa de calor de riesgo inherente y de riesgo residual lo que permitió obtener los niveles de exposición de COOPEALIANZA R.L que se obtienen al subcontratar un centro de datos a una empresa dedicada a este tipo de servicios, lográndose observar además como los controles actuales minimizan los riesgos y además permitiendo identificar en cuales riesgos se requiere mejorar la efectividad del control o bien complementar con otros controles.

Como resultado de los análisis financieros efectuados, tanto la construcción del nuevo centro de datos como la subcontratación resultan financieramente viables, sin embargo la alternativa de subcontratación de un centro de datos resulta en menores requerimientos de inversión y patrimonio, permitiendo el uso de los recursos escasos al giro propio del negocio de la cooperativa, que es la intermediación financiera. Para complementar el análisis financiero, el proceso de gestión de riesgos a la actividad de trasladar el procesamiento y almacenamiento

de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica, da como resultado que la cooperativa puede fortalecer aún más su capacidad de resistencia ante amenazas y vulnerabilidades propias del contexto interno y externo de la cooperativa en cuanto a la subcontratación de servicios con terceros y además respaldado por sus experiencias previas tanto en la construcción de un centro de datos así como la subcontratación del centro de datos alterno que posee actualmente.

1 INTRODUCCION

1.1 Antecedentes

El presente trabajo se desarrolla en la cooperativa costarricense de ahorro y crédito COOPEALIANZA R.L, dicha cooperativa a partir del año 2010 inició como parte de una estrategia organizacional, que todas aquellas actividades o servicios necesarios para su gestión pero que significarán una distracción para la realización de su actividad principal (Ahorro y Crédito) deberían ser evaluados para que eventualmente fuesen realizados por empresas subcontratadas que demostraran capacidad y trayectoria en dicha actividad.

Como parte del alineamiento estratégico que Tecnologías de Información de COOPEALIANZA debió realizar, se identificaron algunas actividades o servicios que tenían características relevantes para convertirse en fuertes candidatos para que empresas especializadas y de trayectoria asumieran dicha responsabilidad, por parte de COOPEALIANZA se estaría gestionando la calidad y desempeño del servicio con una adecuada gestión del riesgo. Algunas de las actividades y servicios que se identificaron fueron: diseño y desarrollo de software, gestión de la mesa de servicio, monitoreo de la capacidad y desempeño de la infraestructura crítica de TI, gestión de la infraestructura de comunicaciones, gestión y soporte de los equipos de cómputo del usuario final y la gestión de los centros de datos.

La totalidad de las actividades y/o servicios mencionados en el párrafo anterior fueron efectivamente subcontratados en el corto plazo, excepto lo que respecta al tema de los centros de datos, cuando se analiza lo que significa la gestión de los centros de datos, nace la necesidad de sustentar dicha decisión enfocados en dos aspectos relevantes para una entidad financiera como COOPEALIANZA R.L, el primer aspecto es gestionar los riesgos de trasladar el almacenamiento y procesamiento de la información crítica de COOPEALIANZA R.L a un tercero; el segundo aspecto es poder sustentar financieramente entre construir un nuevo

centro de datos o bien ser consecuentes con la estrategia organizacional y aprovechar los servicios especializados de empresas de importante trayectoria que ofrecen este tipo de servicios en el territorio costarricense.

Adicional a los dos aspectos anteriores, se agrega la necesidad de reemplazar y/o renovar muchos de los componentes con los que cuenta actualmente el centro de datos ubicado en el cantón de Pérez Zeledón, lo anterior se debe a que la mayoría de estos están por cumplir 10 años de haberse adquirido y puestos en operación, a partir del año 2016 componentes tales como: aires acondicionados, sistemas de suministro ininterrumpido de energía a base de baterías (UPS), alarmas de incendio, alarmas de detección de intrusos, sistemas de identificación biométrico, así como otros componentes eléctricos cumplirán su vida útil y por lo tanto deberán ser cambiados, por otra parte la cooperativa está considerando descartar el edificio donde se encuentra el actual centro de datos y trasladarlo a un nuevo edificio a inicios del año 2017, por lo que se hace también necesario prever cualquier inversión en cuanto a espacio físico en el nuevo edificio, lo anterior en caso que se justifique realizar nuevas inversiones para dicho proyecto versus la alternativa de subcontratar el servicio del centro de datos.

Es por lo anterior que COOPEALIANZA R.L requiere un análisis financiero y de riesgo al trasladar el procesamiento y almacenamiento de la información crítica a un centro de datos subcontratado en el territorio costarricense; además al ser una entidad supervisada por la Superintendencia General de Entidades Financieras (SUGEF) y tener que acatar la normativa SUGEF 14-09 “Reglamento sobre la Gestión de la Tecnología de Información”, lo anterior toma mayor relevancia ya que dicho ente supervisor obliga a todas las entidades financieras a realizar una adecuada gestión de los recursos de TI por medio del proceso COBIT PO5 “Administrar la inversión en TI” y además minimizar el riesgo cuando se seleccionan los centros de datos por medio del proceso COBIT DS12 “Administrar el ambiente físico” y en específico en su objetivo de control detallado DS12.1 “Selección y Diseño del Centro de Datos” establece lo siguiente “Definir y

seleccionar los centros de datos físicos para el equipo de TI para soportar la estrategia de tecnología ligada a la estrategia del negocio. Esta selección y diseño del esquema de un centro de datos debe tomar en cuenta el riesgo asociado con desastres naturales y causados por el hombre. También debe considerar las leyes y regulaciones correspondientes, tales como regulaciones de seguridad y de salud en el trabajo.”

Es por todo lo anterior que COOPEALIANZA R.L día con día reafirma su compromiso de asegurar calidad y disponibilidad en los servicios financieros que ofrece a todos sus asociados y clientes; lo anterior por medio de la adopción e implementación de buenas prácticas, marcos de control y una adecuada gestión de la inversión y de los riesgos que se encuentran inmersos en las actividades de la industria financiera donde se encuentra.

1.2 Problemática

En el año 2004 la cooperativa de ahorro y crédito y servicios múltiples COOPEALIANZA R.L decide destinar recursos financieros al diseño y construcción de su propio centro de datos, con dicha decisión todo el personal de Tecnologías de Información debió involucrarse ya que al tener una estructura organizacional limitada cada miembro tendría que responsabilizarse por mantener en operación dicho centro de datos.

Con lo anterior el personal de Administración de Base de Datos, Sistemas de Información, Soporte Técnico, Mesa de Servicio tendrían que cumplir alguna función de soporte y/o monitoreo de algún componente crítico del centro de datos, sin descuidar sus funciones principales y acordes al área de tecnología para la cual fueron contratados.

Por otra parte la cooperativa tuvo que destinar en dicho periodo, recursos financieros por más de dos millones y medio de dólares, lo anterior sin considerar el costo total anual de propiedad en los que se incurre con un centro de datos de este tipo y que al estar en una zona alejada con respecto a la concentración de proveedores que ofrecen soporte a este tipo de infraestructura, el costo se incrementaría de manera considerable.

También es relevante indicar que en el año 2004 las alternativas existentes en cuanto a subcontratar un centro de datos eran inexistentes o muy limitadas, y por otra parte existía una especie de monopolio y control de los precios, lo que hacía que se convirtiera en un servicio excesivamente costoso; además se debe indicar que la infraestructura de telecomunicaciones estaba muy limitada y se contaba con un único proveedor de servicio, en este caso propiedad del estado costarricense donde no había opción de exigir un acuerdo de nivel de servicio acorde a la criticidad del servicio que la cooperativa requería para acceder a su información principal desde sus distintas ubicaciones.

En el año 2016 el centro de datos principal de COOPEALIANZA R.L ubicado en el cantón de Pérez Zeledón, cumplió más de diez años de haber entrado en operación, es así como todos los principales componentes de infraestructura, eléctricos, mecánicos, físicos y de seguridad deben ser renovados; debemos además agregar que entre los años 2004 y 2006 dicho centro de datos fue implementado en una edificación que no fue diseñada desde su inicio para soportar procesamiento y almacenamiento crítico de información, sino que más bien se realizaron adaptaciones y remodelaciones a fin de incorporar los diferentes componentes que requería la cooperativa para un centro de datos.

La cooperativa como parte de su misión, visión y objetivos estratégicos ha establecido duplicar la empresa cada tres años, lo anterior requiere de un importante compromiso e inversión en aspectos de continuidad y seguridad de la información crítica y relevante para soportar el negocio de la cooperativa.

Como parte de la planificación estratégica de Tecnologías de Información de COOPEALIANZA R.L para el periodo 2015 – 2017 (COOPEALIANZA R.L, 2014), específicamente en el análisis de fortalezas, oportunidades, debilidades y amenazas (FODA) se identificó la siguiente oportunidad “Reducir los costos en infraestructura física en centros de datos y aprovechar los servicios con terceros en la nube y centros de datos subcontratados.”

Es por lo anterior que la cooperativa requiere sustentar de una manera razonable la inversiones y esfuerzos requeridos para un nuevo centro de datos, considerando una correcta gestión de los recursos financieros y de los riesgos que podrían impactar de manera negativa la integridad, disponibilidad y confidencialidad de la información crítica que mantiene la cooperativa.

1.3 Justificación del problema

El tema de este proyecto se elige ya que para la cooperativa de ahorro y crédito y servicios múltiples costarricense COOPEALIANZA R.L se vuelve crucialmente importante contar con un análisis financiero y de riesgo que le permita gestionar de una manera eficiente los recursos con los que cuenta la cooperativa y con el objetivo de contar con una base sólida para decidir entre volver a invertir en un propio centro de datos de procesamiento crítico, o bien, aprovechar las alternativas existentes y en constante evolución por parte de empresas dedicadas al negocio de centros de datos certificados dentro del territorio costarricense.

Las inversiones realizadas hace más de 10 años por COOPEALIANZA R.L en su propio centro de datos ubicado en el cantón de Pérez Zeledón, significaron inversiones cercanas a los dos millones y medio de dólares, esto a su vez significó importantes inversiones alrededor de los costos totales de propiedad y por el hecho de mantener en operación un centro de datos de procesamiento crítico.

Al entrar en operación el centro de datos en el año 2006 y con el gran inconveniente de encontrarse ubicado a una distancia de más de 136 kilómetros de la capital, los tiempos de atención por parte de los proveedores para atender averías, realizar mantenimientos preventivos y correctivos no logran ser inferiores a las seis horas; casi diez años después y para una empresa del tamaño de COOPEALIANZA R.L, dichos tiempos de atención en caso de producirse un incidente o una contingencia en el centro de datos eventualmente podría producir importantes pérdidas financieras y afectación de la imagen.

Adicional a lo anterior la cooperativa tuvo que incurrir en mantener componentes bastante complejos y que requieren de un monitoreo constante a fin de asegurar su operación continua en el tiempo, componentes tales como: planta eléctrica, sistemas de suministro eléctrico ininterrumpido, aires acondicionados de precisión, sistemas de monitoreo, sistemas de prevención de intrusos y alarmas contra robo, sistemas de prevención temprana del fuego, instalación de gabinetes de protección de equipamiento, por mencionar algunos. Lo anterior significó además que algunos de dichos componentes tuviesen que duplicarse a fin de aumentar los niveles de disponibilidad y que ante cualquier incidente o falla en un componente, el otro soportara la operación mientras tanto se corregía el problema. Como puede notarse tanto la cooperativa como su personal debieron asumir inversiones, roles y responsabilidades distintas al giro de negocio de COOPEALIANZA R.L.

Para una entidad financiera como COOPELIANZA R.L, donde su principal negocio es la colocación de crédito, el ahorro y los servicios financieros múltiples se convierte en una importante decisión estratégica no sólo redirigir recursos financieros hacia su principal negocio sino que además se vuelve relevante que el personal de Tecnologías de Información y otras áreas de la cooperativa se enfoquen más al giro de negocio principal y traslade la operativa actual de mantener el centro de datos hacia una empresa especializada en dicho campo, con lo anterior contribuir con el negocio de la cooperativa en gestionar de una manera eficiente y razonable los recursos de Tecnologías de Información.

Por otra parte la alta administración definió dentro de sus estrategias de largo plazo la adopción paulatina pero constante de subcontratar aquellos servicios que generen valor al negocio de la cooperativa y permitan contribuir con la rentabilidad de la misma.

Para lo anterior la cooperativa estableció la siguiente creencia, que no sólo considera los negocios con nuestros clientes y asociados, sino que además considera todos aquellos negocios que se realizan con socios y proveedores, la creencia dice “Nos gustan los buenos negocios” lo cual significa “Conocemos y comprendemos los servicios financieros ofrecidos y por eso buscamos nuevos negocios, pensando siempre en ganar - ganar”.

En congruencia con la estrategia organizacional y la anterior creencia, Tecnologías de Información de COOPEALIANZA R.L estableció en su planificación estratégica para el periodo 2015 – 2017 la siguiente estrategia: “Crecer responsablemente en la contratación de servicios de terceros; otorgando tareas operativas especializadas a empresas de reconocida trayectoria, enfocando al personal de TI en las metas crucialmente importantes, generando altos niveles de disponibilidad, seguridad, desempeño y calidad en los servicios tecnológicos que se entregan, todo lo anterior alineado a las creencias de COOPEALIANZA R.L.”.

Con el resultado del análisis financiero y de riesgo, la cooperativa tendrá un importante insumo para respaldar la decisión estratégica de invertir en un nuevo centro de datos o bien tener el respectivo sustento financiero y de riesgo para justificar la subcontratación, lo cual es de gran relevancia al ser una entidad financiera regulada por la Superintendencia General de Entidades Financieras (SUGEF) y para asegurarle a su base de asociados y de clientes de servicios financieros de calidad y que se encuentren siempre disponibles cuando son requeridos.

1.4 Objetivo general

Realizar un análisis financiero y de riesgo al trasladar el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica para que la alta administración justifique la decisión.

1.5 Objetivos específicos

- Elaborar un análisis financiero del costo inicial y de mantenimiento anual estimado de construir un nuevo centro de datos para COOPEALIANZA R.L que soporte el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L para los próximos 10 años para que pueda ser comparado con los costos de un centro de datos subcontratado.
- Desarrollar un análisis financiero de los costos anuales de arrendamiento y servicios complementarios de centros de datos subcontratados para soportar el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L para los próximos 10 años para que pueda ser comparado con los costos de un centro de datos propio.
- Ejecutar el proceso de gestión de riesgos de acuerdo al marco ISO 31000 a la actividad de trasladar el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica para que la alta administración entienda, comprenda y gestione los riesgos de dicha actividad.
- Proporcionar a la alta administración de COOPEALIANZA R.L de recomendaciones para que contribuyan con la decisión estratégica en función de la operación del nuevo centro de datos.

2 MARCO TEORICO

2.1 Marco institucional

Antecedentes de la Institución.

La historia de COOPEALIANZA R.L se remonta al 22 de agosto de 1971, cuando un grupo de 1.175 asociados, con una visión impresionante, lograron fusionar dos pequeñas cooperativas que se ubicaban en San Isidro de El General, COOPESANI y COOPEZEL. Esta unión marcó lo que sería el destino de COOPEALIANZA, la empresa que registra la mayor cantidad de fusiones y absorciones en Costa Rica.

Esta cooperativa en el año 1971, se destacaba por ofrecer a sus asociados productos de ahorro y crédito que se complementaban con suministros agrícolas y artículos para el hogar, con la limitante que ubicaba su único punto de servicio en el distrito de San Isidro de El General.

En 1972 los servicios de COOPEALIANZA se expandieron, ya que ubicó una nueva oficina en el distrito de Pejibaye de Pérez Zeledón, al absorber por fusión a COOPEJI. Durante estos primeros años, COOPEALIANZA se comienza a consolidar en el cantón de Pérez Zeledón al ofrecer servicios y productos de calidad. Dentro de este proceso de consolidación, en 1978 fusiona COOPEPLATANARES que se ubicaba en el distrito de Platanares.

La necesidad de crecer y consolidarse continuó, es así como en 1993 se fusiona con COOPEGOLFO lo que permitió que se posicionara como la entidad financiera de la Zona Sur. El sueño de crecimiento continuo y el nuevo milenio trajo nuevas alianzas estratégicas que permitieron que otras cooperativas se unieran al proceso. En el 2000, lo hizo COOPECOLÓN y cuatro años después COOPECORRALES, cooperativa del cantón de Poás de la provincia de Alajuela.

No dejando de lado el crecimiento y la apertura al cambio, en el 2004 la Cooperativa de Maestros de Nicoya, COOPMANI, decide unirse a COOPEALIANZA. En el 2005, COOPENARANJO se unió a esta gran alianza y en el año 2013, la cobertura de COOPEALIANZA llega al cantón de Grecia mediante la fusión por absorción con COOPETACARES.

El objetivo fundamental de COOPEALIANZA R.L es la actividad de ahorro y crédito, fomentándolo entre sus asociados en forma sistemática y brindando opciones de financiamiento, conjuntamente con una amplia gama de servicios financieros. Su actividad principal es la intermediación financiera la cual está regulada por la Ley de Regulación de la actividad de intermediación Financiera de las Organizaciones Cooperativas Nº 7391, así como por las disposiciones de la Superintendencia de Entidades Financieras (SUGEF), instancia que supervisa sus actuaciones.

Entre sus servicios complementarios se encuentra el pago de servicios públicos (telefonía, agua, electricidad) además el cobro de televisión por cable, televisión satelital, seguros auto - expedidles, asistencias, recargas celulares, cobro de marchamos, cobro de impuestos tributarios y municipales, pago de planillas, por mencionar algunos.

Actualmente COOPEALIANZA R.L posee 53 oficinas distribuidas en 31 cantones; dicha cooperativa cuenta a la fecha con más de 160 000 asociados, además posee una estructura de más de 700 colaboradores que se distribuyen en sus 53 oficinas a lo largo del territorio costarricense. (COOPEALIANZA R.L, s.f.)

Misión y Visión.

Misión.

Somos la Cooperativa de cobertura nacional que ofrece mayor solidez, confianza, seguridad y beneficios a sus asociados, mediante servicios financieros competitivos y con una atención ágil y adecuada de sus necesidades.

Visión.

Seremos una empresa cooperativa que duplica su tamaño en activos cada tres años, reconocida por su desempeño superior sostenido, la excelencia de sus colaboradores, la satisfacción de sus asociados y su contribución a la comunidad.

Estructura Organizativa

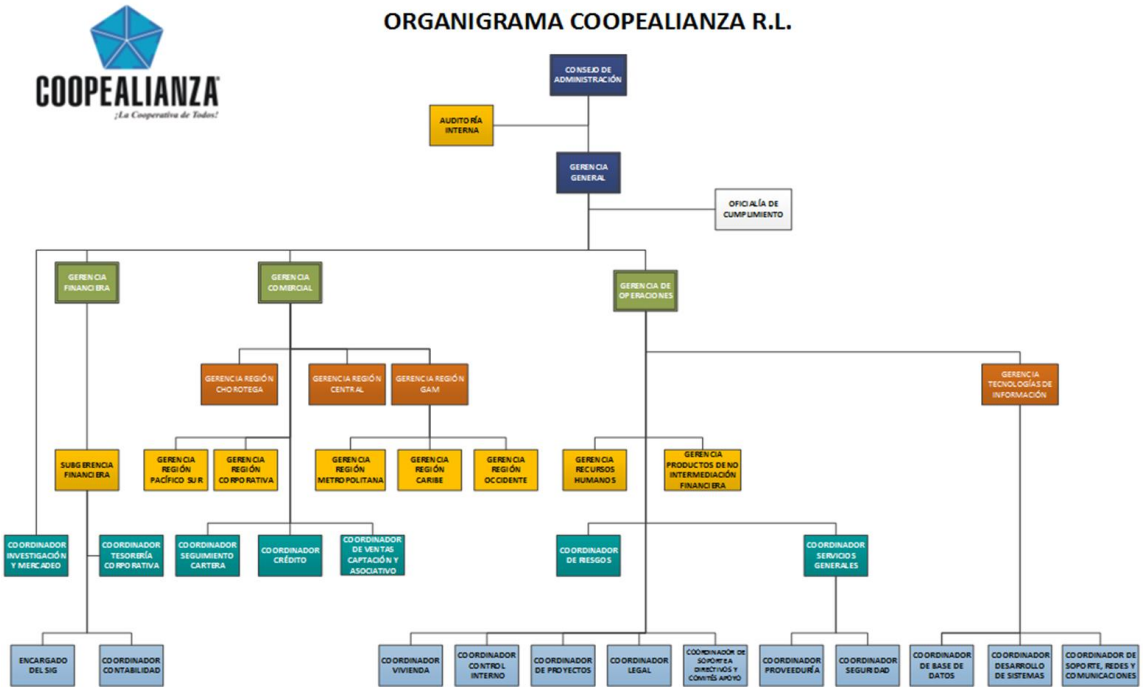


Figura 1: Organigrama Organizacional COOPEALIANZA R.L (COOPEALIANZA R.L, 2014)

Productos que Ofrece.

COOPEALIANZA R.L es una cooperativa que ofrece servicios y productos de ahorro y crédito, así como servicios múltiples. Como parte de los productos de ahorro y crédito, COOPEALIANZA R.L ofrece el ahorro a la vista o ahorro a corto plazo, con este tipo de ahorro se pueden realizar los depósitos y retiros que sean necesarios y por medio de la red de cajeros automáticos ATH se puede retirar efectivo en el lugar de conveniencia; el fondo de inversión múltiple que es un ahorro pactado a un mediano y/o largo plazo, el certificado de ahorro a plazo fijo el cual es un ahorro a un plazo determinado y donde se ofrece la opción que los rendimientos que se obtengan de dicha inversión se retiren a conveniencia o bien se capitalicen en la misma inversión para aumentar dicho patrimonio.

COOPEALIANZA R.L ofrece además diferentes opciones para suplir necesidades de sus asociados por medio de los créditos personales, para vivienda y para desarrollo empresarial. Este tipo de financiamiento se ofrece con una atención personalizada, de una forma ágil y con condiciones muy favorables.

Otros servicios que ofrece COOPEALIANZA R.L a sus asociados y clientes son:

- Tarjeta de débito y crédito.
- Alianza Asistencias.
- Emisión de Firma Digital.
- Transferencias entre entidades financieras por medio de SINPE.
- Cajeros Automáticos de la red ATH.
- Pólizas de vida, hogar, auto expedidles.
- Cancelación de impuestos municipales, Ministerio de Hacienda, terrestres.
- Pago de servicios públicos y otros (AyA, ICE, CCSS, Cable, Colegiaturas)
- Transferencia de dinero por medio de *Western Union*.
- Deducciones de planilla.
- Cancelación automática (ahorros a plazo, servicios públicos, créditos)

- Salarios y pensiones.
- Convenios comerciales.
- Pago de marchamos.

2.2 Marco Teórico

Las empresas establecen metas y objetivos para lograr maximizar las ganancias, obtener resultados financieros positivos y a su vez contribuir con el bienestar de accionistas, empleados, proveedores y clientes. Para lograr lo anterior las organizaciones se apoyan en aspectos que logren gestionar las operaciones financieras que se realizan dentro de la empresa, lo anterior con el objetivo de obtener un panorama o diagnóstico claro sobre las decisiones que deben de tomarse para contribuir con la rentabilidad y sostenibilidad de la empresa en el tiempo.

2.2.1 Análisis Financiero

El análisis financiero se compone de una serie de técnicas, herramientas y metodologías aplicadas a la evaluación, que conforman en elemento de control en la empresa. Mediante esos instrumentos se identifican los problemas y las áreas favorables y críticas de la gestión financiera. Esto constituye un sistema de retroalimentación que permite tomar las acciones para mejorar las áreas de debilidad y aprovechar al máximo las áreas de fortaleza. (Salas, 2001)

2.2.1.1 Construcción del flujo de caja de un proyecto

Es importante cuando se piensa en la construcción de un flujo de caja de un proyecto de inversión tener claridad del horizonte de tiempo que será considerado para determinar las estructuras de ingresos y costos que se visualizan a futuro.

La confección correcta de un flujo de caja es la determinación del horizonte de evaluación que, en una situación ideal, debiera ser igual a la vida útil real del proyecto, del activo o del sistema que origina el estudio. De esta forma, la

estructura de costos y beneficios futuros de la proyección estaría directamente asociada con la ocurrencia esperada de los ingresos y egresos de caja en el total del periodo involucrado. (Sapag, 2001)

La estructura general de un flujo de caja corresponde a varias columnas que representan los momentos en que ocurren los costos y beneficios de un proyecto, Cada momento refleja dos cosas: los movimientos de caja ocurridos durante un periodo, generalmente de un año, y los desembolsos que deben estar realizados para que los eventos del periodo siguiente puedan ocurrir. Por ejemplo, en un proyecto con un horizonte de tiempo de diez años, se deberá construir un flujo de caja con once columnas, una para cada año de funcionamiento y otra para reflejar todos los desembolsos previos a la puesta en marcha, Esta última va antes que las demás, se conoce como momento cero e incluye lo que se denomina calendario de inversiones. (Sapag, 2001)

2.2.1.2 Proyectos de *outsourcing*

Los proyectos de *outsourcing* son, quizás, los que exhiben un mayor desarrollo en los últimos años dentro de las opciones de inversión en mejora que buscan las empresas para optimizar la rentabilidad de su gestión. Esto se explica por las claras ventajas que se han podido observar en aquellas instituciones que han externalizado parte de sus actividades. Entre las principales ventajas se pueden mencionar las siguientes: (Sapag, 2001)

a. concentrar los esfuerzos de la empresa en desarrollar la actividad de su giro principal.

b. compartir el riesgo de las inversiones con el proveedor externo.

c. liberar recursos que pueden ser utilizados en otras actividades más rentables.

d. generar entradas de capital por la eventual venta de activos que se dejan de ocupar.

e. mejorar la eficiencia al traspasar la ejecución de actividades especializadas a expertos.

f. acceder a tecnologías de punta sin tener que realizar inversiones frecuentes en modernizarse, y

g. suplir insuficiencias de capacidad de servicios para apoyar las estrategias de crecimiento.

Sin embargo también se identifican algunas desventajas que se desprenden de los proyectos que subcontratan las empresas, a continuación algunas de estas: (Sapag, 2001)

a. la pérdida de control directo sobre la actividad descentralizada.

b. la dependencia de terceros.

c. el traspaso de información.

d. el eventual mayor costo externo.

e. la administración del proceso de compra a terceros.

f. la pérdida de talentos internos.

Otra desventaja del *outsourcing* es la posible pérdida en la confidencialidad de la información sobre, por ejemplo, niveles de actividad, especialmente cuando se externaliza el almacenamiento o el manejo informático de la empresa. (Sapag, 2001)

Considerando las ventajas y desventajas anteriores es importante que cuando se evalúen proyectos de inversión que involucra la subcontratación de productos o servicios por parte de la organización, se realice una identificación detallada de todos los costos involucrados, tanto directos como indirectos incluyendo aquellos que se relacionan con la administración y supervisión del desempeño con respecto a la relación con el tercero, así como aquellos aspectos que eventualmente

involucran aumentos de algunos costos por parte de los proveedores en el tiempo de la contratación.

2.2.1.3 Requerimiento de capital para una entidad financiera según Basilea

De acuerdo con el documento emitido por el Banco de Pagos Internacionales, denominado “Principios Básicos” para una supervisión bancaria eficaz, el principio 16: Suficiencia de capital, establece que: “El supervisor exige a los bancos unos requerimientos de capital prudentes y adecuados que reflejen los riesgos asumidos, y afrontados, por un banco en el contexto de la situación macroeconómica y de los mercados donde opera. El supervisor define los componentes del capital, teniendo en cuenta su capacidad para absorber pérdidas.” (Banco de Pagos Internacionales, 2012)

En línea con lo anterior, en el caso de Costa Rica la Superintendencia General de Entidades Financieras, a través del Acuerdo SUGEF 3-06, Reglamento sobre la suficiencia patrimonial de entidades financieras, en el artículo 33 establece un mínimo para el obtener un grado normal para el indicador de suficiencia patrimonial del 10%, el cual se calcula según la siguiente fórmula:

$$SP_E = \frac{CB}{RC + 10 * (RP + R\lambda + RO)} * 100[\%]$$

SPE = Suficiencia patrimonial de la entidad.
CB = Capital base.
RC = Activos y pasivos contingentes ponderados por riesgo de crédito más riesgo de precio de liquidación en operaciones con derivados cambiarios.
RO = Requerimiento patrimonial por riesgo operacional.
RP = Requerimiento de capital por riesgo de precio más requerimiento de capital por riesgo de variación de tasas de interés en operaciones con derivados cambiarios.
$R\lambda$ = Requerimiento de capital por riesgo cambiario.

Por otra parte el Acuerdo SUGEF 24-00 Reglamento para juzgar la situación económica-financiera de las entidades fiscalizadas, en el artículo 20, establece

tres niveles de normalidad, con un grado superior del 14%. (Superintendencia General de Entidades Financieras de Costa Rica)

Sin embargo, COOPEALIANZA R.L. como una medida prudencial en la PO-027 “Políticas para el fortalecimiento de la gestión cuantitativa y cualitativa en el Grupo Financiero Alianza”, establece, que la “La Suficiencia Patrimonial de COOPEALIANZA R.L. deberá ser igual o mayor al 16%.”

En el caso particular, de las inversiones relacionadas a un centro de datos, por las características del activo su ponderación de riesgo de crédito (RC) que aplicaría sería del 100%, de conformidad con lo establecido en el artículo 18 del Acuerdo SUGEF 3-06.

Por lo tanto, tomado como base la política interna quiere decir que por cada 100 colones invertidos en el centro de datos, habría un requerimiento de capital de 16 colones que la empresa debería conseguir. A efectos de comprender el impacto de una inversión de este tipo sin aporte de capital debe entenderse que por cada 100 millones de colones, se impacta en la suficiencia patrimonial de COOPEALIANZA R.L. en 0.01%. La suficiencia patrimonial al 30 de noviembre del 2015, asciende a 15.85%.

2.2.1.4 Cálculo y análisis de la viabilidad económica

Cuando se deben realizar análisis de aspectos económicos o financieros en proyectos de inversión a fin de determinar la viabilidad económica y considerar el valor del dinero en el tiempo, se utilizan métodos como el Valor Actual Neto (VAN) y la Tasa Interna de Retorno (TIR), a continuación se describen estos dos métodos.

La viabilidad económica busca definir, mediante la comparación de los beneficios y costos estimados de un proyecto, si es rentable la versión que demanda su implementación. (Sapag, 2001)

2.2.1.4.1 **Valor Actual Neto**

El valor actual neto (VAN) es el método más conocido, mejor y más generalmente aceptado por los evaluadores de proyectos. Mide la rentabilidad del proyecto en valores monetarios que exceden a la rentabilidad deseada después de recuperar toda la inversión. Para ello, calcula el valor actual de todos los flujos futuros de caja proyectados a partir del primer período de operación y le resta la inversión total expresada en el momento cero.

Si el resultado es mayor que cero, mostrará cuánto se gana con el proyecto, después de recuperar la inversión, por sobre la tasa i que se exigía de retorno al proyecto; si el resultado es igual a cero, indica que el proyecto reporta exactamente la tasa i que se quería obtener después de recuperar el capital invertido y, si el resultado es negativo, muestra el monto que falta para ganar la tasa que se deseaba obtener después de recuperada la inversión. (Sapag, 2001)

2.2.1.4.2 **Tasa Interna de Retorno**

La tasa interna de retorno (TIR) es la tasa que iguala la suma de los flujos descontados a la inversión inicial. La TIR es la tasa de interés real que genera el proyecto en “n” periodos. (Casia, 2006)

El análisis financiero va a permitir identificar la estructura de ingresos y costos por medio de los flujos de caja tanto para el proyecto con capital propio, así como para el proyecto de *outsourcing;* además por medio de las técnicas del VAN y el TIR se evalúa el valor del dinero en el tiempo para reforzar el análisis de viabilidad económica.

Adicional al análisis financiero, se hace necesario evaluar los aspectos de gestión del riesgo para el proyecto de outsourcing, básicamente por los riesgos que representa para una empresa entregar parte o la totalidad del procesamiento y/o almacenamiento de su información crítica a un tercero. Para abordar este aspecto

a continuación se incorporan algunos elementos principales del proceso de gestión de riesgos según ISO 31000.

2.2.2 Proceso de Gestión de Riesgos según ISO 31000

Un proceso de gestión de riesgos de acuerdo a ISO 31000, es la aplicación sistemática de políticas de gestión, procedimientos y prácticas para las actividades de comunicación, consultoría, se establece el contexto, la identificación, análisis, evaluación, tratamiento, seguimiento y la revisión de riesgo. (International Organization for Standardization, 2009)

Tal y como se indica, el proceso de gestión de riesgos en las organizaciones no abarca únicamente actividades de identificación, análisis, evaluación, tratamiento, seguimiento y revisión del riesgo, sino que además requiere previamente de un importante compromiso de la alta administración por medio del establecimiento de políticas y procedimientos que logren soportar todas las áreas de la empresa; además es relevante realizar un análisis del contexto externo e interno a la empresa para que de igual manera se fortalezca el proceso con una mejor comprensión de cada uno de los interesados.

Muchos individuos y/o organizaciones podrían preguntarse de que manera el proceso de gestión de riesgos podría ayudarles; se puede indicar que ISO 31000 está diseñado para ayudar a las organizaciones a: (Campos, 2010)

a. Aumentar la probabilidad de lograr los objetivos de fomentar una gestión proactiva.
b. Ser consciente de la necesidad de identificar y tratar los riesgos en toda la organización.
c. Mejorar la identificación de las oportunidades y amenazas.
d. Mejorar la confianza de los interesados en la organización.

e. Efectivamente asignar y utilizar recursos para el tratamiento del riesgo.
f. Reducir al mínimo las pérdidas.
g. Mejorar la capacidad de resistencia de la organización.

2.2.2.1 Establecer el contexto

La organización debe comprender y establecer el contexto externo e interno de cómo se va a relacionar el ámbito de los riesgos particulares a la actividad o contexto.

Lo anterior es como una especie de análisis previo que permitirá dirigir los esfuerzos organizacionales hacia elementos que realmente favorezcan el logro de los principales objetivos que ha definido la empresa, se basa en delimitar y comprender ampliamente el enfoque del proceso de gestión de riesgos; por ejemplo al aplicar el proceso de gestión de riesgos a un proceso de crédito en una entidad financiera difiere en esfuerzo y complejidad de aplicarlo a una actividad o proyecto de migración de software de una versión anterior a otra más reciente; los aspectos a considerar tanto a nivel interno de la organización como del entorno que la rodea van a diferir eventualmente.

El contexto externo se refiere al entorno externo que condiciona, favorece o limita a la organización hacia el logro de los objetivos. Según la International Organization for Standardization (2009), el contexto externo puede incluir, pero no limitarse a:

a. Natural social y cultural, político, jurídico, reglamentario, financiero, tecnológico, económico, y entorno competitivo, ya sea internacional, nacional, regional o local.
b. Factores clave y las tendencias con repercusiones en los objetivos de la organización, y
c. Las relaciones con las percepciones y los valores de los interesados externos.

El contexto interno se refiere a los aspectos internos de la empresa u organización, es decir aspectos como la cultura organizacional, los procesos de negocio que soportan a la empresa, la estructura organizativa establecida y la estrategia organizacional definida.

El contexto interno es cualquier cosa dentro de la organización que puede influir en la manera en la que la organización va a gestionar el riesgo. Debe establecerse debido a que: (International Organization for Standardization, 2009)

a. La gestión del riesgo tiene lugar en el contexto de los objetivos de la organización.
b. Los objetivos y criterios de un determinado proyecto, proceso o actividad debe ser considerado a la luz de objetivos de la organización como un todo, y
c. Algunas organizaciones no reconocen las oportunidades para lograr su proyecto estratégico, de negocios o los objetivos, y esto afecta el compromiso institucional en curso, la credibilidad, confianza y valor.

El contexto interno puede incluir, pero no limitarse a: (International Organization for Standardization, 2009)

a. Gobernanza, la estructura organizativa, las funciones y responsabilidades.
b. Las políticas, los objetivos y las estrategias que están en marcha para alcanzarlos.
c. Capacidades, entendida en términos de recursos y conocimientos (capital, por ejemplo, tiempo, personas, procesos, sistemas y tecnologías)
d. Las relaciones con los y las percepciones y los valores de los grupos de interés internos.
e. Cultura de la organización.

f. Los sistemas de información, flujos de información y la toma de decisiones (tanto formales como informales)
g. Normas, directrices y modelos adoptados por la organización, y
h. La forma y el alcance de las relaciones contractuales.

2.2.2.2 Identificación de riesgos

De acuerdo a ISO 31000, la organización debe identificar las fuentes de riesgo, zonas de impactos, los acontecimientos (incluyendo los cambios en las circunstancias) y sus causas y sus posibles consecuencias. La identificación completa es fundamental, porque el riesgo que no se identifica en esta etapa no se incluye en el análisis posterior. (International Organization for Standardization, 2009)

Se recomienda que en esta etapa participen personas con experiencia y conocimiento comprobado, ISO 31000 indica que las personas con los conocimientos adecuados deberían de participar en la identificación de riesgos. (International Organization for Standardization, 2009)

De acuerdo al párrafo anterior, es importante poder lograr el compromiso de aquellos individuos o áreas de la organización que son requeridos para aportar insumos relevantes debido a su experiencia y conocimiento en el ámbito o contexto del proceso de gestión de riesgos, además suele involucrarse aquellos individuos que eventualmente se verán afectados o involucrados posteriormente, ya sea por la aparición de nuevas rutinas de control del riesgo o la adopción de nuevas responsabilidades y/o funciones como resultado de la mitigación de los riesgos.

2.2.2.3 Análisis de riesgos

Al realizar el análisis de riesgos, cada riesgo es analizado determinando su impacto y probabilidad.

El análisis puede ser cualitativo, cuantitativo o semi – cuantitativo, o una combinación de estos, dependiendo de las circunstancias. Consecuencias y la probabilidad puede ser determinada por la modelización de los resultados de un evento o serie de eventos, o por la extrapolación de los estudios experimentales o de los datos disponibles. (International Organization for Standardization, 2009)

Como resultado del análisis de riesgos la organización puede identificar en un mapa de calor como el que se muestra en la figura 2, el nivel de probabilidad e impacto resultante para el riesgo inherente (riesgo sin controles). Además el mapa de calor es de gran ayuda para que de una manera gráfica se muestre el desplazamiento que tiene un riesgo desde una zona crítica (extrema o alta) a una menos crítica (moderado, bajo y muy bajo) y viceversa, dicha categorización de colores es lo que la organización define como su apetito al riesgo; es decir los niveles de riesgo aceptables se ubican en el mapa de calor en la zona sin demarcar (Muy bajo, Bajo, Moderado); estos riesgos estarán sujetos a actividades o planes de mitigación una vez que se hayan atendido los riesgos críticos o con mayor prioridad, es decir los riesgos que se encuentran ubicados en la zona demarcada (Alto y Extremo).

	Impacto	Insignificante	Bajo	Moderado	Significativo	Crítico
Probabilidad	Valor	1	2	3	4	5
Casi cierta	5	Moderado	Alto	Extremo	Extremo	Extremo
Probable	4	Bajo	Moderado	Alto	Extremo	Extremo
Posible	3	Bajo	Bajo	Moderado	Alto	Extremo
Poco probable	2	Muy bajo	Bajo	Bajo	Moderado	Alto
Remota	1	Muy bajo	Muy bajo	Bajo	Moderado	Alto

Figura 2: Mapa de calor análisis de riesgo inherente (Unidad de Riesgo Corporativo COOPEALIANZA R.L, 2015)

En esta etapa, se ha indicado que cada riesgo es analizado de acuerdo a probabilidad e impacto de forma tal que para cada riesgo se relacionen dichas variables y pueda ser graficado en el mapa de calor de riesgo inherente. A continuación se muestra en la figura 3 la tabla con las variables de probabilidad donde el rubro “Casi cierta” tiene una valor de 5, “Probable” un valor de 4,

“Posible” un valor de 3, “Poco probable” un valor de 2, “Remota” un valor de 1; por otra parte en la figura 4 se muestran las variables de impacto y su respectivo valor y descripción.

Probabilidad	Valor	Descripción
Casi cierta (1 al mes)	5	Casi certeza (inminente), se espera que ocurra un evento de esta naturaleza en la mayoría de las circunstancias. Se detectan situaciones que permiten estimar que este evento podría suceder al menos una vez en un período de un mes.
Probable (1 a 3 meses)	4	Es probable que ocurra un evento de esta naturaleza, en la mayoría de las circunstancias. Se detectan situaciones que permiten estimar que este evento podría suceder al menos una vez en un período de uno a tres meses.
Posible (3 a 5 meses)	3	El evento podría ocurrir en algún momento. Se detectan situaciones que permiten estimar que este evento podría suceder al menos una vez cada tres a cinco meses.
Poco probable (5 a 10 meses)	2	Es poco probable que el evento suceda pero podría ocurrir en algún momento. Se detectan situaciones que permiten estimar que este evento podría suceder al menos una vez en un período de cinco a diez meses.
Remota (1 al año)	1	Puede ocurrir solo en circunstancias excepcionales. Es muy poco probable que el evento se presente y no se detectan vulnerabilidades que aumenten su probabilidad de ocurrencia. En condiciones excepcionales se podría presentar un evento en el año.

Figura 3: Tabla de probabilidad del riesgo (Unidad de Riesgo Corporativo COOPEALIANZA R.L, 2015)

Impacto	Valor	Descripción
Crítico	5	Enorme pérdida financiera (más de ¢62.500.000) o afectación total al desempeño de los procesos. El evento causaría fallas, pérdidas o consecuencias inaceptables para el logro de los objetivos fundamentales. Efecto severo al servicio al cliente, pérdida de confianza (otras áreas del negocio, clientes, socios y el público en general). Puede provocar una masiva declinación del negocio.
Significativo	4	Alta pérdida financiera (¢27.500.001 a ¢62.500.000) o alto efecto al normal desempeño de los procesos. El evento causaría pérdidas severas o altos incrementos en costo y tiempo, que amenazan el alcance de objetivos intermedios. Afecta en forma significativa el servicio al cliente; áreas del negocio, clientes, socios y público. Pérdida de oportunidades o de clientes.
Moderado	3	Mediana pérdida financiera (¢10.000.001 a ¢27.500.000) o mediana afectación al normal desempeño de los procesos. El evento causaría pérdidas moderadas o incrementos en costo y tiempo, pero los objetivos importantes pueden aún lograrse. Impacto visible desde fuera del área (otras áreas, clientes o socios, público en general), pero no es significativo en el cliente externo o interno.
Bajo	2	Baja pérdida financiera (¢3.000.001 a ¢10.000.000) o efecto menor al normal desempeño de los procesos. El evento causaría pérdidas menores o incrementos bajos en costo y tiempo. Los requerimientos y objetivos pueden ser alcanzados
Insignificante	1	Mínima pérdida financiera (¢3.000.000 o menos) o mínima afectación al normal desempeño de los procesos. El evento no tendría efecto en la actividad ni sobre sus objetivos.

Figura 4: Tabla de impacto del riesgo (Unidad de Riesgo Corporativo COOPEALIANZA R.L, 2015)

Una vez efectuado el análisis de riesgo con base en los aspectos de probabilidad e impacto indicados en las figuras 3 y 4, se utiliza la matriz que se muestra en la figura 5 que permite determinar el nivel de cada riesgo.

NIVEL DE RIESGO	PUNTAJE DE CRITICIDAD	DESCRIPCIÓN
EXTREMO	5	Cuando su materialización puede afectar severamente el producto o servicio, se puedan perder oportunidades importantes de negocio o causar un daño grave a la imagen de la institución ante el público, socios o autoridades (incluyendo entes reguladores), así como verse afectada severamente su operatividad, de tal manera que se exponga a la entidad a pérdidas cuantiosas o sanciones legales y administrativas.
ALTO	4	Cuando la materialización puede afectar el producto o servicio, se puedan perder oportunidades de negocio y desmejorar la imagen de la institución, con lo cual podrían perderse clientes o verse afectada su operatividad en forma significativa.
MODERADO	3	Cuando su materialización represente un peligro potencial de impacto estrictamente a lo interno de la entidad; aunque no significativo para los clientes, socios o entes reguladores.
BAJO	2	Cuando su materialización acarrea consecuencias de baja importancia para la entidad
MUY BAJO	1	Cuando su materialización no acarrea consecuencias significativas para la entidad.

Figura 5: Niveles de riesgo (Unidad de Riesgo Corporativo COOPEALIANZA R.L, 2015)

Al obtenerse los resultados del análisis de probabilidad e impacto (riesgo inherente), se deben confrontar con el análisis de los controles que se determinen existen para cada riesgo; dicha evaluación se basa en una escala de valores que determina la capacidad de los mismos para la mitigación de los riesgos en cuanto a su calidad y frecuencia, esta escala se muestra en la figura 6.

Calidad	Puntaje	Descripción
Ínfima o Nula	5	Ausentes o inexistentes, pobres o de calidad muy cuestionable, mal definidos o diseñados. La falta de calidad aumenta en forma extraordinaria la probabilidad de materialización de un riesgo.
Baja, Insuficiente	4	No alcanzan un estándar aceptable por presentar muchas debilidades o deficiencias en diseño y documentación. Son informales o parciales, no se aplican en forma apropiada y no ofrecen garantía razonable para el logro de objetivos.
Media,Buena	3	Actividades de control diseñadas, documentadas y en aplicación. En general, los controles son buenos pero con algunas debilidades, que aunque no representan una exposición seria, se pueden mejorar en aras de una garantía más razonable sobre el logro de objetivos.
Alta,Confiable	2	Fuertes procesos de control, que operan apropiadamente, y ofrecen un nivel razonable de garantía. Además de ser estandarizados, cuentan con la supervisión por parte de los responsables o jefaturas.
Excelente	1	Procesos y actividades de control muy fuertes, operan apropiadamente, están supervisados por instancias superiores, con procedimientos y medidas conocidas por los involucrados y que pasan las pruebas periódicas de diseño y operación (eficientes).

Frecuencia	Puntaje	Descripción
Inexistente o Nula	4	Ausencia de controles. En ningún caso se aplican actividades de control, lo que implica total exposición al riesgo inherente.
Ocasional	3	Se aplica con poca frecuencia (semanal, mensual o sólo cuando alguien lo solicita). Con esta poca frecuencia, se incrementa la probabilidad de que se materialice el riesgo para el que fue diseñado.
Habitual	2	Aplicación diaria del control, o varias veces a la semana. No se aplica sobre cada transacción por lo que existe la posibilidad de que, en el intervalo de tiempo, se materialice el riesgo.
Permanente	1	El control se aplica sobre cada una de las transacciones durante el momento de su procesamiento. Puede ser en tiempo real o inmediatamente después, a través de registros o bitácoras de cada uno de los movimientos.

Figura 6: Escala de valoración de controles calidad y frecuencia (Unidad de Riesgo Corporativo COOPEALIANZA R.L, 2015)

Al considerar el efecto de los controles existentes y determinar la cobertura de riesgo, se procede a calcular el valor del riesgo residual para mostrarlo de igual manera en un mapa de calor que determina los niveles de riesgo residual.

2.2.2.4 Evaluación de riesgos

ISO 31000 indica que el propósito de la evaluación de riesgos es ayudar en la toma de decisiones, basada en los resultados de análisis de riesgos, sobre riesgos que necesitan tratamiento y la prioridad para la aplicación del tratamiento.

Evaluación de los riesgos que supone la comparación del nivel de riesgo identificado durante el proceso de análisis con criterios de riesgo establecidos cuando se considera el contexto. Basándose en esta comparación, la necesidad de que el tratamiento puede ser necesario. (International Organization for Standardization, 2009)

Para lograr un nivel de comparación, en esta etapa es importante que se haya definido el apetito al riesgo tal y como se indicó en el apartado anterior (Figura 2),

esto tiene como objetivo determinar los riesgos sobre los que se necesitan tratamiento y/o prioridades de tratamiento.

2.2.2.5 Tratamiento del riesgo

ISO 31000 indica que el tratamiento del riesgo consiste en seleccionar una o más opciones de modificación de los riesgos, y la aplicación de esas opciones.

Las opciones de tratamiento pueden incluir los siguientes: (International Organization for Standardization, 2009)

a. Evitar el riesgo al decidir no iniciar o continuar con la actividad que da lugar al riesgo.
b. Tomar o aumentar el riesgo con el fin de perseguir una oportunidad.
c. Eliminar la fuente de riesgo.
d. Los cambios en la probabilidad.
e. Cambiar las consecuencias.
f. La distribución del riesgo con la otra parte o partes (incluidos los contratos y la financiación de riesgo), y
g. Mantener el riesgo por decisión informada.

De acuerdo a la Metodología para la Gestión del Riesgo Operativo y TI en el Grupo Financiero Alianza, para el tratamiento de los riesgos, se podrá optar por algunos de los siguientes tipos de medidas:

a. **Evitar el riesgo**: significa salir de las actividades o de las condiciones que dan lugar a riesgo. Evitar riesgos se aplica cuando no hay otra respuesta adecuada. Este es el caso cuando:
    i. No hay ninguna otra respuesta rentable que puede tener éxito en la reducción de la frecuencia y de la magnitud por debajo de los umbrales definidos para el apetito del riesgo.

ii. El riesgo no puede ser compartido o transferido.
iii. El riesgo se juzga inaceptable por la administración.

Algunos ejemplos relacionados con la cobertura de riesgos de TI pueden incluir la reubicación de un centro de datos fuera de una región con importantes peligros naturales, o negarse a participar en un proyecto muy grande, cuando el caso de negocio muestra un notable riesgo de fracaso.

b. **Reducir el riesgo**: si el riesgo no puede ser evitado porque crea grandes dificultades operacionales, el siguiente paso es reducirlo al más bajo nivel posible. La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles. Se consigue mediante la optimización de los procedimientos y la implementación de controles.
c. **Transferir el riesgo**: hace referencia a buscar respaldo y compartir con otro (terceros) parte del riesgo, como por ejemplo tomar pólizas de seguros. Esta técnica es usada para eliminar el riesgo de un lugar y pasarlo a otro o de un grupo a otro. Así mismo, el riesgo puede ser minimizado compartiéndolo con otro grupo o dependencia. Los ejemplos incluyen tener un seguro para los incidentes relacionados con TI, la subcontratación de parte de las actividades de TI, o establecer un proyecto de riesgo de TI compartido con el proveedor a través de acuerdos de precios fijos o acuerdos de inversión compartida. Tanto en un sentido físico y jurídico estas técnicas no alivian una empresa de un riesgo, pero puede afectar la capacidad de la otra parte en la gestión del riesgo y reducir las consecuencias económicas si se produce un evento adverso.
d. **Asumir el riesgo**: asumir significa que no se tomen medidas relativas con un riesgo particular, y la pérdida es asumida cuando y si se produce. En algunos casos el riesgo se asume sin haberse reducido o transferido o después de evaluarlo y priorizarlo, se acepta la pérdida residual probable.

El proceso de gestión de riesgos al complementarse con otro tipo de análisis, tal como el análisis financiero, ofrece a las organizaciones de un importante sustento para la toma de decisiones, por ejemplo una organización podría estar en capacidad de realizar una importante inversión ya que el análisis financiero resulta atractivo o viable pero sin embargo al complementarlo con el proceso de gestión de riesgos eventualmente la empresa podría identificar algunos eventos de riesgo con altos costos de mitigación que a la postre no hubiesen sido identificados en el análisis financiero como tal; ahora bien en caso contrario un análisis financiero con resultado favorable y la aplicación del proceso de gestión de riesgo con riesgos razonablemente gestionados ofrece mayor tranquilidad y confianza a los distintos interesados de la organización.

2.3 Marco conceptual

Problema de investigación: ANALISIS FINANCIERO Y DE RIESGO AL TRASLADAR EL PROCESAMIENTO Y ALMACENAMIENTO DE LA INFORMACION CRITICA DE COOPEALIANZA R.L A UN CENTRO DE DATOS SUBCONTRATADO EN COSTA RICA				
Enfoque teórico	**Concepto central (Variable)**	**Subvariables**	**Indicadores (deben ser medibles)**	**Fuente de información**
Proyectos de Inversión formulación y Evaluación.	El análisis financiero son una serie de técnicas, herramientas y metodologías aplicadas a la evaluación, que conforman un elemento de control en la empresa (Salas, 2001)	- Construcción de Flujos de Caja. - Cálculo y análisis de la viabilidad económica.	- Flujo de Caja Proyecto Capital Propio. - Flujo de Caja Proyecto Outsourcing. - Informe de resultado análisis de la viabilidad económica.	Nassir Sapag Chain, Editorial Pearson Educación.
Norma ISO 31000:2009 Gestión de Riesgos – Principios y Guías.	El proceso de gestión de riesgos es la aplicación sistemática de politicas de gestión, procedimientos y prácticas para las actividades de comunicación, consultoría, se establece el contexto, y la identificación, análisis, evaluación, tratamiento,	- Establecer el contexto. - Identificación de riesgos. - Análisis de riesgos. - Evaluación de riesgos.	- Informe de evaluación de riesgo. - Mapa de calor riesgo inherente. - Mapa de calor riesgo residual. - Tratamiento del riesgo.	Organización Internacional de Normalización (ISO)

	seguimiento y la revisión del riesgo. (International Organization for Standardization, 2009)			

3 MARCO METODOLOGICO

3.1 Métodos de Investigación

Las condiciones del proyecto hacen que el método más adecuado para la investigación sea el método analítico - sintético. Este método consiste en la separación de las partes de un todo para estudiarlas en forma individual (Análisis), y la reunión racional de elementos dispersos para estudiarlos en su totalidad (Síntesis). (Muñoz Razo, 1998)

Es por lo tanto que una vez realizado el análisis financiero y de riesgo y obteniéndose los respectivos entregables producto de los mismos, todo se integra para emitir conclusiones y recomendaciones para que sean tomadas en cuenta por la administración de COOPEALIANZA R.L.

Obtención de datos.

Para la obtención de datos con el objetivo de realizar el análisis financiero al construir un nuevo centro de datos y para la modalidad de subcontratarlo, se obtendrán datos de proveedores sobre los principales costos de los componentes y/o servicios que formen parte según la modalidad.

Para la obtención de datos con el objetivo de realizar el análisis de riesgo al subcontratar un centro de datos a una empresa dedicada a este tipo de servicios, se estará realizando encuestas a un grupo interdisciplinario de COOPEALIANZA R.L a fin de obtener calificaciones de probabilidad, impacto y calidad de los

controles sobre los riesgos identificados Anexo 2 “Riesgos identificados Actividad Subcontratar el Centro de Datos” tanto para el riesgo inherente como para el riesgo residual, lo anterior se estará realizando de acuerdo a tablas de calificación del riesgo que se estarán incorporando en el desarrollo del estudio.

Procesamiento de la información.

Una vez recolectados los datos sobre los principales costos alrededor de construir un nuevo centro de datos y de subcontratarlo, dichos datos se estarán incorporando a la técnica financiera del flujo de caja para el proyecto con capital propio como para el flujo de caja para el proyecto de subcontratación del centro de datos; además se aplicará técnicas financieras como el valor actual neto (VAN) y la tasa interna de retorno (TIR) para obtener un resultado financiero que permita a la cooperativa tomar decisiones adecuadas con respecto a la gestión de los recursos.

Por otra parte y con respecto al análisis de riesgo, una vez realizadas las respectivas encuestas, los resultados de las mismas se estarán incorporando en un informe de evaluación del riesgo y mostrándose además en un mapa de calor de riesgo inherente y de riesgo residual.

Interpretación de los datos.

Una vez realizado el flujo de caja para ambas modalidades, construir y subcontratar un centro de datos, y haberse aplicado las técnicas del VAN y el TIR; se obtendrán resultados financieros que van a permitir a la cooperativa contar con un cálculo y análisis de la viabilidad económica para ambas modalidades.

Con respecto al análisis de riesgo, se podrá interpretar por medio del informe de evaluación del riesgo y el mapa de calor de riesgo inherente y de riesgo residual, los niveles de exposición de COOPEALIANZA R.L que se obtienen al subcontratar

un centro de datos a una empresa dedicada a este tipo de servicios, lográndose observar además como los controles actuales minimizan los riesgos y además permitiendo identificar en cuales riesgos se requiere mejorar la efectividad del control o bien complementar con otros controles.

3.2 Fuentes de información

Fuentes Primarias

La fuente primaria para la realización de este trabajo considera el criterio experto de funcionarios de COOPEALIANZA R.L, para el análisis financiero se estará considerando el aporte de la Gerencia Financiera y para el análisis de riesgo se considera el criterio experto de la Unidad de Riesgo Corporativo, así como el criterio experto de los funcionarios de COOPEALIANZA R.L interesados en las decisiones alrededor del futuro centro de datos (Seguridad de la Información, Continuidad de Operaciones, Control Interno, Auditoria Interna y Tecnologías de Información) Dicha información se obtendrá a través de observación directa y la encuesta.

Para la elaboración de la encuesta se tomará en cuenta las recomendaciones emitidas por la Unidad de Riesgo Corporativo de COOPEALIANZA R.L; dichas encuestas tienen como objetivo evaluar la probabilidad/impacto de los riesgos identificados y la efectividad de los controles propuestos para el tratamiento del riesgo, todo lo anterior para el análisis de riesgo. En el Anexo 3 “Encuesta Evaluar Probabilidad e Impacto del Riesgo” se muestra el formato utilizado para obtener datos de los encuestados.

Las técnicas de campo son aquellas que nos permiten entrar en contacto directo con el objeto de estudio y recoger la información de las fuentes primarias. Algunas de las herramientas más usuales son las propias de la investigación de campo: observación, entrevista, encuesta y cuestionario. (Ramírez, 2011)

Para la realización de este trabajo se estará considerando las siguientes técnicas:

Observación Directa: es la inspección que se hace directamente a un fenómeno dentro del medio en que se presenta, a fin de contemplar todos los aspectos inherentes a su comportamiento y características dentro de ese campo. En estos casos el observador entra en contacto directo con el fenómeno observado, pudiendo permanecer aislado del mismo o participar en él. (Muñoz Razo, 1998)

Encuesta: es la recopilación de datos concretos, dentro de un tópico de opinión específico, mediante el uso de cuestionarios o entrevistas, con preguntas y respuestas precisas que permiten hacer una rápida tabulación y análisis de esa información. (Muñoz Razo, 1998)

Fuentes Secundarias

Como fuente de información secundaria se utilizará datos e información proporcionada por empresas proveedoras de componentes de centros de datos lo anterior con el objetivo de obtener costos iniciales y de mantenimiento de los principales componentes de los centros de datos. Además se estará considerando la consulta a información documental de sitios de Internet, libros, tesis y revistas; tanto para reforzar el análisis financiero con la aplicación de técnicas e instrumentos financieros así como para la realización del análisis de riesgo.

El resumen de las fuentes de información e instrumentos (herramientas) que se utilizarán en este proyecto se presenta en el Cuadro 1:

Cuadro 1 Fuentes de Información Utilizadas

Objetivos	Fuentes de información		Instrumentos
	Primarias	Secundarias	
Elaborar un análisis financiero del costo inicial y de mantenimiento anual estimado de construir un nuevo centro de datos para COOPEALIANZA R.L que soporte el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L para los próximos 10 años para que pueda ser comparado con los costos de un centro de datos subcontratado.	Criterio experto de la Gerencia Financiera de COOPEALIANZA R.L.	Consulta a datos e información proporcionada por empresas proveedoras de componentes de centros de datos y consulta de información documental de libros.	Observación Directa
Desarrollar un análisis financiero de los costos anuales de arrendamiento y servicios complementarios de centros de datos subcontratados para soportar el procesamiento y almacenamiento de la información crítica de	Criterio experto de la Gerencia Financiera de COOPEALIANZA R.L.	Consulta a datos e información proporcionada por empresas proveedoras de servicios de centros de datos y consulta de información documental de libros.	Observación Directa

Objetivos	Fuentes de información		Instrumentos
COOPEALIANZA R.L para los próximos 10 años para que pueda ser comparado con los costos de un centro de datos propio.			
Ejecutar el proceso de gestión de riesgos de acuerdo al marco ISO 31000 a la actividad de trasladar el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica para que la alta administración entienda, comprenda y gestione los riesgos de dicha actividad.	Criterio experto de personal clave de COOPEALIANZA R.L y la Unidad de Riesgos Corporativa de COOPEALIANZA R.L	Consulta a información documental sitios de Internet, tesis y revistas.	Observación Directa y Encuesta

3.3 Alcances y limitaciones

Los alcances y limitaciones y su relación con los objetivos del proyecto final de graduación se ilustran en el cuadro 4, a continuación.

Cuadro 2 Alcances y limitaciones

Objetivos	Alcances	Limitaciones
Elaborar un análisis financiero del costo inicial y de mantenimiento anual estimado de construir un nuevo centro de datos para COOPEALIANZA R.L que soporte el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L para los próximos 10 años para que pueda ser comparado con los costos de un centro de datos subcontratado.	El análisis financiero incluirá los costos iniciales y de mantenimiento más representativo al construir un nuevo centro de datos; entre estos están metros cuadrados de construcción, diseño e implementación eléctrica, sistemas de respaldo eléctrico, sistema de enfriamiento, gabinetes para equipos, sistema de prevención temprana de incendio	El análisis financiero no incluye costos iniciales y de mantenimiento para el equipamiento del centro de datos, es decir servidores, almacenamiento, equipo de comunicación, por mencionar algunos. Además podría ocurrir que los costos enviados por los proveedores para la realización de este trabajo no muestren descuentos importantes ya que no se trata de una compra inmediata donde se puede obtener un descuento relevante, sino más bien de una estimación de costos.
Desarrollar un análisis financiero de los costos anuales de arrendamiento y servicios complementarios de centros de datos subcontratados para soportar el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L para	Este análisis financiero incluirá los costos anuales de arrendamiento y servicios	Este análisis financiero no incluye costos de equipamiento del centro de datos, es decir servidores,

Objetivos	Alcances	Limitaciones
los próximos 10 años para que pueda ser comparado con los costos de un centro de datos propio.	complementarios estrictamente necesarios para poner en operación un centro de datos, es decir el alquiler de gabinetes para los equipos, suministro de energía eléctrica, respaldo eléctrico, sistema de enfriamiento, vigilancia, sistema de prevención temprana de incendio.	almacenamiento, equipo de comunicación, por mencionar algunos. Además podría ocurrir que los costos enviados por los proveedores para la realización de este trabajo no muestren descuentos importantes ya que no se trata de una compra inmediata donde se puede obtener un descuento relevante, sino más bien de una estimación de costos.
Ejecutar el proceso de gestión de riesgos de acuerdo al marco ISO 31000 a la actividad de trasladar el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica para que la alta administración entienda, comprenda y gestione los riesgos de dicha actividad.	El proceso de gestión de riesgos de acuerdo al marco ISO 31000 que tiene como alcance este trabajo incorpora: -Establecer el contexto. -Identificación de riesgos. -Análisis de riesgos. - Evaluación de	El entregable “Tratamiento del riesgo” va a ofrecer una propuesta de controles para los riesgos identificados y que minimicen en un rango aceptable por COOPEALIANZA R.L cualquier impacto negativo, para efectos de este trabajo dichos controles no serán evaluados ni implementados.

Objetivos	Alcances	Limitaciones
	riesgos.	

3.4 Entregables

Los entregables y su relación con los objetivos del proyecto se ilustran en el cuadro 5, a continuación.

Cuadro 3 Entregables

Objetivos	Entregables
Elaborar un análisis financiero del costo inicial y de mantenimiento anual estimado de construir un nuevo centro de datos para COOPEALIANZA R.L que soporte el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L para los próximos 10 años para que pueda ser comparado con los costos de un centro de datos subcontratado.	- Flujo de Caja Proyecto Capital Propio. - Informe de resultado análisis de la viabilidad económica.
Desarrollar un análisis financiero de los costos anuales de arrendamiento y servicios complementarios de centros de datos subcontratados para soportar el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L para los próximos 10 años para que pueda ser comparado con los costos de un centro de datos propio.	- Flujo de Caja Proyecto *Outsourcing*. - Informe de resultado análisis de la viabilidad económica.
Ejecutar el proceso de gestión de riesgos de	- Informe de evaluación de riesgo.

acuerdo al marco ISO 31000 a la actividad de trasladar el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica para que la alta administración entienda, comprenda y gestione los riesgos de dicha actividad.	- Mapa de calor riesgo inherente. - Mapa de calor riesgo residual. - Tratamiento del riesgo (Propuesta de Controles)

4 DESARROLLO

4.1 Análisis Financiero

Para el siguiente análisis financiero se considera dos escenarios; el primer escenario toma en cuenta que la cooperativa invierta en un nuevo centro de datos en el cantón de Pérez Zeledón, tal y como lo hizo en el año 2006; y el segundo escenario considera que la cooperativa subcontrate el centro de datos en Costa Rica a una empresa especializada en este tipo de servicio.

Para ambos casos se hace necesario identificar e incorporar todos los desembolsos previos de ambas alternativas, lo que se denomina en un flujo de caja el momento cero. Posterior al momento cero se debe identificar e incorporar todos los movimientos ya sean estos costos y/o beneficios en el periodo de tiempo. Para ambas alternativas se va a considerar un periodo de tiempo de 5 años posterior al momento cero.

Al momento de iniciar un proyecto de construir un nuevo centro de datos, es importante identificar los aspectos, componentes y/o recursos estrictamente necesarios. Para lo anterior podemos considerar algunas definiciones de centros de datos que realizaron otros autores:

- “Un *data center* es aquella ubicación donde se concentran todos los recursos necesarios para el procesamiento de información de una organización. Un *data center* viene a ser básicamente un edificio o sala de gran tamaño usada para mantener en él una gran cantidad de equipamiento electrónico (servidores, sistemas de almacenamiento de datos, equipos de comunicaciones, etc). Son creados y mantenidos por las organizaciones con el objetivo de tener acceso a la información necesaria para sus operaciones.” (González, 2010)

- “Un centro de datos o “*Data Center*” en su traducción al inglés, es el espacio físico destinado para el alojamiento de cierta cantidad de servidores, los cuales están destinados al tráfico y procesamiento de datos. Este mismo aloja todas las facilidades y estructura necesaria para su óptimo funcionamiento. Esta misma infraestructura con sus facilidades, dependerá en complejidad del mercado meta y los requerimientos de la empresa o cliente al cual pertenece el centro de datos. “ (Astúa Chavarría, 2010)
- “Un *Data Center* es un área centralizada para el almacenamiento, manejo y distribución de los datos e información organizada alrededor de un área de conocimiento o un negocio particular.” (ANSI/TIA-942, 2005)

Con respecto a la última definición, podemos agregar además que tanto ANSI (*American National Standards Institute*) como TIA (*Telecomunications Industry Association*) han definido en el estándar TIA-942 que la infraestructura de soporte para un centro de datos debe estar compuesto por cuatro subsistemas, los cuales se indican a continuación:

- Telecomunicaciones
- Arquitectura
- Sistema eléctrico
- Sistema mecánico

Los cuatro subsistemas indicados anteriormente, a su vez incorporan ciertos componentes relevantes para un centro de datos tal y como se muestra en el cuadro 4. (ANSI/TIA-942, 2005)

Cuadro 4 Subsistemas de un centro de datos según ANSI/TIA-942

Telecomunicaciones	Arquitectura	Sistema eléctrico	Sistema mecánico
Cableado de racks / gabinetes, cableado horizontal, paneles de conexión (*patch panels*)	Protección ignifuga	Puesta a tierra	Sistema de climatización
Accesos redundantes del ISP (Enlaces de comunicación / Internet)	Barreras de vapor en el entechado	Generadores eléctricos	Sistema de detección de incendio
	Techos y pisos	UPS	Extinción por agente limpio
	Sala de UPS	Sistema pararrayos	Detección de líquidos
	Control de acceso	Supresores de transientes (minimiza los fallos de componentes, reinicios de sistemas, corrupción de datos)	Rociadores ante incendios
	CCTV		Cañerías, drenajes, condensadores

De acuerdo a los subsistemas indicados por ANSI (*American National Standards Institute*) así como por TIA (*Telecomunications Industry Association*) en el estándar TIA-942 y considerando la experiencia de la cooperativa en el año 2006 en cuanto a construir un centro de datos, podemos detallar ciertos componentes relevantes y sus costos estimados para que sirvan de insumo para preparar el flujo

de caja correspondiente al construir un nuevo centro de datos. A continuación por medio de la construcción de un flujo de caja, se enlistan los principales costos para el momento cero y para el escenario de invertir en un nuevo centro de datos en el cantón de Pérez Zeledón.

4.1.1 Construcción de un nuevo centro de datos

4.1.1.1 Flujo de caja

En el cuadro 5 se muestran los montos requeridos como inversión inicial y los costos de operación necesarios para brindar los servicios de un nuevo centro de datos para COOPEALIANZA R.L. Los datos fueron proporcionados por las áreas de Recursos Humanos, Proveeduría Corporativa, Seguridad Corporativa y Servicios Generales de COOPEALIANZA R.L, es importante recalcar que para las categorías Arquitectura, Telecomunicaciones, Sistema Mecánico y Sistema Eléctrico, dichos costos no poseen los eventuales descuentos que se realizan al momento de una compra definitiva por parte de la cooperativa.

Cuadro 5 Flujo de caja en dólares construcción de un centro de datos

Categorías	Año 0	Año 1	Año 2	Año 3	Año 4	Año 5	Total /
Arquitectura	111,833	600	600	600	600	3,748	117,981
Telecomunicaciones	43,500	0	0	0	0	0	43,500
Sistema Mecánico	71,860	17,600	18,050	18,523	19,019	19,540	164,591
Sistema Eléctrico	144,000	18,600	19,530	31,507	21,532	22,608	257,777
Servicios Públicos	0	37,900	41,672	45,820	50,381	55,396	231,169
Personal de Soporte y Seguridad	0	100,667	105,700	110,985	116,534	122,361	556,247
Costo Total	**371,193**	**175,367**	**185,552**	**207,434**	**208,065**	**223,653**	**1,371,264**

Según el cuadro anterior, la inversión inicial o momento cero requerido para poner en funcionamiento el proyecto asciende a $371,193, siendo las principales categorías el sistema eléctrico y el de arquitectura, representando un 68.92%. (Financiero, 2015)

Por otra parte, tenemos los costos de operación para el periodo de tiempo del año 1 y hasta el año 5, podemos observar que el rubro más representativo es la

categoría de personal de soporte y seguridad, que representa en promedio durante los cinco años el 79.6% de los costos totales de operación. Estos costos crecen a una tasa promedio del 6.30%, como consecuencia que muchos de estos están condicionados a incrementos inflacionarios (contratos y personal).

4.1.1.2 Ingresos y/o beneficios esperados

Considerando que por el tipo de inversión (construir un centro de datos), no existe un ingreso o beneficio directo que se pueda asociar al proyecto, fue necesario construir un modelo que permita asociar un monto de beneficios de tener un centro de datos considerando el aspecto de alta disponibilidad de los servicios financieros que soporta, para esto se contó con el apoyo de la Gerencia Financiera de COOPEALIANZA R.L.

Debemos entender que COOPEALIANZA R.L. como entidad financiera que brinda servicios en modalidad las veinticuatro horas del día, los siete días de la semana y los trescientos sesenta y cinco días del año, debe procurar mantener el mayor porcentaje de disponibilidad posible, pues cuanto esto tendría un efecto directo sobre la generación de ingresos, costos adicionales por recuperación de las operaciones y costos de oportunidad incuantificables por la pérdida de confianza y afectación de la imagen corporativa.

Ahora bien, para la construcción del modelo se determinó en primera instancia el monto del ingreso anual de COOPEALIANZA R.L. para el año 2015 en forma anualizada, este monto ascendió a ₡45,427,909,091, luego se calculó la tasa de crecimiento promedio para los últimos cuatro años (18.94%).

Posteriormente, utilizando como base los ingresos del año 2015 y la tasa de crecimiento promedio de los ingresos anuales, se proyectaron los ingresos para los cinco años siguientes; asimismo, se calculó el ingreso diario, pues resultará necesario para posteriormente calcular los ingresos o beneficios del proyecto.

Cuadro 6 Ingresos anuales, diarios y beneficios esperados durante el periodo del proyecto

	Año 2015	Año 1	Año 2	Año 3	Año 4	Año 5
Ingreso anual	45,427,909,091	54,030,785,304	64,262,824,748	76,432,548,987	90,906,905,628	108,122,332,701
Ingreso diario	124,460,025	148,029,549	176,062,534	209,404,244	249,060,015	296,225,569
Contribución a los ingresos	226,517,245	269,413,779	320,433,811	381,115,724	453,289,228	539,130,536

Para determinar la contribución del proyecto a los ingresos anuales de COOPEALIANZA R.L., se comparó la meta de disponibilidad (99.50%) establecida en el Plan Estratégico de Tecnologías de Información para el período 2015-2017 versus la disponibilidad real alcanzada (99.99%) al mes de noviembre 2015 proporcionada por el área de Administración de Base de Datos de la cooperativa, lográndose una eficiencia de 0.49% en términos relativos, equivalente a 1.82 días. Por lo tanto, este factor se multiplica por el ingreso diario y se obtiene la contribución a los ingresos tal y como se muestra en la moneda colones en el cuadro 6. (Financiero, 2015)

4.1.1.3 Cálculo y análisis de la viabilidad económica

Para determinar la factibilidad financiera del proyecto se utilizaron los criterios que se muestran en el cuadro 7. (Financiero, 2015)

Cuadro 7 Criterios para el cálculo y análisis de la viabilidad económica

Valor actual neto (VAN)	Se utilizó como criterio que debería ser superior al 25% de la inversión inicial ($92,798), según criterio aplicado por COOPEALIANZA R.L.
Tasa interna de retorno (TIR)	Para valorar el dato de la TIR se comparará contra la tasa de Costo Medio Ponderado de Capital (wacc), que también será utilizada como factor de descuento y de conformidad con la metodología interna aplicada por COOPEALIANZA R.L., dicha tasa es de 10.88%.

Valor Actual Neto (VAN)

En el cuadro 8 se muestra la inversión inicial; así como los flujos de costos, beneficios, el flujo de caja acumulativo y descontado, correspondientes a los cinco

años del proyecto, este último utilizando la tasa promedio de capital. (Financiero, 2015)

Cuadro 8 Cálculo del valor actual neto de la construcción de un centro de datos

Periodos	Costos	Beneficios	Flujo de caja acumulativo	Factor de descuento	Flujo de caja descontado
0	(371,193)	0	(371,193)	1,00	(371,193)
1	(175,367)	498,914	323,548	0,90	291,800
2	(185,552)	593,396	407,844	0,81	331,732
3	(207,434)	705,770	498,336	0,73	365,563
4	(208,065)	839,424	631,359	0,66	417,699
5	(223,653)	998,390	774,737	0,60	462,262
Valor Actual Neto	**$ (1,103,544)**	**$2,601,407**	**$1,497,863**		**$1,497,863**

Debemos recordar que todo VAN mayor a cero, en principio resulta viable; pero en este caso particular, se estresa aún más el proyecto y COOPEALIANZA R.L. establece que debería ser mayor al 25% de la inversión inicial ($92,798.25), monto que es superado ampliamente pues el VAN del proyecto alcanzó $1,497,863.

Tasa Interna de Retorno

Al calcular la tasa interna de retorno sobre la columna de flujo de caja acumulativo, mostrado en el Cuadro 8 y utilizando la fórmula de la Hoja de Cálculo Microsoft Excel, se obtiene que la misma asciende a 104.75%, superando ampliamente el factor Costo Medio Ponderado de Capital determinado por COOPEALIANZA R.L. del 10.88%.

4.1.2 Subcontratar el centro de datos

4.1.2.1 Flujo de caja

Seguidamente se muestra en el cuadro 9 el monto requerido como inversión inicial y los costos de operación necesarios para contratar los servicios de un centro de datos. (Financiero, 2015)

Cuadro 9 Costo total de subcontratar el centro de datos

Categorías	Año 0	Año 1	Año 2	Año 3	Año 4	Año 5	Total /
Arquitectura	0	72,000	75,600	79,380	83,349	87,516	397,845
Telecomunicaciones	0	102,000	107,100	112,455	118,078	123,982	563,614
Sistemas Mecánico	0	0	0	0	0	0	0
Sistema Eléctrico	0	0	0	0	0	0	0
Servicios Públicos	0	0	0	0	0	0	0
Personal de Soporte y Seguridad	0	6,000	6,300	6,615	6,946	7,293	33,154
Costo Total de Propiedad /	**0**	**$180,000**	**$189,000**	**$198,450**	**$208,373**	**$218,791**	**$994,614**

Inversión inicial: En esta alternativa por la naturaleza del proyecto no existe inversión inicial, lo que limita su valoración únicamente a través del VAN.

Costos de operación: El principal costo de operación de esta alternativa resulta en la categoría de Telecomunicaciones, representando casi el 57% de los costos totales de operación y seguido de los costos de arquitectura con un 40%, que corresponde al alquiler inicial de dos gabinetes para alojar equipamiento de procesamiento y almacenamiento propiedad de la cooperativa. Los costos de dos gabinetes con un consumo de 2Kw de potencia fueron proporcionados por la Proveeduría Corporativa de COOPEALIANZA R.L y corresponden al promedio del costo por gabinete de tres centros de datos en Costa Rica categoría certificada TIER III. Los costos de personal de soporte y seguridad corresponde al servicio de manos remotas en caso que el personal de Tecnologías de Información de la cooperativa requiera ejecutar alguna acción de revisión visual o por ejemplo cambio de cinta de respaldo en el sitio sin la necesidad de trasladarse al centro de datos, en este caso se haría por medio de personal asignado y entrenado para tal fin en el centro de datos contratado.

4.1.2.2 Ingresos y/o beneficios esperados

En lo que respecta a los ingresos esperados de la inversión, se utilizarán los mismos determinados en la alternativa de construcción de un centro de datos, según el cuadro 6.

4.1.2.3 Cálculo y análisis de la viabilidad económica

Para determinar la factibilidad financiera del proyecto se utiliza el valor actual neto, con el criterio que deberá ser superior a cero, utilizando como factor de descuento el Costo Medio Ponderado de Capital (wacc), que es de un 10.88%. En el cuadro 10, se muestra la inversión inicial; así como los flujos de costos, beneficios, el flujo de caja acumulativo y descontado, correspondientes a cinco años del proyecto, este último utilizando la tasa promedio de capital. (Financiero, 2015)

Cuadro 10 Cálculo del valor actual neto de subcontratar el centro de datos

Periodos	Costos	Beneficios	Flujo de caja acumulativo	Factor de descuento	Flujo de caja descontado
0	0	0	0	1,00	0
1	(180,000)	498,914	318,914	0,90	287,621
2	(189,000)	593,396	404,396	0,81	328,928
3	(198,450)	705,770	507,320	0,73	372,154
4	(208,373)	839,424	631,052	0,66	417,496
5	(218,791)	998,390	779,599	0,60	465,163
Valor Actual Neto	**$ (730,046)**	**$2,601,407**	**$1,871,361**		**$1,871,361**

En este caso el VAN debe ser mayor a cero, situación que se cumple ampliamente, pues el mismo alcanzó $1,871,361.

4.1.3 Comparación de alternativas

Considerando que el único criterio disponible en la evaluación financiera de ambas alternativas es el VAN, seguidamente en el cuadro 11 se realiza un comparativo de los flujos de efectivo descontados. (Financiero, 2015)

Cuadro 11 Comparativo de alternativas mediante flujos de efectivo descontados

Periodos	Construcción de un centro de datos	Subcontratación de un centro de datos	Diferencia
0	(371,193)	0	- 371,193.00
1	291,800	287,621	4,178.00
2	331,732	328,928	2,805.00
3	365,563	372,154	-6,590.00
4	417,699	417,496	203.00
5	462,262	465,163	-2,902.00
Valor Actual Neto	**$1,497,863**	**$1,871,361**	- 373,499.00

Del cuadro anterior, es evidente que financieramente resulta mejor la subcontratación de un centro de datos, pues evita incurrir en todos los costos asociados a la inversión inicial, que asciende a $371,193. Además, al comparar los flujos de operación (años 1-5) se genera también un ahorro adicional de $2,306, para un total de $373,499.

Adicionalmente, es importante indicar que la opción de subcontratación evita generar inversión en activos por la suma de ₡200,444,220 (tipo de cambio utilizado 540 ₡/$) y por lo tanto, un incremento en el requerimiento de patrimonio por la suma de ₡32,071,075.2 o en su defecto una afectación del indicador de suficiencia patrimonial de 0.02%, según sensibilización realizada por la Gerencia Financiera de COOPEALIANZA R.L.

4.2 Gestión de riesgos a subcontratar el nuevo centro de datos de COOPEALIANZA R.L

4.2.1 Establecer el contexto

Como parte del proceso de gestión de riesgos y antes de iniciar con una etapa de identificación de riesgos, se hace necesario comprender el contexto externo e interno de trasladar el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica. Es por lo anterior que a continuación se abordan aspectos relevantes del contexto externo e interno y que favorece el involucramiento y participación de los distintos involucrados de la cooperativa en las siguientes etapas del proceso de gestión de riesgo.

4.2.1.1 Contexto externo

El contexto externo puede abordarse para este estudio bajo dos aspectos relevantes: la regulación en materia de gestión de la Tecnología de Información por parte de la SUGEF hacia la cooperativa y la oferta de servicios por parte de

terceros que tiene a la fecha de este estudio la cooperativa con respecto a centros de datos sub contratados en Costa Rica.

Como es conocido, en Costa Rica las entidades financieras supervisadas por la SUGEF deben acatar el reglamento SUGEF 14-09 “Reglamento sobre la Gestión de la Tecnología de Información”, dicho reglamento basado en COBIT 4 indica como parte de sus áreas de enfoque del Gobierno de TI la “Administración de Riesgos” donde COBIT lo describe así “La administración de riesgos requiere conciencia de los riesgos por parte de los altos ejecutivos de la empresa, un claro entendimiento del apetito de riesgo que tiene la empresa, comprender los requerimientos de cumplimiento, transparencia de los riesgos significativos para la empresa, y la inclusión de la responsabilidades de administración de riesgos dentro de la organización”, la cooperativa por lo anterior y de manera responsable debe sustentar cualquier decisión entregando los insumos necesarios a la alta administración para que exista la debida transparencia y comprensión de los riesgos que se están administrando, ya sea minimizándolos, trasladándolos, aceptándolos o evitándolos.

Con respecto a la oferta de servicios en materia de subcontratación de centros de datos que tiene a la fecha de este estudio la cooperativa y de acuerdo al artículo titulado “Costa Rica mantiene el segundo lugar en *data centers* en Latinoamérica” de la revista *IT NOW* del mes de julio 2015 se indica lo siguiente “El aumento en centros de datos certificados en Costa Rica, construidos bajo estándares de alto nivel que garantizan un mínimo de caídas al año ha permitido la consolidación de una infraestructura tecnológica de alto nivel. Según el estudio de la entidad certificadora *Uptime Institute*, el país se encuentra en el segundo lugar en centros de almacenamiento de datos y edificaciones certificadas en Latinoamérica, por debajo nada más de Brasil.” (Agüero, 2015)

Según lo anterior se identifica una importante inversión de empresas en el territorio costarricense enfocado a servicios para organizaciones que requieren de

procesamiento y almacenamiento de información bajo altos estándares de seguridad y de acuerdo a buenas prácticas de la industria con respecto a centros de datos. Lo anterior permite a las organizaciones trasladar riesgos con respecto al resguardo y procesamiento de información dejando que un tercero gestione y controle aspectos tales como espacio físico requerido, seguridad física, acondicionamiento ambiental, suministro y respaldo eléctrico.

Otro aspecto relevante es las posibilidades de inversión y características que posee Costa Rica para consolidarse como un país atractivo para la construcción de centros de datos, con respecto a esto el periódico El Financiero indica lo siguiente “Alexander Monestel, de Data Center Consultores, explicó que Costa Rica tiene todo el potencial en ser un hub de tecnología ya que ha sido un modelo de países exitosos en atraer inversión extranjera directa. "El Foro Económico mundial dice que aquellos países que tengan como eje estratégico el manejo de datos y *data center* serán los más prósperos", afirmó Monestel.” (Chacón, 2015)

Esta misma fuente además indica “Los expertos consideran que Costa Rica puede convertirse en líder en la región porque posee reservas y parques nacionales, biodiversidad, ocupa el tercer puesto a nivel mundial en las países más verdes y el 93% de producción de las energías son renovables” (Chacón, 2015)

De acuerdo a un artículo de El Financiero, Costa Rica es el segundo país de América Latina –después de Brasil y superando incluso a mercados como México– por la cantidad de centros de datos certificados (14) por el *Uptime Institute*, la entidad internacional constituida como autoridad en la materia. (Cordero, 2015)

4.2.1.2 Contexto interno

Como parte de la planificación estratégica de Tecnologías de Información de COOPEALIANZA R.L para el año 2015 – 2017 se estableció la siguiente estrategia “Crecer responsablemente en la contratación de servicios de terceros;

otorgando tareas operativas especializadas a empresas de reconocida trayectoria, enfocando al personal de TI en las metas crucialmente importantes, generando altos niveles de disponibilidad, seguridad, desempeño y calidad en los servicios tecnológicos que se entregan, todo lo anterior alineado a las creencias de COOPEALIANZA R.L".

Para contribuir con la estrategia anterior se complementó con el establecimiento de los siguientes objetivos estratégicos:

- Mantener que entre un 70% y 80% de las tareas operativas especializadas estén soportadas por un contrato formal con empresas de trayectoria en servicios tecnológicos al cierre de cada año.

El objetivo estratégico anterior contribuye con el traslado de tareas operativas especializadas hacia la subcontratación de empresas de trayectoria en servicios tecnológicos; lo anterior además contribuye a que la estructura de Tecnología de Información de COOPEALIANZA realice cada vez menos tareas operativas y se enfoque más a generar valor y enfoque al negocio principal de la cooperativa.

Es importante resaltar que el enfoque estratégico anterior, conlleva reforzar lo hecho hasta la fecha en lo que se refiere a la administración de los servicios de terceros; el mismo ente supervisor SUGEF indica en el Reglamento Sobre la Gestión de la Tecnología de Información, publicado en el diario oficial La Gaceta N° 50 del jueves 12 de marzo del 2009 y modificado por el Consejo Nacional de Supervisión del Sistema Financiero, mediante Artículo 5 del Acta de la Sesión 853-2010, celebrada el 21 de mayo del 2010 con publicación en el diario oficial "La Gaceta" Nº 115 del 15 de junio del 2010 en su CAPÍTULO II GESTIÓN DE LA TECNOLOGÍA DE INFORMACIÓN, Artículo 6. Marco para la Gestión de TI, entre otras cosas lo siguiente: "La entidad que contrate parte o la totalidad de sus procesos a proveedores locales o extranjeros de tecnologías de información deben incluir obligatoriamente el proceso DS2 "Administrar los servicios de

terceros” dentro de su marco para la gestión de TI”. Lo anterior conlleva reforzar los controles existentes y evaluar riesgos de acuerdo al proceso COBIT anterior.

Por otra parte otro riesgo de la estrategia anterior, es que el ente supervisor cambie el modelo de calificación de TI, por un modelo donde también se califique a los proveedores críticos de TI y que dicha calificación sea parte de la calificación de la entidad, sin duda esto tendrá como consecuencia que eventualmente se deba seguir invirtiendo en reforzar las capacidades y competencias del recurso humano de TI a nivel interno, para balancear un poco las dependencias que puedan originarse con los terceros.

El otro objetivo estratégico relevante para este estudio desde el punto de vista del contexto interno, es el siguiente:

- Lograr que el 100% de las aplicaciones Core se encuentren soportadas por soluciones de centro de datos subcontratados al cierre del año 2017.

El objetivo anterior busca contribuir con la cooperativa en reducir costos al construir un nuevo centro de datos y de los costos totales de propiedad al mantenerlo; sin embargo al incursionar en un proyecto de este tipo se hace necesario complementar cualquier análisis financiero con el tema de riesgo, a fin que la cooperativa pueda comprender, reducir, trasladar, aceptar o evitar cualquier evento o circunstancia alrededor del cumplimiento de dicho objetivo.

El objetivo anterior sin duda debe estar respaldado por un análisis de riesgos con el objetivo que la alta administración entienda y conozca los riesgos de procesar la información crítica de la cooperativa con un tercero, comprendiendo aspectos como que la responsabilidad de la disponibilidad, integridad y confidencialidad de la información sensible de la cooperativa estará en infraestructura crítica de una empresa que se dedica a este tipo de servicio, contra los beneficios de mejorar la eficiencia en la gestión de TI, mejorar la gestión de los recursos y la inversión en materia de tecnología y que el personal de TI no se desenfoque en actividades

operativas direccionadas a mantener en funcionamiento un centro de datos; y más bien apoye en mayor porcentaje de su tiempo a generar valor y eficiencia al negocio propio de COOPEALIANZA R.L.

Posterior a la comprensión del contexto externo e interno de la cooperativa alrededor de trasladar el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica, se continúa con la etapa de identificación de riesgos como parte también relevante del proceso de gestión del riesgo.

4.2.2 Identificación de riesgos

Para esta etapa se hizo necesario involucrar personal de la cooperativa con amplio conocimiento y experiencia y que de una u otra manera se verán involucrados en dicho proceso, los participantes incluyeron las siguientes áreas de la cooperativa: Auditoría Interna, Control Interno, Unidad de Riesgos Corporativo, Seguridad de la Información, Continuidad de Operaciones, Unidad Legal, Servicios Generales, Oficina de Proyectos y Tecnologías de Información. La obtención de datos a los participantes fue realizada por medio de sesiones de trabajo y la realización de encuestas.

Por otra parte y para realizar una adecuada identificación de riesgos de acuerdo al contexto externo e interno identificado y que a su vez permita categorizar dichos riesgos con respecto a procesos reconocidos de control y gestión de Tecnologías de Información, se considera el marco de referencia COBIT 4.1. Lo anterior da como resultado que los riesgos identificados están debidamente distribuidos en 9 procesos COBIT. Seguidamente el cuadro 12 muestra los dominios y procesos de acuerdo a la identificación que propone COBIT.

Cuadro 12 Procesos COBIT

COBIT		Descripción
Dominio	Proceso	
Adquirir e implementar	AI3	Adquirir y mantener la infraestructura tecnológica
	AI6	Administrar cambios
Entrega y soporte	DS2	Administrar servicios de terceros
	DS4	Garantizar la continuidad del servicio
	DS5	Garantizar la seguridad de los sistemas
	DS9	Administrar la configuración
	DS10	Administrar los problemas
	DS12	Administrar el ambiente físico
Monitorear y evaluar	ME3	Monitorear y evaluar el control interno

(Unidad de Riesgo Corporativo COOPEALIANZA R.L, 2015)

Los riesgos fueron identificados y catalogados de acuerdo a los procesos COBIT anteriores, considerando además el contexto externo e interno de trasladar el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica.

Es importante indicar que al establecer el contexto externo e interno, no sólo se consideraron los riesgos alrededor del centro de datos a subcontratar, sino que además se tomaron en cuenta riesgos que actualmente posee la cooperativa con su actual y propio centro de datos; y que eventualmente dichos riesgos pueden tener variaciones relevantes al trasladar el procesamiento y almacenamiento a un centro de datos de un tercero. El cuadro 13 detalla los principales diecisiete (17) riesgos identificados, su categorización con respecto a los procesos COBIT y su respectiva definición.

Cuadro 13 Riesgos

No.	Proceso COBIT	Riesgo	Definición
1	AI3	Daño en los equipos de la plataforma tecnológica	Un funcionario de Tecnología de Información de la cooperativa o un empleado subcontratado al realizar mantenimiento, trabajos de actualización, instalaciones y/o mejoras, afecta de manera considerable equipamiento de tecnología crítico de la cooperativa tal como: servidores de datos, almacenamiento, equipo de comunicación; provocando que los servicios críticos de la cooperativa

			no puedan ser entregados a los clientes y asociados. También se considera afectaciones provocadas por terceros sin autorización o provocados por desastres naturales.
2	AI3	Inadecuada migración y/o traslado de datos al centro de datos	Un administrador de base de datos de la cooperativa o un empleado subcontratado al realizar una migración y/o traslado de datos, por inadecuado dimensionamiento del ancho de banda requerido o por daño en los equipos durante el traslado, o por negligencia provoca afectaciones importantes a la integridad, confidencialidad y disponibilidad de la información crítica de la cooperativa.
3	AI6	Inadecuada gestión de cambios	Un funcionario de Tecnología de Información de la cooperativa o un empleado subcontratado por la implementación de un cambio no aprobado o un cambio que no fue probado en un ambiente controlado de pruebas provoca degradación o no disponibilidad de servicios críticos de la cooperativa, pérdida de confianza y credibilidad del área de TI o incumplimiento de acuerdos de niveles de servicio.
4	DS4	Cierre de operaciones del proveedor del centro de datos	El proveedor del centro de datos por quiebra, embargo o desastre natural no puede ofrecer la entrega continua de los servicios pactados provocando a la cooperativa importantes pérdidas económicas, pérdida de oportunidades de negocio, pérdida de imagen, procesos legales y hasta un eventual cierre de operaciones.
5	DS2	Personal no calificado del proveedor del centro de datos	El personal del proveedor del centro de datos o el personal de otro tercero que contrata el proveedor del centro de datos por falta de conocimiento, habilidades, experiencia y/o rotación de personal no realiza las labores de una manera eficiente y segura provocando afectación a la integridad, confidencialidad y disponibilidad de la información, pérdidas económicas y/o pérdida de imagen de la cooperativa.
6	DS2	Inadecuado monitoreo del desempeño del proveedor del centro de datos	El Encargado de Gestión de Proveedores no establece formalmente en la cooperativa actividades de monitoreo periódicas

			del desempeño del proveedor del centro de datos provocando que exista incumplimiento de los acuerdos de niveles de servicio pactados y/o degradación o no disponibilidad del servicio contratado.
7	DS5	Operaciones ilícitas o fraudulentas desarrolladas por personal propio o externo	Un funcionario de Tecnología de Información de la cooperativa y/o personal del proveedor del centro de datos o el personal de otro tercero que contrata el proveedor del centro de datos realiza transacciones y/o operaciones ilícitas o fraudulentas por exceso de confianza, por ausencia de mecanismos de monitoreo a los accesos otorgados a personal interno o externo, por vulnerabilidades en los sistemas, por desmotivación o descontento provocando importantes pérdidas económicas, pérdida de imagen, afectación a la integridad y confidencialidad de la información, procesos legales e incremento de costos.
8	DS4	Imposibilidad de recuperarse ante un desastre en el centro de datos	La cooperativa y el proveedor del centro de datos no cuentan con un plan de continuidad que considere las acciones necesarias para soportar antes, durante y después un evento con un impacto significativo provocando importantes pérdidas económicas, degradación o no disponibilidad del servicio, pérdida de imagen, procesos legales y hasta el cierre de operaciones de la cooperativa.
9	DS5	Divulgación de información confidencial	Un funcionario de Tecnología de Información de la cooperativa y/o personal del proveedor del centro de datos o el personal de otro tercero que contrata el proveedor del centro de datos por dolo, negligencia, inexistencia o inapropiada clasificación de la información divulga información sensible y/o confidencial de la cooperativa o información clasificada del proveedor del centro de datos provocando sanciones por incumplimiento de normativa externa y/o leyes, pérdida de confianza en el negocio, pérdidas económicas y/o pérdida de imagen.
10	DS5	Pérdida de integridad de la información	Un funcionario de Tecnología de

			Información de la cooperativa y/o personal del proveedor del centro de datos o el personal de otro tercero que contrata el proveedor del centro de datos por dolo, negligencia, inadecuada administración de los datos altere/cambie sin autorización y justificación información sensible, crítica y/o relevante de la cooperativa provocando la transmisión y/o almacenamiento de datos que son incompletos o inexactos, pérdidas económicas, pérdida de imagen y/o pérdida de confianza en el negocio.
11	DS5	No disponibilidad de la información	Un funcionario de Tecnología de Información de la cooperativa y/o personal del proveedor del centro de datos o el personal de otro tercero que contrata el proveedor del centro de datos por dolo, negligencia, por inexistencia de mecanismos de alta disponibilidad en la infraestructura origina que información sensible, crítica y/o relevante de la cooperativa no esté disponible cuando la cooperativa lo requiere provocando sanciones por incumplimiento de normativa externa y/o leyes, pérdida de oportunidades de negocios, pérdida de imagen y/o pérdida de confianza en el negocio.
12	DS10	Inadecuada gestión de problemas, incidentes y eventos	Un funcionario de Tecnología de Información de la cooperativa y/o personal del proveedor del centro de datos o el personal de otro tercero que contrata el proveedor del centro de datos por deficiencias en el proceso de comunicación de incidentes, por poca disponibilidad de recurso humano, por ausencia de una área (*Help Desk*) especializada origina el no mantener formalmente actividades de gestión y control de problemas, incidentes y eventos que minimicen cualquier impacto negativo para la cooperativa provocando degradación o no disponibilidad del servicio, interrupciones en la continuidad del negocio, pérdida de imagen, pérdida económica y/o pérdida de clientes.
13	DS12	Afectaciones de instalaciones críticas por desastres naturales y/o ataques físicos	La cooperativa y el proveedor del centro de datos no cuentan con un plan de continuidad que considere las acciones necesarias para

			soportar antes, durante y después afectaciones ante desastres naturales y/o ataques físicos de cualquier instalación de la cooperativa propia o subcontratada que procese o almacene información crítica provocando importantes pérdidas económicas, degradación o no disponibilidad del servicio, pérdida de imagen, procesos legales y hasta el cierre de operaciones de la cooperativa.
14	DS12	Espacio físico insuficiente en el centro de datos subcontratado	La Gerencia de Tecnologías de Información y las Jefaturas de TI realizan un inadecuado dimensionamiento del espacio requerido en el centro de datos por la cooperativa tanto para las necesidades actuales como futuras, lo anterior por falta de un proceso de monitoreo de tendencias y/o nuevas tecnologías de la industria, por falta de alineamiento de TI con el negocio provocando pérdida de oportunidades de negocios, incremento de costos, pérdida de confianza entre las partes (TI, negocio y proveedor) y entrega del servicio no acorde a los requerimientos de la cooperativa.
15	ME2	Incumplimiento de normativas relacionadas con regulaciones y leyes	La Gerencia de Tecnologías de Información y las Jefaturas de TI por falta de divulgación de normativas, por falta de compromiso para aplicar las normativas, por un inadecuado proceso de inducción y capacitación, por negligencia se incumpla de manera parcial o total normativas de entes regulatorios tales como el acuerdo SUGEF 14-09, otra normativa de la SUGEF o normativa del Banco Central de Costa Rica (BCCR) con respecto al Sistema Nacional de Pagos Electrónicos (SINPE), así como leyes tales como Ley 8968 “Ley de protección de la persona frente al tratamiento de sus datos personales” provocando procesos legales, pérdida de imagen, sanciones de entes supervisores, pérdidas económicas u otras sanciones administrativas.
16	DS12	Dificultad para monitorear y verificar la administración sobre el ambiente físico subcontratado	La Gerencia de Tecnologías de Información, las Jefaturas de TI y Seguridad Corporativa por falta de dispositivos o herramientas que

			permitan el monitoreo del espacio físico contratado, por inadecuados procedimientos y acuerdos para tramitar accesos al centro de datos ante situaciones de emergencia, por restricciones del proveedor (acceso fuera de horario, uso de dispositivos de grabación, por falta de comunicación por parte del proveedor ante cambios en sus políticas internas se origina dificultad para ejercer el control sobre el ambiente físico administrado por el tercero provocando pérdida económica, no disponibilidad del servicio, pérdida de imagen, procesos legales, pérdida de confianza entre las partes (TI, negocio y proveedor) y/o la entrega del servicio no acorde a los requerimientos de la cooperativa.
17	DS9	Información documentada no refleja la arquitectura actual	El administrador de la configuración por la inexistencia de un repositorio actualizado de la configuración, por inexistencia de un proceso para administrar la configuración, por un inadecuado o inexistente proceso de gestión de cambios no mantiene actualizados los estándares, procedimientos, metodologías, directrices, políticas, repositorio de configuración acorde a la infraestructura actual de la cooperativa provocando dificultad para la toma de decisiones, incumplimiento de normativa interna y externa, la existencia de un plan de infraestructura tecnológica inconsistente, costos no contemplados, riesgos no mitigados, planes de contingencia mal diseñados.

(Unidad de Riesgo Corporativo COOPEALIANZA R.L, 2015)

Posterior a la identificación de los riesgos y su categorización con respecto a los procesos COBIT, además de la respectiva definición; se hace necesario identificar las causas internas y/o externas que podrían originar los riesgos identificados, las cuales fueron determinadas de acuerdo a cada riesgo, el cuadro 14 muestra las causas para cada riesgo.

Cuadro 14 Causas

No.	Riesgo	Causas
1	Daño en los equipos de la plataforma tecnológica	-Dolo -Fallas o inadecuado funcionamiento del sistema eléctrico -Fallas o inadecuado funcionamiento del sistema de enfriamiento -Sabotaje -Desastres naturales -Defectos de fábrica -Negligencia -Vandalismo
2	Inadecuada migración y/o traslado de datos al centro de datos	-Inadecuado dimensionamiento del ancho de banda -Interrupción en la comunicación -Daño en los equipos durante el traslado -Imposibilidad de traslado físico de los datos -Negligencia -Inadecuada planificación en el proceso de migración -Pérdida de integridad de los datos durante el traslado
3	Inadecuada gestión de cambios	-Cambios no cumplen con arquitectura de tecnología global -Cambios no documentados -Control y seguimiento insuficiente sobre los cambios -Falta de prioridades en la gestión de cambios según los requerimientos del negocio -Cambios no autorizados ni detectados al ambiente de producción -Inadecuada dirección tecnológica -Falta de estudios técnicos y funcionales -Falta de una visión integral del negocio -Ausencia de un Comité de Arquitectura y Comité de Gestión de Proyectos e Inversiones -Ausencia de un Gestor de Cambios -Falta de personal capacitado -Incumplimiento del marco normativo -Falta de integración con los procesos de administración de problemas y configuración -Inadecuada priorización de cambios según las necesidades del negocio -Mal manejo de versiones en el desarrollo de software -Ausencia de un asistente de Administración de Proyectos de TI
4	Cierre de operaciones del proveedor del centro de datos	-Imposibilidades legales para operar -Quiebras o embargos -Desastres naturales -Ataque externo (lógico o físico) -Incapacidad del proveedor del centro de datos de adaptarse a tendencias y/o nuevas tecnologías de la industria requeridas por la organización

5	Personal no calificado del proveedor del centro de datos	-Acuerdos de nivel de servicio que no cumplen con los requerimientos de la cooperativa -Rotación de personal -Ausencia de un plan de capacitación y entrenamiento periódico -Inadecuada selección y reclutamiento del personal por parte del proveedor
6	Inadecuado monitoreo del desempeño del proveedor del centro de datos	-Ausencia de un responsable de la relación con el proveedor del centro de datos -Ausencia de un marco normativo -Herramientas de monitoreo inadecuadas -Incumplimiento de los cronogramas de monitoreo -No disponibilidad de los responsables de los procesos requirentes
7	Operaciones ilícitas o fraudulentas desarrolladas por personal propio o externo	-Modificaciones de software no autorizadas -Negligencia de personal -Exceso de confianza -Ausencia de mecanismos de monitoreo a los accesos otorgados a personal interno o externo -Uso de herramientas de software no autorizadas -Inapropiado establecimiento de roles de acceso -Falta de aplicación de la política conozca a su empleado -Falta de especificaciones en los requerimientos de seguridad en los sistemas -Vulnerabilidades en los sistemas -Desmotivación o descontento del personal -Suplantación de personal -Inadecuado manejo de las claves a los sistemas -Falta de mecanismos en seguridad de redes -Extorción -Ineficientes medidas de prevención detección y corrección -Inexistencia o incumplimiento de la normativa -Falta de aplicación de la política conozca a su proveedor -Dolo -Negligencia
8	Imposibilidad de recuperarse ante un desastre en el centro de datos	-Ausencia de un plan de continuidad del proveedor y/o de la cooperativa -El plan de recuperación del proveedor y/o TI no cumple con los requerimientos o infraestructura actuales del negocio -No idoneidad del personal a cargo en el momento del desastre -Ineficiente divulgación y disponibilidad del plan de continuidad
9	Divulgación de información confidencial	-Inadecuada protección de datos sensibles en la transferencia, reproducción, eliminación, almacenamiento y actualización

		-Inexistencia o inapropiada clasificación de la información -Falta de monitoreo y restricción de aplicaciones no autorizadas -Dolo -Negligencia -Falta de cultura de seguridad de la información -Inexistente o inapropiado marco normativo -Violaciones a la seguridad lógica de la información -Inadecuada administración de los datos
10	Pérdida de integridad de la información	-Cambios aplicados directamente a los datos -Negligencia -Dolo -Inexistente o inapropiado marco normativo -Violaciones a la seguridad lógica de la información -Fallas en las comunicaciones -Inadecuada administración de los datos
11	No disponibilidad de la información	-Incapacidad para restaurar información o volver a un estado anterior provocado por un incidente o desastre -Inexistencia de mecanismos de alta disponibilidad en la infraestructura -Negligencia -Dolo -Inexistente o inapropiado marco normativo -Violaciones a la seguridad lógica de la información -Fallas en las comunicaciones -Ausencia de un plan de continuidad del proveedor y/o de la cooperativa -El plan de recuperación del proveedor y/o TI no cumple con los requerimientos o infraestructura actuales del negocio -Inadecuada administración de los datos -No idoneidad del personal a cargo en el momento del desastre -Ineficiente divulgación y disponibilidad del plan de continuidad -Dificultad para acceder físicamente a la infraestructura instalada en el centro de datos subcontratado
12	Inadecuada gestión de problemas, incidentes y eventos	-Recurrencia de problemas e incidentes -Falta de pistas de auditoría de los problemas, incidentes y sus soluciones para un manejo proactivo -Deficiencias en el proceso de comunicación de incidentes -Poca disponibilidad de recurso humano -Inexistencia de una base de datos de conocimiento -Ausencia de una área (*Help Desk*) especializada -Inapropiada inversión del tiempo -La magnitud o complejidad del incidente supera la capacidad de respuesta

		-Incumplimiento de la normativa externa e interna
13	Afectaciones de instalaciones críticas por desastres naturales y/o ataques físicos	-Falta de planificación en la ubicación de las instalaciones -Falta de implementar las medidas de protección -Falta de un análisis de riesgos antes de la planificación de los proyectos de selección y/o construcción -Negligencia -Afectación por factores externos(huelgas, terremotos, incendios, tormentas eléctricas, huracanes, inundaciones, actividad volcánica, *cyber* terrorismo) -Incumplimiento de normativa externa y/o leyes
14	Espacio físico insuficiente en el centro de datos subcontratado	-TI no alineado con el negocio -Falta de un proceso de monitoreo de tendencias y/o nuevas tecnologías de la industria -Requerimientos regulatorios -Inadecuado dimensionamiento del espacio requerido en el centro de datos
15	Incumplimiento de normativas relacionadas con regulaciones y leyes	-Falta de divulgación de normativas -Falta de compromiso para aplicar las normativas -Inadecuado proceso de inducción y capacitación -Desconocimiento de las normas -Falta de seguimiento y monitoreo del cumplimiento de la normativa -Rotación de personal -Negligencia -Dolo -Ambigüedad de las normas
16	Dificultad para monitorear y verificar la administración sobre el ambiente físico subcontratado	-Falta de dispositivos o herramientas que permitan el monitoreo del espacio físico contratado -Inadecuados procedimientos y acuerdos para tramitar accesos al centro de datos ante situaciones de emergencia o inusuales -Restricciones del proveedor(acceso fuera de horario, uso de dispositivos de grabación) -Falta de comunicación por parte del proveedor ante cambios en sus políticas internas
17	Información documentada no refleja la arquitectura actual	-Inexistencia de repositorio actualizado de la configuración -No existe un proceso para administrar la configuración -Falta de personal -Complejidad de la infraestructura y su documentación -Inadecuado o inexistente gestión de cambios -Inadecuado funcionamiento del software -Incumplimiento de la normativa interna y/o externa -Inexistencia de normativa

(Unidad de Riesgo Corporativo COOPEALIANZA R.L, 2015)

Para detallar la manera de ocurrencia de los riesgos, así como los efectos que tendrían sobre el desencadenamiento de otros riesgos, propios del proceso o de

otros, o sea, los efectos o impactos de una posible materialización del riesgo durante el proceso de este estudio y debido a la no administración adecuada del riesgo, se definieron como se muestra en el cuadro 15, las consecuencias para cada riesgo.

Cuadro 15 Consecuencias

No.	Riesgo	Consecuencias
1	Daño en los equipos de la plataforma tecnológica	-Pérdidas económicas -Incremento de costos -Pérdida de oportunidades de negocio -Degradación o no disponibilidad del servicio -Pérdida de imagen -Procesos legales
2	Inadecuada migración y/o traslado de datos al centro de datos	-Afectación a la integridad, confidencialidad y disponibilidad de la información -Pérdidas económicas -Incremento de costos -Pérdida de oportunidades de negocio -Degradación o no disponibilidad del servicio -Pérdida de imagen -Procesos legales
3	Inadecuada gestión de cambios	-Pérdidas económicas -Esfuerzos mal dirigidos -Dificultad de mantenimiento y pruebas -Problemas de integración -Pérdida de competitividad -TI no alineado con el negocio -Incapacidad para atender requerimientos -Problemas de compatibilidad -Incumplimiento de acuerdos de niveles de servicio -Degradación o no disponibilidad del servicio -Pérdida de oportunidades de negocios -Fraude -Pérdida de confianza y credibilidad
4	Cierre de operaciones del proveedor del centro de datos	-Afectación a la integridad, confidencialidad y disponibilidad de la información -Pérdidas económicas -Incremento de costos -Pérdida de oportunidades de negocio -Degradación o no disponibilidad del servicio -Pérdida de imagen -Procesos legales -Cierre de operaciones de la cooperativa
5	Personal no calificado del proveedor del centro de datos	-Afectación a la integridad, confidencialidad y disponibilidad de la información -Pérdidas económicas

		-Incremento de costos -Pérdida de oportunidades de negocio -Degradación o no disponibilidad del servicio -Pérdida de imagen -Procesos legales
6	Inadecuado monitoreo del desempeño del proveedor del centro de datos	-Incumplimiento de los acuerdos de niveles de servicio -Afectación a la integridad y confidencialidad de la información -Pérdidas económicas -Incremento de costos -Pérdida de oportunidades de negocio -Degradación o no disponibilidad del servicio -Pérdida de imagen -Procesos legales
7	Operaciones ilícitas o fraudulentas desarrolladas por personal propio o externo	-Procesos legales -Pérdidas económicas -Pérdida de imagen -Rotación de personal -Sanciones a la Cooperativa -Afectación a la integridad y confidencialidad de la información -Incremento de costos -Pérdida de oportunidades de negocio -Degradación o no disponibilidad del servicio
8	Imposibilidad de recuperarse ante un desastre en el centro de datos	-Afectación a la integridad, confidencialidad y disponibilidad de la información -Pérdidas económicas -Incremento de costos -Pérdida de oportunidades de negocio -Degradación o no disponibilidad del servicio -Pérdida de imagen -Procesos legales -Cierre de operaciones de la cooperativa
9	Divulgación de información confidencial	-Procesos legales -Sanciones por incumplimiento de normativa externa y/o leyes -Pérdida de oportunidades de negocios -Pérdidas económicas -Pérdida de imagen -Pérdida de confianza en el negocio -Cierre de operaciones de la cooperativa
10	Pérdida de integridad de la información	-Datos transmitidos que son incompletos o inexactos -Procesos legales -Sanciones por incumplimiento de normativa externa y/o leyes -Pérdida de oportunidades de negocios -Pérdidas económicas -Pérdida de imagen

		-Pérdida de confianza en el negocio
11	No disponibilidad de la información	-Procesos legales -Sanciones por incumplimiento de normativa externa y/o leyes -Pérdida de oportunidades de negocios -Pérdidas económicas -Pérdida de imagen -Pérdida de confianza en el negocio -Falta de información para tomar medidas defensivas
12	Inadecuada gestión de problemas, incidentes y eventos	-Afectación de la disponibilidad, integridad y confidencialidad de la información -Pérdida de imagen -Pérdida económica -Pérdida de asociados y clientes -Rotación de personal -Pérdida de oportunidades de negocios -Interrupciones en la continuidad del negocio -Degradación o no disponibilidad del servicio -Sanciones a la Cooperativa -Procesos legales
13	Afectaciones de instalaciones críticas por desastres naturales y/o ataques físicos	-Pérdida económica -Daños en equipos -Pérdida información -No disponibilidad del servicio -Pérdida de imagen -Pérdida de productividad -Cierre parcial o total de las operaciones de la cooperativa -Procesos legales
14	Espacio físico insuficiente en el centro de datos subcontratado	-Procesos legales -Pérdida de oportunidades de negocios -Pérdidas económicas -Pérdida de imagen -Incremento de costos -Pérdida de confianza entre las partes(TI, negocio y proveedor) -Entrega del servicio no acorde a los requerimientos del negocio
15	Incumplimiento de normativas relacionadas con regulaciones y leyes	-Procesos legales -Pérdida de imagen -Sanciones de entes supervisores -Pérdidas económicas -Sanciones administrativas
16	Dificultad para monitorear y verificar la administración sobre el ambiente físico subcontratado	-Pérdida económica -No disponibilidad del servicio -Pérdida de imagen -Procesos legales -Pérdida de confianza entre las partes(TI, negocio y proveedor)

		-Entrega del servicio no acorde a los requerimientos del negocio
17	Información documentada no refleja la arquitectura actual	-Dificultad para la toma de decisiones -Incumplimiento de normativa interna y externa -Plan de infraestructura tecnológica inconsistente -TI no alineado con el negocio -Costos no contemplados -Riesgos no mitigados -Planes de contingencia mal diseñados -Documentación de la arquitectura critica inconsistente -Imposibilidad de restaurar un elemento de configuración a un estado anterior -Degradación o no disponibilidad de los servicios

(Unidad de Riesgo Corporativo COOPEALIANZA R.L, 2015)

Una vez identificados los riesgos, y haberlos alineado a procesos reconocidos de gestión y control en tecnologías de información, incorporando su respectiva definición e identificado sus causas y consecuencias; se tiene los insumos necesarios para abordar la siguiente etapa del proceso de gestión del riesgo, denominada “Análisis de riesgo”, en esta etapa se hace necesario valorar cada riesgo de acuerdo a su probabilidad e impacto, considerando los insumos recolectados en las etapas de establecimiento del contexto e identificación del riesgos, el objetivo de la siguiente etapa es obtener el riesgo inherente y el riesgo residual; para este último se hace necesario además identificar los controles que la cooperativa ha implementado o mantiene en operación.

4.2.3 Análisis de riesgo

Para cumplir con el proceso de gestión de riesgos, de forma que se pueda valorar y priorizar los riesgos con base en la información obtenida en la etapa de identificación, se llevó a cabo un análisis de dichos riesgos. Este análisis se basó en variables de probabilidad e impacto y en la evaluación de los controles, de forma que, para cada uno de los riesgos identificados se determinaron y relacionaron dichas variables. Igualmente, por medio de un mapa de calor de riesgos se conoce el nivel de riesgo inherente (sin controles) y residual (con controles).

El cuadro 16 muestra para cada riesgo los controles existentes o que se encuentran implementados por la cooperativa a la fecha de este estudio.

Cuadro 16 Controles existentes

No.	Riesgo	Controles
1	Daño en los equipos de la plataforma tecnológica	-Aplicación integral de la "Parte A Asignación de Recursos Tecnológicos, Parte B Uso de Recursos Tecnológicos" de la directriz DI-074 "Administración, asignación y seguridad de los recursos y servicios de TI" - "Responsabilidades sobre los recursos" en el perfil del puesto - Aplicación integral del procedimiento PR-TI-OPE-002 "Administración del desempeño y la capacidad" - Aplicación integral de los estándares tecnológicos - Mecanismos existentes de seguridad física (gabinete, control de acceso biométrico, puerta con cerradura, alarma de detección de intrusos, sistema de prevención temprana de incendio)
2	Inadecuada migración y/o traslado de datos al centro de datos	-Aplicación del procedimiento PR-TI-BD-032 "Migración de base datos Oracle" -Aplicación de la ME-AP-001 " Metodología para la administración de proyectos"
3	Inadecuada gestión de cambios	-Aplicación del procedimiento PR-TI-OPE-004 "Control de cambios en aplicaciones e infraestructura de TI" (todo el procedimiento). -Aplicación de la Directriz DI-120 "Funcionamiento de los comités administrativos y grupos de apoyo" PARTE D: Comité de Arquitectura y PARTE G: Comité de Gestión de Proyectos y Cambios de TI. -Aplicación de la Directriz DI-025 "Administración y control de tecnologías de información, punto 3 Administración de cambios. -Uso de la herramienta de software de administración de cambios
4	Cierre de operaciones del proveedor del centro de datos	-Se cuenta con una ubicación geográficamente alejada para procesamiento y almacenamiento alternativo documentado en el plan de continuidad del negocio PL-SG-CO-001 -Se cuenta con un diseño de red que permite que la información sea distribuida entre diferentes centros de datos documentado en el plan de continuidad del negocio PL-SG-CO-001 -Se cuenta con una solución de replicación de base de datos documentado en el plan de continuidad del negocio PL-SG-CO-001
5	Personal no calificado del proveedor del centro de datos	-Aplicación del procedimiento PR-LEG-002

		"Requerimiento de contrato" paso 2 -Aplicación integral del procedimiento PR-SG-GPP-001 "Acreditación de proveedores de COOPEALIANZA R.L y Subsidiarias" -Aplicación integral del procedimiento PR-SG-GPP-003 "Evaluación de proveedores críticos e importantes" -Aplicación de la metodología ME-SG-GPP-001 "Administración de servicios de terceros" en su punto 5.6 "Monitorear el desempeño de proveedores"
6	Inadecuado monitoreo del desempeño del proveedor del centro de datos	-Aplicación de la metodología ME-SG-GPP-001 "Administración de servicios de terceros" en su punto 5.6 "Monitorear el desempeño de proveedores" -Aplicación integral del procedimiento PR-SG-GPP-003 "Evaluación de proveedores críticos e importantes" -Aplicación del procedimiento PR-LEG-002 "Requerimiento de contrato" paso 2
7	Operaciones ilícitas o fraudulentas desarrolladas por personal propio o externo	-Estándar #7 " Estándares y reglas de seguridad para aplicaciones y sistemas donde se establece la aplicación de mecanismos de autenticación de acceso al sistema. -Aplicación del Plan de Seguridad de la Información donde se definen las revisiones que debe realizar el área de seguridad de la información. -Ejecución de un mecanismo formal para la creación de usuarios, entrega de permisos y dada de baja de usuarios según procedimientos: PR-SG-SI-001 Inclusión de formas nuevas y registro y modificación de parámetros(integral), PR-SG-SI-002 Solicitud, creación e inactivación usuarios; creación, modificación, asignación y derogación de roles de acceso (integral), PR-SG-SI-003 Creación de usuarios en el dominio y los sistemas(integral), PR-SG-SI-004 Inactivación de usuarios en los sistemas(integral), PR-SG-SI-005 Creación de roles en los sistemas(integral), PR-SG-SI-006 Asignación de roles de acceso a los usuarios (integral), PR-SG-SI-007 Derogación de roles en los sistemas(integral), PR-SG-SI-008 Modificación de roles de acceso(integral), PR-SG-SI-009 Activación de usuarios en los sistemas(integral), PR-TI-BD-002 Mantenimiento de usuarios en las Bases de Datos (integral) -Aplicación de la directriz DI-113 donde se norma la gestión de Seguridad de la Información capítulo 5. -Aplicación de la directriz DI-025 "Administración y control de tecnologías de información(Puntos 4 y 7 del CAPÍTULO III ENTREGA Y SOPORTE) -Se efectúan pruebas en conformidad con los procedimientos: PR-TI-SI-013 "Cambios: Mantenimiento-corrección y mantenimiento de mejoras" (integral), y PR-TI-SI-015 "Proyectos"(integral) y PR-TI-SI-021 "Aprobación, publicación y eliminación de archivos en el

		servidor de aplicaciones" -Ejecución del procedimiento PR-SG-SI-017 Monitoreo de actividades de los usuarios en los sistemas utilizados en COOPEALIANZA (Paso 4), aplica para personal interno.
8	Imposibilidad de recuperarse ante un desastre en el centro de datos	-Se cuenta con una ubicación geográficamente alejada para procesamiento y almacenamiento alternativo documentado en el plan de continuidad del negocio PL-SG-CO-001 -Se cuenta con un diseño de red que permite que la información sea distribuida entre diferentes centros de datos documentado en el plan de continuidad del negocio PL-SG-CO-001 -Se cuenta con una solución de replicación de base de datos documentado en el plan de continuidad del negocio PL-SG-CO-001 -Se cuenta con un plan de continuidad que contiene una estrategia de recuperación de TI -Aplicación del procedimiento PR-LEG-002 "Requerimiento de contrato" paso 2 -Aplicación integral del procedimiento PR-SG-GPP-001 "Acreditación de proveedores de COOPEALIANZA R.L y Subsidiarias"
9	Divulgación de información confidencial	-Se cuenta con acuerdos de confidencialidad con los proveedores normado en el procedimiento PR-SG-GPP-001 "Acreditación de proveedores de COOPEALIANZA R.L y Subsidiarias" en el apartado observaciones -Aplicación del procedimiento PR-LEG-002 "Requerimiento de contrato" paso 7 -Aplicación de la metodología ME-SG-SI-001 "METODOLOGÍA CLASIFICACIÓN Y ETIQUETADO DE INFORMACIÓN EN COOPEALIANZA R.L. Y SUBSIDIARIAS" (integral), -Aplicación de la directriz DI-113 "Directriz de seguridad de la información en COOPEALIANZA R.L. y Subsidiarias integral. -Aplicación integral del Procedimiento PR-SG-SI-018 "Atención de requerimientos Corporativos" -Aplicación del procedimiento PR-SG-SI-013 Administración de la seguridad de TI. (Paso número 3) -Se efectúan pruebas en conformidad con los procedimientos: PR-TI-SI-013 "Cambios: Mantenimiento-corrección y mantenimiento de mejoras" (integral), y PR-TI-SI-015 "Proyectos"(integral) -Ejecución de un mecanismo formal para la creación de usuarios, entrega de permisos y dada de baja de usuarios según procedimientos: PR-SG-SI-001 Inclusión de formas nuevas y registro y modificación de parámetros(integral), PR-SG-SI-002 Solicitud, creación e inactivación usuarios; creación, modificación, asignación y derogación de roles

		de acceso (integral), PR-SG-SI-003 Creación de usuarios en el dominio y los sistemas(integral), PR-SG-SI-004 Inactivación de usuarios en los sistemas(integral), PR-SG-SI-005 Creación de roles en los sistemas(integral), PR-SG-SI-006 Asignación de roles de acceso a los usuarios (integral), PR-SG-SI-007 Derogación de roles en los sistemas(integral), PR-SG-SI-008 Modificación de roles de acceso(integral), PR-SG-SI-009 Activación de usuarios en los sistemas(integral), PR-TI-BD-002 Mantenimiento de usuarios en las Bases de Datos (integral) -Ejecución del procedimiento PR-SG-SI-014 Entrega de Información Clasificada (Paso 4)
10	Pérdida de integridad de la información	-Se efectúan pruebas técnicas del sistema y de usuarios en conformidad con los procedimientos: PR-TI-SI-013 "Cambios: Mantenimiento-corrección y mantenimiento de mejoras" (integral), y PR-TI-SI-015 "Proyectos"(integral) -Ejecución del procedimiento PR-SG-SI-016 Reporte, registro, categorización de incidentes que afecten la Seguridad de la Información paso 3 -Ejecución del procedimiento PR-SG-SI-017 Monitoreo de actividades de los usuarios en los sistemas utilizados en COOPEALIANZA (Paso 4) -Aplicación de la directriz DI-025 "Administración y control de tecnologías de información (Puntos 4 y 7 del CAPÍTULO III ENTREGA Y SOPORTE) -Aplicación de la directriz DI-113 "Directriz de seguridad de la información en COOPEALIANZA R.L. y Subsidiarias integral. -Ejecutar el cronograma de pruebas del plan de continuidad PL-SG-CO-001, "Prueba de integridad y disponibilidad de los datos"
11	No disponibilidad de la información	-Aplicación del procedimiento PR-SG-SI-013 Administración de la seguridad de TI. (Paso número 3) -Ejecución del procedimiento PR-SG-SI-016 Reporte, registro, categorización de incidentes que afecten la Seguridad de la Información paso 3 -Aplicación de la Directriz DI-025 "Administración y control de tecnologías de información (Puntos 4 y 7 del CAPÍTULO III ENTREGA Y SOPORTE) -Aplicación del Plan de capacidad y desempeño PL-TI-001 -Aplicación del Plan de continuidad del negocio PL-SG-CO-001
12	Inadecuada gestión de problemas, incidentes y eventos	-Aplicación del PR-SI-CO-001 "Atención, escalabilidad y notificación por interrupción del servicio crítico T.I." pasos del 1 al 13 -Aplicación del PR-TI-011 "Análisis de cambios y

		problemas relacionados y su afectación a la CMBD." pasos del 1 al 13. -Aplicación del PR-TI-007 "Atención de incidentes y problemas que afecten servicios críticos TI." pasos del 1 al 34. -Aplicación del PR-TI-006 "Reporte de incidentes a proveedores de TI." pasos del 1 al 19.
13	Afectaciones de instalaciones críticas por desastres naturales y/o ataques físicos	-Evaluación y verificación de la aplicación del estándar Tecnológico de COOPEALIANZA R.L y Subsidiarias.
14	Espacio físico insuficiente en el centro de datos subcontratado	-Aplicación del plan de capacidad y desempeño PL-TI-001 “Plan para la Administración del desempeño y la capacidad”
15	Incumplimiento de normativas relacionadas con regulaciones y leyes	-Revisión de Auditoria Externa e interna -Aplicación de la ME-SCI-CI-003 " Autoevaluación de la Gestión y el Control de COOPEALIANZA R.L"
16	Dificultad para monitorear y verificar la administración sobre el ambiente físico subcontratado	No se identificaron controles
17	Información documentada no refleja la arquitectura actual	-Para el proceso de administración de la configuración se cuentan con herramientas como *Metrix* (administración de licencias) y RCM (*Remote Condition Management Configuration Manager* -equipos de comunicación) de la empresa GCI, que suministran información al repositorio central de configuración (CMDB) -El Repositorio Central de Configuración contiene: hardware, software, middleware, parámetros, documentación, los procedimientos, nombre, número de versión y detalles de licenciamiento. -Existe un procedimiento el cual se encarga de normalizar el proceso para administrar la configuración: (PR-TI-OPE-001 Administración de la configuración y revisión de la infraestructura de forma Integral). - Envío anual del Perfil Tecnológico, Acuerdo SUGEF 14-09. - Aplicación de forma integral del Procedimiento PR-TI-OPE-001 Administración de la configuración y revisión de la infraestructura de forma integral. - Aplicación del Procedimiento PR-TI-011 Análisis de cambios y problemas relacionados y su afectación a la CMBD en sus pasos 4, 5 y 7. - Auditorías Externas (Seguimiento oportunidades de mejora, Acuerdo SUGEF 14-09) -Aplicación del PR-TI-OPE-004 "CONTROL DE CAMBIOS EN APLICACIONES E INFRAESTRUCTURA SOPORTADA POR TECNOLOGÍAS DE INFORMACIÓN" en sus pasos 12,13 y 14. -Autoevaluación del proceso según metodología ME-SCI-

		CI-002 “Evaluación del marco de control de Tecnologías de Información”, Capitulo VIII. RECURSOS/ 2. RECURSOS TECNOLÓGICOS/ Capitulo IX. AUTOEVALUACIÓN DE LOS CONTROLES INTERNOS DE TECNOLOGÍAS DE INFORMACIÓN.

(Unidad de Riesgo Corporativo COOPEALIANZA R.L, 2015)

Para cumplir con el proceso de gestión de riesgos, de forma que se pueda valorar y priorizar los riesgos con base en la información obtenida en la etapa de identificación, se realizan a continuación un análisis basado en la tabla de probabilidad del riesgo (Figura 3) y la tabla de impacto del riesgo (Figura 4) para obtener el grado de valoración de un evento de riesgo inherente con relación a su máxima exposición posible, es decir, sin tener en cuenta los controles existentes o considerando que no exista gestión alguna del riesgo.

En el cuadro 17 se muestran los riesgos con la respectiva valoración resultante para el riesgo inherente y que fue realizada por medio de una encuesta a 12 participantes de distintas áreas de la cooperativa (Unidad Corporativa de Riesgos, Tecnologías de Información, Auditoría Interna, Control Interno, Seguridad de la Información, Administración de Proyectos, Continuidad del Negocio). El nivel de criticidad fue obtenido de acuerdo al mapa de riesgo inherente de la figura 7, que es el resultado del valor de probabilidad por el valor de impacto, por ejemplo para el riesgo “Daño en los equipos de la plataforma tecnológica” la probabilidad resultante fue “Probable” y el impacto fue “Crítico”, dando como resultado un nivel de criticidad para este riesgo de “Extremo” (Zona Roja) con un puntaje de criticidad de 5 de acuerdo a la Figura 13 Nivel del Riesgo, lo anterior por el hecho de ubicarse en la zona roja.

	Impacto	Insignificante	Bajo	Moderado	Significativo	Crítico
Probabilidad	Valor	1	2	3	4	5
Casi cierta	5	Moderado	Alto	Extremo	Extremo	Extremo
Probable	4	Bajo	Moderado	Alto	Extremo	Extremo
Posible	3	Bajo	Bajo	Moderado	Alto	Extremo
Poco probable	2	Muy bajo	Bajo	Bajo	Moderado	Alto
Remota	1	Muy bajo	Muy bajo	Bajo	Moderado	Alto

Figura 7 Mapa del Riesgo Inherente (Unidad de Riesgo Corporativo COOPEALIANZA R.L, 2015)

Cuadro 17 Valoración del riesgo inherente

		Riesgo Inherente Resultado de la Encuesta		
No.	**Riesgo**	**Probabilidad de Ocurrencia**	**Impacto**	**Criticidad**
1	Daño en los equipos de la plataforma tecnológica	Probable (1 a 3 meses)	Crítico	Extremo
2	Inadecuada migración y/o traslado de datos al centro de datos	Casi cierta (1 al mes)	Crítico	Extremo
3	Inadecuada gestión de cambios	Probable (1 a 3 meses)	Moderado	Alto
4	Cierre de operaciones del proveedor del centro de datos	Remota (1 al año)	Crítico	Alto
5	Personal no calificado del proveedor del centro de datos	Probable (1 a 3 meses)	Significativo	Extremo
6	Inadecuado monitoreo del desempeño del proveedor del centro de datos	Casi cierta (1 al mes)	Significativo	Extremo
7	Operaciones ilícitas o fraudulentas desarrolladas por personal propio o externo	Casi cierta (1 al mes)	Crítico	Extremo
8	Imposibilidad de recuperarse ante un desastre en el centro de datos	Casi cierta (1 al mes)	Crítico	Extremo
9	Divulgación de información confidencial	Casi cierta (1 al mes)	Crítico	Extremo
10	Pérdida de integridad de la información	Probable (1 a 3 meses)	Crítico	Extremo
11	No disponibilidad de la información	Probable (1 a 3 meses)	Crítico	Extremo
12	Inadecuada gestión de problemas, incidentes y eventos	Probable (1 a 3 meses)	Significativo	Extremo
13	Afectaciones de instalaciones críticas por desastres naturales y/o ataques físicos	Posible (3 a 5 meses)	Crítico	Extremo
14	Espacio físico insuficiente en el centro de datos subcontratado	Posible (3 a 5 meses)	Significativo	Alto
15	Incumplimiento de normativas relacionadas con regulaciones y leyes	Casi cierta (1 al mes)	Significativo	Extremo
16	Dificultad para monitorear y verificar la administración sobre el ambiente físico subcontratado	Probable (1 a 3 meses)	Moderado	Alto
17	Información documentada no refleja la arquitectura actual	Casi cierta (1 al mes)	Moderado	Extremo

(Unidad de Riesgo Corporativo COOPEALIANZA R.L, 2015)

Una vez obtenido el riesgo inherente, podemos visualizar cada uno de los riesgos de acuerdo a su identificador numérico en un mapa de calor para una mejor comprensión. La figura 8 nos muestra que los riesgos se ubican en niveles de criticidad “Extremo” y “Alto” sin considerar ningún efecto de controles.

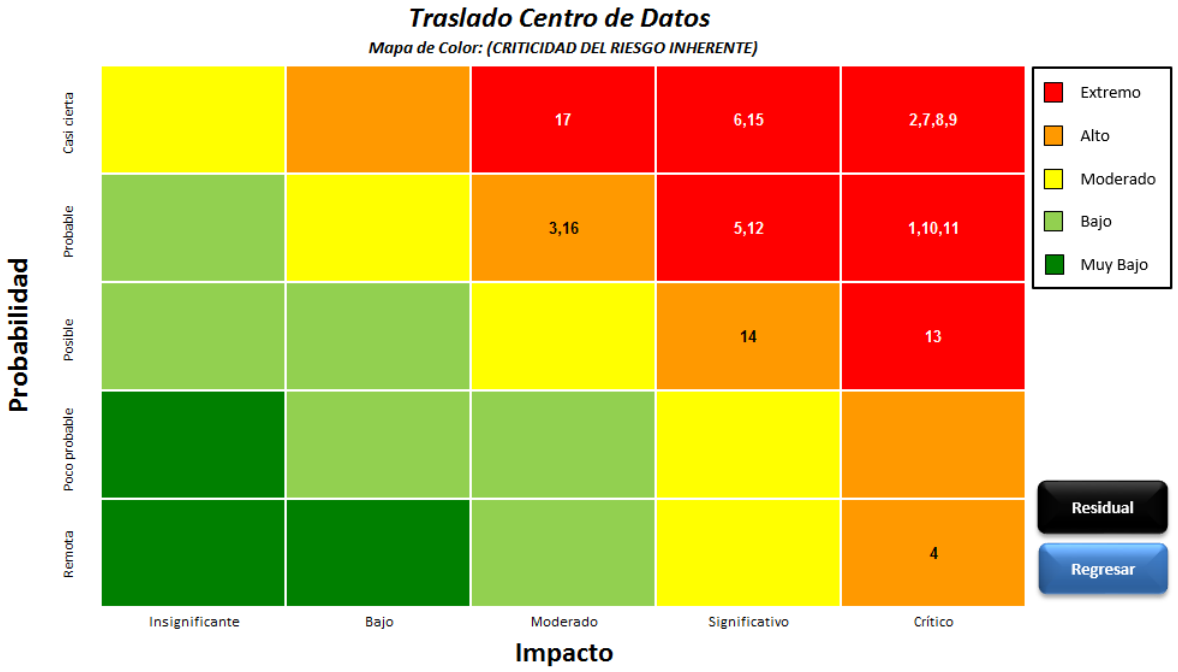


Figura 8 Mapa de Calor Criticidad del Riesgo Inherente (Unidad de Riesgo Corporativo COOPEALIANZA R.L, 2015)

Para reducir los niveles de exposición al riesgo que se muestra en la figura 8, se hace necesario evaluar los controles existentes a fin de medir la capacidad de estos para mitigar los riesgos y obtener el riesgo residual. Para lo anterior se realizó una encuesta a los 12 participantes del proceso en cuanto a la calidad y frecuencia de cada uno de los controles existentes.

Al tratarse de una importante cantidad de controles existentes, el cuadro 18 muestra la evaluación de los controles para el riesgo “Daño en los equipos de la plataforma tecnológica” y en el cuadro 19 se muestra el resultado resumen de la evaluación de los controles para los 17 riesgos analizados. Importante señalar que la calidad y la frecuencia del control se obtienen de acuerdo a la figura 6, la ponderación es el porcentaje de importancia del control que el grupo interdisciplinario acuerda y define, además se aplica un factor de estrés de 0.80 que lo que persigue es que la mitigación de los controles no produzcan una reducción total del riesgo (que el riesgo nunca sea 0) para que dé como resultado la madurez del control que resulta de las escalas que se muestran en la figura 9.

	Frecuencia	Permanente	Habitual	Ocasional	Inexistente
Calidad	Valor	1	2	3	4
Ínfima o Nula	5	Sin control	Sin control	Sin control	Sin control
Baja, Insuficiente	4	Débil	Débil	Débil	Sin control
Media, Buena	3	Satisfactoria	Adecuada	Débil	Sin control
Alta, Confiable	2	Excelente	Satisfactoria	Débil	Sin control
Excelente	1	Excelente	Excelente	Adecuada	Sin control

Madurez	Sin control	Débil	Adecuada	Satisfactoria	Excelente
%	0%	25%	50%	75%	100%

Figura 9 Nivel de Madurez y Mitigación de Controles (Unidad de Riesgo Corporativo COOPEALIANZA R.L, 2015)

Cuadro 18 Análisis de los controles para el riesgo "Daño en los equipos de la plataforma tecnológica"

Control	Calidad del Control	Frecuencia del Control	Ponderación	Madurez del Control
Aplicación integral de la "Parte A Asignación de Recursos Tecnológicos, Parte B Uso de Recursos Tecnológicos" de la directriz DI-074 "Administración, asignación y seguridad de los recursos y servicios de TI"	Media, Buena	Permanente	30%	Satisfactoria
"Responsabilidades sobre los recursos" en el perfil del puesto	Media, Buena	Permanente	20%	Satisfactoria
Aplicación integral del procedimiento PR-TI-OPE-002 "Administración del desempeño y la capacidad"	Media, Buena	Nula Inexistente	5%	Nula
Aplicación integral de los estándares tecnológicos	Alta, Confiable	Permanente	5%	Excelente
Mecanismos existentes de seguridad física (gabinete, control de	Alta, Confiable	Habitual	40%	Satisfactoria

acceso biométrico, puerta con cerradura, alarma de detección de intrusos, sistema de prevención temprana de incendio)				

(Unidad de Riesgo Corporativo COOPEALIANZA R.L, 2015)

Cuadro 19 Resumen Evaluación de los Controles

No.	Riesgo	Criticidad	Evaluación Controles
1	Daño en los equipos de la plataforma tecnológica	Extremo	Satisfactoria
2	Inadecuada migración y/o traslado de datos al centro de datos	Extremo	Satisfactoria
3	Inadecuada gestión de cambios	Alto	Satisfactoria
4	Cierre de operaciones del proveedor del centro de datos	Alto	Excelente
5	Personal no calificado del proveedor del centro de datos	Extremo	Satisfactoria
6	Inadecuado monitoreo del desempeño del proveedor del centro de datos	Extremo	Satisfactoria
7	Operaciones ilícitas o fraudulentas desarrolladas por personal propio o externo	Extremo	Satisfactoria
8	Imposibilidad de recuperarse ante un desastre en el centro de datos	Extremo	Excelente
9	Divulgación de información confidencial	Extremo	Satisfactoria
10	Pérdida de integridad de la información	Extremo	Satisfactoria
11	No disponibilidad de la información	Extremo	Satisfactoria
12	Inadecuada gestión de problemas, incidentes y eventos	Extremo	Satisfactoria
13	Afectaciones de instalaciones críticas por desastres naturales y/o ataques físicos	Extremo	Excelente
14	Espacio físico insuficiente en el centro de datos subcontratado	Alto	Nula
15	Incumplimiento de normativas relacionadas con regulaciones y leyes	Extremo	Excelente
16	Dificultad para monitorear y verificar la administración sobre el ambiente físico subcontratado	Alto	Nula
17	Información documentada no refleja la arquitectura actual	Extremo	Satisfactoria

(Unidad de Riesgo Corporativo COOPEALIANZA R.L, 2015)

Al contar con los resultados del riesgo inherente y los resultados de la evaluación de los controles, se tiene los insumos para obtener el grado de valoración del riesgo al considerar el efecto de los controles existentes y determinar la respectiva cobertura de riesgo. Recordemos que dicha valoración se realiza por medio de la encuesta realizada a los participantes y como resultado de la fórmula de la figura 10, donde la madurez es el porcentaje de cobertura o mitigación de los controles existentes y la valoración máxima tiene un valor de 5.

$$Valoración\ Riesgo\ Residual = \frac{(Probabilidad \times Impacto) \times (1 - Madurez)}{Valoración\ Máxima}$$

Figura 10 Fórmula Valoración de riesgo residual (Unidad de Riesgo Corporativo COOPEALIANZA R.L, 2015)

Al realizar la valoración del riesgo residual para cada riesgo, se obtiene los resultados del cuadro 20.

Cuadro 20 Resultado Riesgo Inherente y Efecto de los Controles (Riesgo Residual)

		Riesgo Inherente Resultado de la Encuesta			Riesgo Residual Resultado Encuesta Efecto de Controles
No.	**Riesgo**	**Probabilidad de Ocurrencia**	**Impacto**	**Criticidad**	**Criticidad**
1	Daño en los equipos de la plataforma tecnológica	Probable (1 a 3 meses)	Crítico	Extremo	Moderado
2	Inadecuada migración y/o traslado de datos al centro de datos	Casi cierta (1 al mes)	Crítico	Extremo	Moderado
3	Inadecuada gestión de cambios	Probable (1 a 3 meses)	Moderado	Alto	Bajo
4	Cierre de operaciones del proveedor del centro de datos	Remota (1 al año)	Crítico	Alto	Muy Bajo
5	Personal no calificado del proveedor del centro de datos	Probable (1 a 3 meses)	Significativo	Extremo	Moderado
6	Inadecuado monitoreo del desempeño del proveedor del centro de datos	Casi cierta (1 al mes)	Significativo	Extremo	Moderado
7	Operaciones ilícitas o fraudulentas desarrolladas por personal propio o externo	Casi cierta (1 al mes)	Crítico	Extremo	Moderado
8	Imposibilidad de recuperarse ante un desastre en el centro de datos	Casi cierta (1 al mes)	Crítico	Extremo	Bajo
9	Divulgación de información confidencial	Casi cierta (1 al mes)	Crítico	Extremo	Moderado
10	Pérdida de integridad de la información	Probable (1 a 3 meses)	Crítico	Extremo	Moderado
11	No disponibilidad de la información	Probable (1 a 3 meses)	Crítico	Extremo	Moderado
12	Inadecuada gestión de problemas, incidentes y eventos	Probable (1 a 3 meses)	Significativo	Extremo	Moderado
13	Afectaciones de instalaciones críticas por	Posible (3 a 5 meses)	Crítico	Extremo	Bajo

	desastres naturales y/o ataques físicos				
14	Espacio físico insuficiente en el centro de datos subcontratado	Posible (3 a 5 meses)	Significativo	Alto	Extremo
15	Incumplimiento de normativas relacionadas con regulaciones y leyes	Casi cierta (1 al mes)	Significativo	Extremo	Bajo
16	Dificultad para monitorear y verificar la administración sobre el ambiente físico subcontratado	Probable (1 a 3 meses)	Moderado	Alto	Extremo
17	Información documentada no refleja la arquitectura actual	Casi cierta (1 al mes)	Moderado	Extremo	Moderado

(Unidad de Riesgo Corporativo COOPEALIANZA R.L, 2015)

Para un mejor entendimiento del efecto de los controles sobre el riesgo inherente en la figura 11 se muestra un comparativo para cada riesgo y que permite identificar el nivel de riesgo residual.

No.	Riesgo	Riesgo Inherente		Riesgo Residual
1	Daño en los equipos de la plataforma tecnológica	Extremo	→ → →	Moderado
2	Inadecuada migración y/o traslado de datos al centro de datos.	Extremo	→ → →	Moderado
3	Inadecuada gestión de cambios	Alto	→ → →	Bajo
4	Cierre de operaciones del proveedor del centro de datos	Alto	→ → →	Muy Bajo
5	Personal no calificado del proveedor del centro de datos	Extremo	→ → →	Moderado
6	Inadecuado monitoreo del desempeño del proveedor del centro de datos	Extremo	→ → →	Moderado
7	Operaciones ilícitas o fraudulentas desarrolladas por personal propio o externo	Extremo	→ → →	Moderado
8	Imposibilidad de recuperarse ante un desastre en el centro de datos	Extremo	→ → →	Bajo
9	Divulgación de información confidencial	Extremo	→ → →	Moderado
10	Pérdida de integridad de la información	Extremo	→ → →	Moderado
11	No disponibilidad de la información	Extremo	→ → →	Moderado
12	Inadecuada gestión de problemas, incidentes y eventos	Extremo	→ → →	Moderado
13	Afectaciones de instalaciones críticas por desastres naturales y/o ataques físicos	Extremo	→ → →	Bajo
14	Espacio físico insuficiente en el centro de datos subcontratado	Alto	→ → →	Extremo
15	Incumplimiento de normativas relacionadas con regulaciones y leyes	Extremo	→ → →	Bajo
16	Dificultad para monitorear y verificar la administración sobre el ambiente físico subcor	Alto	→ → →	Extremo
17	Información documentada no refleja la arquitectura actual	Extremo	→ → →	Moderado

Figura 11 Comparativo Riesgo Inherente / Riesgo Residual (Unidad de Riesgo Corporativo COOPEALIANZA R.L, 2015)

El nivel de riesgo residual puede comprenderse de una mejor manera al observar la figura 12, donde se muestra la matriz de exposición del riesgo residual.

	Madurez	Excelente	Satisfactoria	Adecuada	Débil	Nula
Riesgo Inherente	Valor	1	2	3	4	5
Extremo	5	Bajo	Moderado	Alto	Extremo	Extremo
Alto	4	Muy bajo	Bajo	Moderado	Alto	Extremo
Moderado	3	Muy bajo	Bajo	Bajo	Moderado	Alto
Bajo	2	Muy bajo	Muy bajo	Bajo	Bajo	Moderado
Muy Bajo	1	Muy bajo	Muy bajo	Muy bajo	Muy bajo	Bajo

Figura 12 Exposición del riesgo (Residual) (Unidad de Riesgo Corporativo COOPEALIANZA R.L, 2015)

Los niveles de riesgo establecidos poseen un valor de criticidad y una descripción tal y como se muestra en la figura 13.

NIVEL DE RIESGO	PUNTAJE DE CRITICIDAD	DESCRIPCIÓN
EXTREMO	5	Cuando su materialización puede afectar severamente el producto o servicio, se puedan perder oportunidades importantes de negocio o causar un daño grave a la imagen de la institución ante el público, socios o autoridades (incluyendo entes reguladores), así como verse afectada severamente su operatividad, de tal manera que se exponga a la entidad a pérdidas cuantiosas o sanciones legales y administrativas.
ALTO	4	Cuando la materialización puede afectar el producto o servicio, se puedan perder oportunidades de negocio y desmejorar la imagen de la institución, con lo cual podrían perderse clientes o verse afectada su operatividad en forma significativa.
MODERADO	3	Cuando su materialización represente un peligro potencial de impacto estrictamente a lo interno de la entidad; aunque no significativo para los clientes, socios o entes reguladores.
BAJO	2	Cuando su materialización acarrea consecuencias de baja importancia para la entidad
MUY BAJO	1	Cuando su materialización no acarrea consecuencias significativas para la entidad.

Figura 13 Nivel del Riesgo (Unidad de Riesgo Corporativo COOPEALIANZA R.L, 2015)

Al igual que el riesgo inherente y para una mejor comprensión, podemos visualizar cada uno de los riesgos de acuerdo a su identificador numérico en un mapa de calor de riesgo residual. La figura 14 nos muestra que los riesgos se ubican en niveles de criticidad “Extremo”, “Moderado” y “Bajo” considerando la cobertura de los controles existentes.

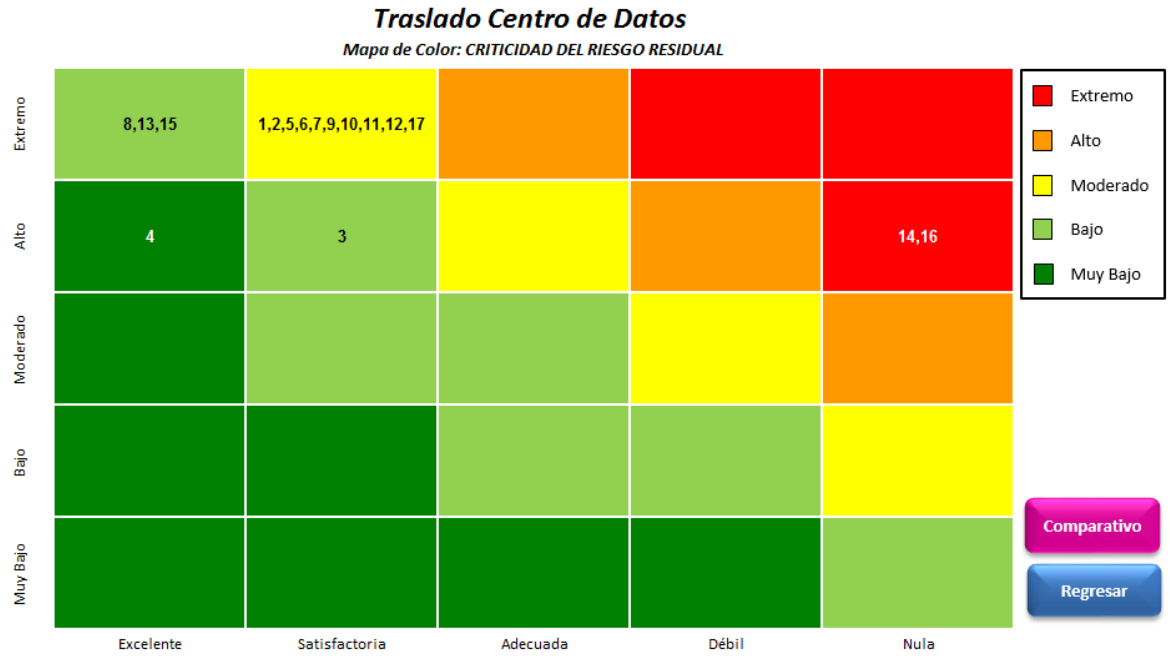


Figura 14 Mapa de Calor Riesgo Residual (Unidad de Riesgo Corporativo COOPEALIANZA R.L, 2015)

Al contar con los resultados del análisis de riesgo, se puede continuar con la siguiente etapa del proceso de gestión de riesgos, denominada “Evaluación de riesgo”, donde el principal objetivo es determinar los riesgos que necesitan tratamiento y/o prioridades de tratamiento.

4.2.4 Evaluación de riesgo

Para la priorización de cualquier medida o tratamiento del riesgo, la cooperativa ha establecido el nivel de tolerancia del riesgo y el apetito al riesgo, lo anterior por medio de la Unidad de Riesgo Corporativa de COOPEALIANZA R.L; con respecto al nivel de tolerancia el indicador de exposición al riesgo residual será el comprendido en “Moderado”, “Bajo” y “Muy Bajo”.

Por otra parte el apetito al riesgo determina los parámetros de aceptabilidad de riesgos, los cuales con criterios que permiten determinar si un nivel de riesgo especifico se ubica dentro de la categoría de nivel de riesgo aceptable o no. La

figura 15 nos muestra de una manera gráfica (mapa de calor) los niveles de riesgo aceptables o el apetito al riesgo que ha establecido la cooperativa.

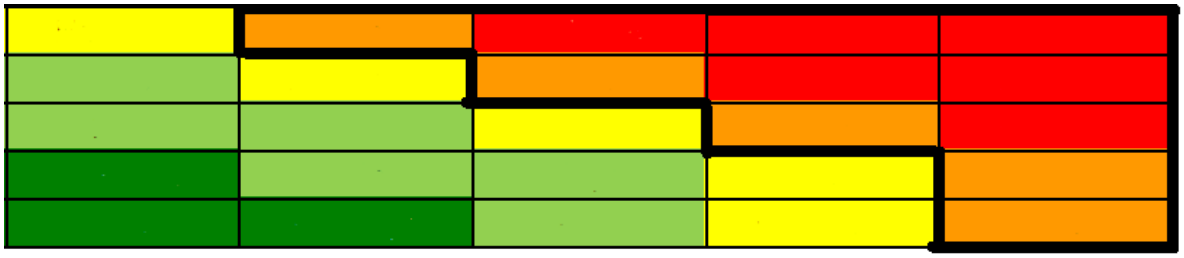


Figura 15 Mapa de calor / Apetito al riesgo (Unidad de Riesgo Corporativo COOPEALIANZA R.L, 2015)

El nivel de riesgo aceptable se ubica en el mapa de calor de la figura 15 en la zona sin demarcar (Verde Oscuro, Verde Claro, Amarillo). Los riesgos que se ubican en dicha zona no están sujetos a planes o acciones de mitigación; sin embargo deben seguir siendo mitigados mediante las medidas de control existentes y una vez se hayan atendido los riesgos críticos o con mayor prioridad (zona demarcada Naranja y Rojo), podrá mejorarse los controles existentes o bien proponerse nuevos controles.

Por el contrario, si el nivel de riesgo obtenido se ubica en el cuadrante seleccionado en la figura 15 con color negro (zona demarcada naranja y rojo), no se considera un nivel de riesgo aceptable y por lo tanto dichos riesgos deben ser administrados.

El responsable del tratamiento de un riesgo, deberá indicar si el nivel de riesgo se asume o bien se aplica otra medida de tratamiento, en caso de la medida de “Asumir el riesgo”; debe considerar y justificar algunos aspectos tales como el costo beneficio y/o la incapacidad de ejecutar algún plan o acción de mitigación, donde su implementación vaya en contra del interés de la cooperativa o por escasez de recursos para la administración y/o ejecución de la medida.

El nivel de tolerancia y el apetito de riesgo fueron establecidos con base al criterio técnico y análisis de la Unidad de Riesgos Corporativa de COOPEALIANZA R.L, en conjunto con el Comité de Riesgos Corporativo, dichos aspectos tienen revisiones y aprobaciones anuales.

Una vez establecidos los aspectos y/o criterios de priorización para la atención de los riesgos, se puede continuar con la siguiente etapa del proceso de gestión de riesgos, denominada tratamiento del riesgo.

4.2.5 Tratamiento del riesgo

Con respecto a esta etapa del proceso de gestión del riesgo, el grupo interdisciplinario se reúne y propone en conjunto medidas de atención al riesgo, sin embargo como primer paso debe establecer el tipo de tratamiento para los riesgos resultado del análisis y evaluación del riesgo. En el cuadro 21 se muestra el detalle de los riesgos y la medida a adoptar.

Cuadro 21 Riesgo Inherente / Riesgo Residual / Medida de Tratamiento del Riesgo

		Riesgo Inherente Resultado de la Encuesta			Riesgo Residual	Medida a Adoptar
No.	**Riesgo**	**Probabilidad de Ocurrencia**	**Impacto**	**Criticidad**	**Criticidad**	
1	Daño en los equipos de la plataforma tecnológica	Probable (1 a 3 meses)	Crítico	Extremo	Moderado	Asumir el riesgo
2	Inadecuada migración y/o traslado de datos al centro de datos	Casi cierta (1 al mes)	Crítico	Extremo	Moderado	Asumir el riesgo
3	Inadecuada gestión de cambios	Probable (1 a 3 meses)	Moderado	Alto	Bajo	Asumir el riesgo
4	Cierre de operaciones del proveedor del centro de datos	Remota (1 al año)	Crítico	Alto	Muy Bajo	Asumir el riesgo
5	Personal no calificado del proveedor del centro de datos	Probable (1 a 3 meses)	Significativo	Extremo	Moderado	Asumir el riesgo
6	Inadecuado monitoreo del desempeño del proveedor del centro de datos	Casi cierta (1 al mes)	Significativo	Extremo	Moderado	Asumir el riesgo
7	Operaciones ilícitas o fraudulentas desarrolladas por personal propio o externo	Casi cierta (1 al mes)	Crítico	Extremo	Moderado	Asumir el riesgo

8	Imposibilidad de recuperarse ante un desastre en el centro de datos	Casi cierta (1 al mes)	Crítico	Extremo	Bajo	Asumir el riesgo
9	Divulgación de información confidencial	Casi cierta (1 al mes)	Crítico	Extremo	Moderado	Asumir el riesgo
10	Pérdida de integridad de la información	Probable (1 a 3 meses)	Crítico	Extremo	Moderado	Asumir el riesgo
11	No disponibilidad de la información	Probable (1 a 3 meses)	Crítico	Extremo	Moderado	Asumir el riesgo
12	Inadecuada gestión de problemas, incidentes y eventos	Probable (1 a 3 meses)	Significativo	Extremo	Moderado	Asumir el riesgo
13	Afectaciones de instalaciones críticas por desastres naturales y/o ataques físicos	Posible (3 a 5 meses)	Crítico	Extremo	Bajo	Asumir el riesgo
14	Espacio físico insuficiente en el centro de datos subcontratado	Posible (3 a 5 meses)	Significativo	Alto	Extremo	Reducir el riesgo
15	Incumplimiento de normativas relacionadas con regulaciones y leyes	Casi cierta (1 al mes)	Significativo	Extremo	Bajo	Asumir el riesgo
16	Dificultad para monitorear y verificar la administración sobre el ambiente físico subcontratado	Probable (1 a 3 meses)	Moderado	Alto	Extremo	Reducir el riesgo
17	Información documentada no refleja la arquitectura actual	Casi cierta (1 al mes)	Moderado	Extremo	Moderado	Asumir el riesgo

(Unidad de Riesgo Corporativo COOPEALIANZA R.L, 2015)

Como se ha indicado, para continuar con el proceso de gestión del riesgo, es necesario llevar a cabo planes o acciones mitigadoras de riesgos. En el cuadro 22 se muestra los elementos necesarios que debe contener el tratamiento del riesgo y para aquellos riesgos fuera del apetito al riesgo de la cooperativa.

Cuadro 22 Acciones de Mitigación del Riesgo Residual Priorizado

Riesgo	**Espacio físico insuficiente en el centro de datos subcontratado**			
Plan o acción mitigadora	**Responsable**	**Fecha máxima de cumplimiento**	**Resultado esperado**	**Análisis Costo / Beneficio**
Prever un 25% de crecimiento extra en relación a un gabinete de 48 Unidades de Rack en el Centro de Datos sub contratado con respecto a la capacidad inicial instalada.	Gerencia Tecnologías de Información	31-12-2017	Contratación inicial del espacio de gabinete hasta por un 25% de crecimiento en el nuevo centro de datos sub contratado.	Al no prever espacio adicional de crecimiento en el mismo centro de datos eventualmente puede ocurrir que se deba de contratar gabinetes en otro centro de datos lo que significaría invertir en enlaces de comunicación primarios

				y secundarios que rondarían mensualidades de hasta $6 000.00 ($72 000.00 anuales), además invertir en nueva infraestructura de telecomunicación y seguridad (Enrutador, Conmutador, Prevención de Intrusos, Cortafuegos) hasta por un monto inicial de inversión de $100000.00. Por el contrario al contratar un gabinete completo en el mismo centro de datos rondaría $36 000.00 anuales, este último caso sería el peor escenario en el mismo centro de datos.
Incorporar en las actualizaciones anuales del plan de capacidad y desempeño, un apartado en dicho documento sobre las capacidades de crecimiento en los Centro de Datos propios y sub contratados.	Responsable Infraestructura y Redes	31-03-2016	Mantener información anual sobre las capacidades de crecimiento disponibles en los centros de datos propios y sub contratados	Se obtiene como beneficio prever la disponibilidad de espacio para crecimiento en los centro de datos propios y sub contratados contra un costo muy bajo de esfuerzo (8 horas) de un funcionario de TI que realice las inspecciones necesarias y actualice el plan.
Incorporar en el formato de casos de negocio, un nuevo apartado con el mismo contenido que el formato “Arquitectura de la Solución” del Plan de Gestión Integral del Proyecto donde se detalle las unidades de racks o de gabinete requeridas en los centros de datos, en caso de ser necesario o requerido para el proyecto respectivo.	Responsable Sistemas de Información	31-03-2016	Los dueños de procesos presenten dentro de los casos de negocio la información requerida para que TI pueda prever el posible crecimiento en la utilización de las unidades de rack o de gabinete en los centros de datos propios y sub contratados.	Como beneficio se obtiene de manera anticipada los requerimientos de crecimiento en los centros de datos, de modo que la cooperativa pueda prever el espacio requerido y los costos asociados, contra un costo muy bajo de esfuerzo (6 horas) de un funcionario que realice los cambios al documento.
Incorporar en el formulario donde se registra la visita en	Responsable de Proceso	31-03-2016	Mantener información	Se obtiene como beneficio el poder

sitio al proveedor que se realiza en el proceso de Gestión de Proveedores aspectos de proyecciones futuras y disponibilidad de espacio en el Centros de Datos de acuerdo a la Metodología ME-SG-GPP-001 “Administración de los Servicios de Terceros”, punto 5.6 “Monitorear el Desempeño de los Proveedores”	SUGEF 14-09 DS2		actualizada del proveedor sobre sus capacidades actuales y sobre sus planes futuros de crecimiento.	contar con la información de capacidad actual y planes futuros de crecimiento para la toma de decisiones y para eventuales contrataciones en nuevos centros de datos, el costo sería bastante bajo ya que sería el tiempo destinado para la modificación del formulario el cual se estima en 3 horas.
Riesgo	**Dificultad para monitorear y verificar la administración sobre el ambiente físico subcontratado**			
Implementar una solución de monitoreo y/o vigilancia gestionada por la cooperativa por medio de una cámara especial CCTV, con sensores de aperturas de puertas del gabinete, cambios de temperatura, humedad, notificaciones y que el seguimiento y el monitoreo se incorpore en los procedimientos establecidos para la central de monitoreo de CCTV de la cooperativa.	Responsable de Proceso SUGEF 14-09 DS12	31-12-2017	Cámara instalada y en operación en el centro de datos sub contratado.	Con un costo estimado de $3 000.00 se tiene como beneficio el poder monitorear y detectar posibles cambios ambientales y de acceso a los gabinetes que podrían afectar la infraestructura instalada de la cooperativa en el centro de datos sub contratado.
Incorporar en el formulario en donde se registra la visita en sitio al proveedor que se realiza en el proceso de Gestión de Proveedores, aspectos de certificaciones y auditorias, de acuerdo a la Metodología ME-SG-GPP-001 “Administración de los Servicios de Terceros”, punto 5.6 “Monitorear el Desempeño de los Proveedores”	Responsable de Proceso SUGEF 14-09 DS2	31-03-2016	Conocer y analizar las certificaciones y auditorias con las que cuenta el centro de datos evaluado.	Como beneficio se obtiene el poder contar con información de certificaciones y auditorias con las que cuenta el centro de datos sub contratado, por un costo bajo y que actualmente ya se está asumiendo en la visita de evaluación anual que se realiza desde el proceso de gestión de proveedores.
Incorporar cláusulas de sanciones y/o multas en la contratación por incumplimiento de los acuerdos de nivel de servicio pactados (SLA) en cuanto a eventos que impacten la disponibilidad del servicio.	Gerencia Tecnologías de Información	31-12-2017	Contrato con la incorporación de cláusula con multas y/o sanciones que contribuyan con los intereses de la Cooperativa	Beneficio contar con cláusulas que protejan los intereses de la Cooperativa en la contracción del nuevo centro de datos contra un costo estimado de 8 horas en la redacción de las cláusulas en conjunto con la unidad legal.

(Unidad de Riesgo Corporativo COOPEALIANZA R.L, 2015)

El cuadro anterior establece la descripción del riesgo a mitigar, un identificador numérico para la acción mitigadora, la descripción del plan y/o acción mitigadora, el responsable del cumplimiento de la misma, así como la fecha de compromiso máxima para tener implementada la acción propuesta, una descripción del resultado esperado y finalmente un pequeño análisis de costo/beneficio.

4.3 Recomendaciones

A continuación se proporcionan algunas recomendaciones como resultado del análisis financiero y de riesgo para la alta administración de COOPEALIANZA R.L para que sean parte de la decisión estratégica en función de la operación del nuevo centro de datos:

- Se recomienda a la administración de COOPEALIANZA R.L desde el punto de vista financiero optar por la subcontratación del centro de datos ya que esta alternativa resulta en menores requerimientos de inversión y patrimonio, permitiendo el uso de los recursos escasos al giro propio del negocio que es la intermediación financiera.
- Se recomienda evaluar los controles para los diez riesgos que fueron catalogados con el nivel de criticidad de riesgo residual “Moderado”; si bien es cierto estos riesgos se ubican en la zona donde no están sujetos a planes o acciones de mitigación de acuerdo a la metodología utilizada, es importante que la administración de la cooperativa continúe reforzando dichos controles o bien evalúe la implementación de nuevos controles para que dichos riesgos no se movilicen eventualmente a zonas de mayor criticidad.
- Se recomienda analizar el escenario alternativo de construir el nuevo centro de datos en alguna de las sucursales donde la cooperativa es dueña del terreno y/o del inmueble, se recomienda prestar especial atención a la sucursal de Ciudad Colón por las facilidades de acceso, cercanía con

aeropuertos, servicios de telecomunicaciones, por mencionar algunos elementos importantes.

- En caso de contratar el procesamiento y almacenamiento crítico a un tercero, se recomienda llevar a la operación los nuevos controles propuestos en este estudio, es decir los 7 controles para los riesgos “Espacio físico insuficiente en el centro de datos subcontratado” y “Dificultad para monitorear y verificar la administración sobre el ambiente físico subcontratado”.

5 CONCLUSIONES

- Como resultado de los análisis financieros efectuados en este estudio, tanto la construcción del nuevo centro de datos como la subcontratación resultan financieramente viables, aunque la alternativa de subcontratación de un centro de datos resulta en menores requerimientos de inversión y patrimonio, permitiendo el uso de los recursos escasos al giro propio del negocio, que es la intermediación financiera.
- Debido a la naturaliza del proyecto de construcción de un nuevo centro de datos, resulta difícil identificar beneficios o ingresos directos que sirvan como insumos a utilizar en métodos financieros como el VAN y el TIR, por cuanto fue necesario utilizar un metodología alternativa que permita cuantificar los mismos, en virtud de la trascendencia de la necesidad de una alta disponibilidad del servicio para un centro de datos.
- En la alternativa de subcontratar el centro de datos, los principales costos están asociados a las categorías de Telecomunicaciones y Arquitectura, los cuales son variables, pudiendo disminuir por aspectos de competencia entre proveedores y optimización de recursos al utilizar nuevas tecnologías como la virtualización o consolidación de servidores. Por otra parte estos costos podrían incrementar en función del crecimiento de las necesidades requeridas por parte de la cooperativa.

- El proceso de gestión de riesgos aplicado a la actividad de trasladar el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica contribuye a mejorar la confianza de los interesados de la cooperativa (Asociados, Ente Supervisor, Auditoría Interna, Auditoría Externa, Consejo de Administración y Administración) ante una decisión de este tipo.
- COOPEALIANZA R.L al ser una entidad financiera supervisada por la SUGEF, debe sustentar sus decisiones de inversión en tecnología donde se tome en cuenta información crítica y/o sensible de clientes financieros desde un enfoque no sólo financiero sino que además debe complementarse con el proceso de gestión de riesgos.
- COOPEALIANZA R.L muestra una importante inversión financiera, de recurso humano y de esfuerzo debido a la adopción de buenas prácticas internacionales como el COBIT, lo anterior debido a los resultados de la efectividad de los controles de los procesos AI3 Adquirir y mantener la infraestructura tecnológica, AI6 Administrar cambios, DS2 Administrar servicios de terceros, DS4 Garantizar la continuidad del servicio, DS5 Garantizar la seguridad de los sistemas, DS9 Administrar la configuración, DS10 Administrar los problemas, DS12 Administrar el ambiente físico y ME3 Monitorear y evaluar el control interno.
- Al aplicarse el proceso de gestión de riesgos a la actividad de trasladar el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica surgen costos producto de los nuevos controles resultantes de las acciones de tratamiento identificadas para los riesgos fuera del apetito al riesgo de la cooperativa.
- La experiencia en la gestión del riesgo y la implementación de controles alrededor del actual centro de datos alterno de COOPEALIANZA R.L, ha permitido una importante evolución de la cooperativa en la gestión y control de un centro de datos que no es propio y del seguimiento y control del desempeño del proveedor que ofrece este tipo de servicios.

- Al aplicarse el proceso de gestión de riesgos a la actividad de trasladar el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica, se logra identificar de una manera justificada la asignación y utilización de recursos para el tratamiento del riesgo.
- La aplicación del proceso de gestión de riesgos a la actividad de trasladar el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica, fortalece la capacidad de resistencia ante amenazas y vulnerabilidades propias del contexto interno y externo de la cooperativa.

6 RECOMENDACIONES

- Se recomienda que Tecnologías de Información de COOPEALIANZA R.L realice el proceso de gestión de riesgos a sus centros de datos propios y contratados al menos una vez al año, lo anterior con el objetivo de monitorear y dar seguimiento a la efectividad y calidad de los controles implementados y que dichos riesgos se mantengan dentro del apetito de riesgo definido por la cooperativa.
- Se recomienda a la administración de COOPEALIANZA R.L realizar un análisis financiero adicional que incorpore los costos al construir un nuevo centro de datos en la sucursal de Ciudad Colón versus los costos de contratar el centro de datos a un tercero resultado de este estudio, lo anterior con el objetivo que la cooperativa analice la conveniencia de no transferir los riesgos de procesar y almacenar la información crítica de la cooperativa hacia un tercero además de analizar los costos de mantenimiento debido a la cercanía con el gran área metropolitana.
- Se recomienda a la administración de COOPEALIANZA R.L que en caso de escoger la opción de subcontratar el centro de datos, identifique e incorpore de forma más detallada todos los costos involucrados tanto directos como

indirectos incluyendo aquellos que se relacionan con la administración y supervisión del desempeño de los servicios y la relación con el proveedor.

- Se recomienda que Tecnologías de Información de COOPEALIANZA R.L realice una evaluación de alternativas de procesamiento y almacenamiento en la nube, considerando soluciones en la nube de proveedores de renombre como Microsoft y Oracle, lo anterior para evaluar los riesgos y costos de dichas alternativas con respecto a los análisis financieros y de riesgo realizados en este estudio.
- Se recomienda a la Gerencia Financiera de COOPEALIANZA definir y documentar formalmente la contribución que proporciona los niveles de disponibilidad de los servicios financieros que ofrece la cooperativa a través de su centro de datos con respecto a los ingresos financieros de genera la cooperativa.
- Se recomienda a la administración de COOPEALIANZA R.L proponer un proyecto conjunto a otras cooperativas para construir un centro de datos certificado, lo anterior con el objetivo de lograr economías de escala y reducir los riesgos de trasladar el procesamiento y almacenamiento de la información a un tercero.
- Se recomienda a la administración de COOPEALIANZA R.L subcontratar un centro de datos con el nivel de certificación *TIER III* de acuerdo a la categorización que establece el *UpTime Institute*.
- Se recomienda a Tecnologías de Información de COOPEALIANZA R.L realizar un análisis detallado de la oferta de servicios de centros de datos que se ofrece en Costa Rica, donde no sólo se considere el costo mensual sino que además se considere aspectos de facilidades de acceso o varias rutas de acceso, cercanía con aeropuertos, redundancia en servicios de telecomunicaciones, agua y electricidad, bajo índice de criminalidad, por mencionar algunos elementos importantes que reducen aún más el riesgo de mantener y/o procesar la información crítica con un tercero.
- Se recomienda a Tecnologías de Información de COOPEALIANZA R.L que realice un análisis de tendencias en cuanto a la evolución de los centros de

datos al menos una vez cada tres años con el objetivo de gestionar el riesgo de la información y servicios críticos de la cooperativa y además con el objetivo de reducir costos.

- Se recomienda a la Gerencia Financiera de COOPEALIANZA R.L utilizar un método complementario como el cálculo del retorno de inversión (ROI) o años de recuperación de la inversión para complementar los análisis financieros del VAN y el TIR, a efectos de facilitar y mejorar la toma de decisiones para los proyectos de inversión.

7 BIBLIOGRAFIA

IT Governance Institute. (2007). *COBIT 4.1*. United States of America: IT Governance Institute.

Aguero, S. (14 de Octubre de 2015). *Revista ITNow*. Obtenido de Revista ITNow: http://revistaitnow.com/costa-rica-mantiene-segundo-lugar-data-centers/

ANSI/TIA-942. (2005). Telecommunications Infraestructure Standard for Data Centers. *Telecommunications Infraestructure Standard for Data Centers*.

Astúa Chavarría, A. (Julio de 2010). Modelo Integral para el diseño de facilidades electromecánicas en centros de datos. San José, Costa Rica: Universidad de Costa Rica Facultad de Ingeniería Escuela de Ingeniería Eléctrica.

Banco de Pagos Internacionales. (20 de Marzo de 2012). *Sitio Web del Banco de Pagos Internacionales.* Recuperado el 16 de Agosto de 2015, de http://www.bis.org/publ/bcbs213_es.pdf

Campos, Y. (2010). Administración de Riesgos en las Tecnologías de Información. México: UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO.

Casia, M. (1 de Octubre de 2006). EVALUACIÓN FINANCIERA-ECONÓMICA DE UN PROYECTO PRIVADO DE AGUA POTABLE EN LA ALDEA CHOCHAL - MUNICIPIO DE CHIANTLA, DEPARTAMENTO DE HUEHUETENANGO. Guatemala.

Chacón, K. (14 de Octubre de 2015). *El Financiero*. Obtenido de El Financiero: http://www.elfinancierocr.com/tecnologia/Podra-Costa-Rica-Silicon-Valley_0_794920505.html

COOPEALIANZA R.L. (11 de Diciembre de 2014). Plan Estratégico de COOPEALIANZA R.L 2015 - 2017. San Isidro de El General, San Josê, Costa Rica: Comité de Planificación COOPEALIANZA R.L.

COOPEALIANZA R.L. (s.f.). *Sitio Web de COOPEALIANZA R.L*. (COOPEALIANZA R.L) Recuperado el 16 de Agosto de 2015, de www.coopealianza.fi.cr

Cordero, C. (15 de Octubre de 2015). *El Financiero*. Obtenido de El Financiero: http://www.elfinancierocr.com/tecnologia/Datacenter_Consultores-Orotina-Comex-Cinde-Micitt_0_792520761.html

Financiero, C. R. (24 de Noviembre de 2015). Análisis Financiero Subcontratar Centro de Datos. (N. R. Madrigal, Entrevistador)

González, P. (Julio de 2010). METODOLOGÍA PARA OPTIMIZAR EL MANEJO DE ENERGÍA EN DATA CENTERS Y DISEÑO DE UN SISTEMA DE MONITOREO ENERGÉTICO PARA EL DATA CENTER DE GRUPO ELECTROTÉCNICA. San José, Costa Rica: Universidad de Costa Rica Facultad de Ingeniería Escuela de Ingeniería Eléctrica.

International Organization for Standardization. (2009). *Gestión de Riesgos - Principios y Guías.* Suiza: ISO.

Muñoz Razo, C. (1998). *Cómo elaborar y asesorar una investigación de tesis.* Pearson Educación.

Ramírez, J. (2011). *Cómo diseñar una investigación académica* (1a Edición ed.). Heredia, Heredia, Costa Rica: Montes de María Editores.

Salas, T. (2001). *Análisis y Diagnóstico Financiero.* San José: Guayacán.

Sapag, N. (2001). *Evaluación De Proyectos De Inversión En La Empresa.* Buenos Aires, Argentina: Pearson Education.

Superintendencia General de Entidades Financieras de Costa Rica. (s.f.). *Sitio Web de la Superintendencia General de Entidades Financieras de Costa Rica*. Recuperado el 16 de Agosto de 2015, de www.sugef.fi.cr

Unidad de Riesgo Corporativo COOPEALIANZA R.L. (27 de Abri de 2015). Metodología para la Gestión del Riesgo Operativo y Tecnologías de Información en el Grupo Financiero Alianza. San Isidro de El General, San José, Costa Rica.

8 ANEXOS

Anexo 1: Acta de constitución, Cronograma: Plan de trabajo

ACTA DE CONSTITUCIÓN DEL PROYECTO FINAL DE GRADUACIÓN			
Nombre completo del estudiante:	***NORBERTO LEE RODRIGUEZ MADRIGAL***		
Nombre de la carrera:	***Maestría en Tecnología de la Información***	***Generación***	***04***
Título del proyecto	Análisis Financiero y de Riesgo al trasladar el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica.		
Fecha de inicio del proyecto:	***23-09-2015***	***Fecha tentativa de finalización del proyecto:***	***06-01-2016***
Justificación del proyecto	El tema de este proyecto se elige ya que para la cooperativa de ahorro y crédito y servicios múltiples costarricense COOPEALIANZA R.L se vuelve crucialmente importante contar con un análisis financiero y de riesgo que le permita gestionar de una manera eficiente los recursos con los que cuenta la cooperativa y con el objetivo de contar con una base sólida para decidir entre volver a invertir en un centro de datos de procesamiento crítico propio, o bien, aprovechar las alternativas existentes y en constante evolución por parte de empresas dedicadas al negocio de centros de datos certificados dentro del territorio costarricense. Las inversiones realizadas hace más de 10 años por COOPEALIANZA R.L en su propio centro de datos ubicado en el cantón de Pérez Zeledón, significaron inversiones cercanas a los dos millones y medio de dólares, esto a su vez significó importantes inversiones alrededor de los costos		

	totales de propiedad y por el hecho de mantener en operación un centro de datos de procesamiento crítico. Al entrar en operación el centro de datos en el año 2006 y con el gran inconveniente de encontrarse ubicado a una distancia de más de 136 kilómetros de la capital, los tiempos de atención por parte de los proveedores para atender averías, realizar mantenimientos preventivos y correctivos no logran ser inferiores a las seis horas; casi diez años después y para una empresa del tamaño de COOPEALIANZA R.L, dichos tiempos de atención en caso de producirse un incidente o una contingencia en el centro de datos eventualmente podría producir importantes pérdidas financieras y afectación de la imagen. Adicional a lo anterior la cooperativa tuvo que incurrir en mantener componentes bastante complejos y que requieren de un monitoreo constante a fin de asegurar su operación continua en el tiempo, componentes tales como: planta eléctrica, sistemas de suministro eléctrico ininterrumpido, aires acondicionados de precisión, sistemas de monitoreo, sistemas de prevención de intrusos y alarmas contra robo, sistemas de prevención temprana del fuego, instalación de gabinetes de protección de equipamiento, por mencionar algunos. Lo anterior significó además que algunos de dichos componentes tuviesen que duplicarse a fin de aumentar los niveles de disponibilidad y que ante cualquier incidente o falla en un componente, el otro soportara la operación mientras tanto se corregía el problema. Como puede notarse tanto la cooperativa como su personal debieron asumir inversiones, roles y responsabilidades distintas al giro de negocio de COOPEALIANZA R.L. Para una entidad financiera como COOPELIANZA R.L, donde su principal negocio es la colocación de crédito, el ahorro y los servicios financieros múltiples se convierte en una importante decisión estratégica no sólo redirigir recursos financieros hacia su principal negocio sino que además se vuelve relevante que el personal de Tecnologías de Información y otras áreas de la cooperativa se enfoquen más al giro de negocio principal y traslade la operativa actual de mantener el centro de datos hacia una empresa especializada en dicho campo, con lo anterior contribuir con el negocio de la cooperativa en gestionar de una manera eficiente y razonable los recursos de Tecnologías de Información. Por otra parte la alta administración definió dentro de sus estrategias de largo plazo la adopción paulatina pero constante de subcontratar aquellos servicios que generen valor al negocio de la cooperativa y permitan contribuir con la rentabilidad de la misma.

	Para lo anterior la cooperativa estableció la siguiente creencia, que no sólo considera los negocios con nuestros clientes y asociados, sino que además considera todos aquellos negocios que se realizan con socios y proveedores, la creencia es “Nos gustan los buenos negocios” lo cual significa “Conocemos y comprendemos los servicios financieros ofrecidos y por eso buscamos nuevos negocios, pensando siempre en ganar - ganar”. En congruencia con la estrategia organizacional y la anterior creencia, Tecnologías de Información de COOPEALIANZA R.L estableció en su planificación estratégica para el periodo 2015 – 2017 la siguiente estrategia: “Crecer responsablemente en la contratación de servicios de terceros; otorgando tareas operativas especializadas a empresas de reconocida trayectoria, enfocando al personal de TI en las metas crucialmente importantes, generando altos niveles de disponibilidad, seguridad, desempeño y calidad en los servicios tecnológicos que se entregan, todo lo anterior alineado a las creencias de COOPEALIANZA R.L.”. Con el resultado del análisis financiero y de riesgo, la cooperativa tendrá un importante insumo para respaldar la decisión estratégica de invertir en un nuevo centro de datos o bien tener el respectivo sustento financiero y de riesgo, lo cual es de gran relevancia al ser una entidad financiera regulada por la Superintendencia General de Entidades Financieras (SUGEF) y para asegurarle a su base de asociados y de clientes de servicios financieros de calidad y que se encuentren siempre disponibles cuando son requeridos.
Diagnóstico e Identificación del Problema	En el año 2016 el centro de datos principal de COOPEALIANZA R.L ubicado en Pérez Zeledón, cumplirá más de diez años de haber entrado en operación, es así como todos los principales componentes de infraestructura, eléctricos, mecánicos, físicos y de seguridad de igual manera deben ser renovados; por otra parte la cooperativa requiere analizar si en lugar de construir un nuevo centro de datos más bien aprovecha las oportunidades que ofrecen los centros de datos subcontratados que cumplen con certificaciones tales como *COBIT*, *ITIL*, ISO 27000 y certificaciones *TIER* del *UpTime Institute*, por mencionar algunas. Como parte de la planificación estratégica de Tecnologías de Información de COOPEALIANZA R.L para el periodo 2015 – 2017, específicamente en el análisis de fortalezas, oportunidades, debilidades y amenazas (FODA) se identificó la siguiente oportunidad “Reducir los costos en infraestructura física en centros de datos y aprovechar los servicios con terceros en la nube y centros de datos subcontratados.”
Metodolo	Obtención de datos: para la obtención de datos con el objetivo de realizar el análisis financiero al construir un nuevo centro de datos y

gía	para la modalidad de subcontratarlo, se obtendrán datos de proveedores sobre los principales costos de los componentes y/o servicios que formen parte según la modalidad. Para la obtención de datos con el objetivo de realizar el análisis de riesgo al subcontratar un centro de datos a una empresa dedicada a este tipo de servicios, se estará realizando encuestas a un grupo interdisciplinario de COOPEALIANZA R.L a fin de obtener calificaciones de probabilidad e impacto sobre los riesgos identificados Anexo 2 “Riesgos identificados Actividad Subcontratar el Centro de Datos” tanto para el riesgo inherente como para el riesgo residual, lo anterior se estará realizando de acuerdo a las tablas de probabilidad e impacto del riesgo que se estarán incorporando en el estudio. Procesamiento de la información: una vez recolectados los datos sobre los principales costos alrededor de construir un nuevo centro de datos y de subcontratarlo, dichos datos se estarán incorporando a la técnica financiera del flujo de caja para el proyecto con capital propio como para el flujo de caja para el proyecto de subcontratación del centro de datos; además se aplicará técnicas financieras como el valor actual neto (VAN) y la tasa interna de retorno (TIR) para obtener un resultado financiero que permita a la cooperativa tomar decisiones adecuadas con respecto a la gestión de los recursos. Por otra parte y con respecto al análisis de riesgo, una vez realizadas las respectivas encuestas, los resultados de las mismas se estarán incorporando en un informe de evaluación del riesgo y mostrándose además en un mapa de calor de riesgo inherente y de riesgo residual. Interpretación de los datos: una vez realizado el flujo de caja para ambas modalidades, construir y subcontratar un centro de datos, y haberse aplicado las técnicas del VAN y el TIR; se obtendrán resultados financieros que van a permitir a la cooperativa contar con un cálculo y análisis de la viabilidad económica para ambas modalidades. Con respecto al análisis de riesgo, se podrá interpretar por medio del informe de evaluación del riesgo y el mapa de calor de riesgo inherente y de riesgo residual, los niveles de exposición de COOPEALIANZA R.L que se obtienen al subcontratar un centro de datos a una empresa dedicada a este tipo de servicios, lográndose observar además como los controles actuales minimizan los riesgos y además permitiendo identificar en cuales riesgos se requiere mejorar la efectividad del control o bien complementar

	con otros controles.
Alternativas, Ideas o Soluciones	*1.* Elaborar un análisis de los costos principales alrededor de un nuevo centro de datos para los próximo 10 años, donde se incluya los costos iniciales para establecer un nuevo centro de datos, incluyendo aspectos como los metros cuadrados requeridos, gabinetes requeridos para la protección y seguridad del equipamiento, los costos de enfriamiento, costos de suministro y respaldo eléctrico, costos de seguridad física y ambiental; así como los costos totales anuales estimados de propiedad. Lo anterior comparado con los costos de arrendamiento de al menos tres opciones de centros de datos subcontratados existentes en el mercado costarricense. *2.* Elaborar un análisis de riesgo con respecto a subcontratar el procesamiento crítico de la cooperativa a una empresa dedicada al negocio de alquiler o arrendamiento de centro de datos; dicho análisis se propone que se realice de acuerdo a lo que indica la norma australiana AS/NZs 4360 o ISO 31000. *3.* Identificar las alternativas tecnológicas complementarias que ofrecen las empresas que ofrecen centros de datos subcontratados, por ejemplo servicios de respaldo, de replicación de datos entre centros de datos, de seguridad, monitoreo de infraestructura por mencionar algunos. *4.* Elaborar un análisis de los aspectos operativos requeridos, por ejemplo personal especializado necesario, capacitación requerida de dicho personal, certificación en algún marco de servicio como por ejemplo ITIL, por mencionar algunos.
Selección de la mejor alternativa	Por un tema de tiempo se podría realizar únicamente las alternativas 1 y 2, es decir enfocarse en el análisis financiero y de riesgo, lo anterior se justifica ya que a la cooperativa lo que le interesa es mantener un proceso adecuado de gestión de los recursos de TI y además que exista un adecuado análisis de riesgo que respalde la decisión de trasladar hacia un tercero la custodia y procesamiento crítico de la información de la cooperativa; comprendiendo como resultado del análisis aquellos riesgos que puede minimizar o eventualmente aceptar. Con respecto a las alternativas 3 y 4 pueden verse como un valor agregado o aspecto complementario, ya que viene aportar una serie de servicios complementarios que ofrecen las empresas de centros de datos enfocados en personal certificado, tecnologías de procesamiento y almacenamiento,

	seguridad por mencionar algunos.
Resultados, productos e impactos obtenidos	Con este proyecto se tendrán como principales resultados o productos los siguientes: - Flujo de Caja Proyecto centro de datos capital propio. - Flujo de Caja Proyecto centro de datos subcontratado. - Informe de resultado análisis de la viabilidad económica. - Informe de evaluación de riesgo. - Mapa de calor riesgo inherente. - Mapa de calor riesgo residual. - Tratamiento del riesgo (Propuesta de Controles) Con este proyecto el principal producto e impacto resultante es contar con un análisis financiero y de riesgo, que se convierte en un aspecto fundamental y requerido para una empresa como COOPEALIANZA la cual es regulada y donde decisiones de este tipo deben tener el respectivo sustento financiero que justifique de una manera razonable las inversiones y desde el punto de vista de riesgo ya que la cooperativa al ser supervisada por la SUGEF debe acatar lo que respecta a gestión y control de Tecnologías de Información considerando el acuerdo SUGEF 14-09, donde dicho acuerdo está basado en los Objetivos de Control para la Información y la Tecnología relacionada COBIT 4.0 y que indica en su proceso DS12 Administración del ambiente físico y en específico en su objetivo de control detallado DS12.1 Selección y Diseño del Centro de Datos lo siguiente "Definir y seleccionar los centros de datos físicos para el equipo de TI para soportar la estrategia de tecnología ligada a la estrategia del negocio. Esta selección y diseño del esquema de un centro de datos debe tomar en cuenta el riesgo asociado con desastres naturales y causados por el hombre. También debe considerar las leyes y regulaciones correspondientes, tales como regulaciones de seguridad y de salud en el trabajo." Como parte de la planificación estratégica de Tecnologías de Información de COOPEALIANZA R.L para el periodo 2015 – 2017, específicamente en el análisis de fortalezas, oportunidades, debilidades y amenazas (FODA) se identificaron amenazas tales como "Los desastres naturales pueden afectar la continuidad del negocio" y "Dependencia de terceros puede poner en riesgo la permanencia de la empresa por falta de control en los procesos". Es por lo anterior que el resultado de este trabajo viene a contribuir con la cooperativa en el sentido de sustentar decisiones en cuanto a la gestión de recursos de tecnología de información y a su vez gestionando los riesgos de tecnología de información que pueden afectar la continuidad de las

	operaciones principales de la cooperativa.
Beneficiados con el proyecto(involucrados)	Como principal beneficiario directo del proyecto se encuentra la cooperativa de ahorro y crédito y servicios múltiples COOPEALIANZA R.L, debido a que se busca elegir una opción que le garantice a dicha cooperativa gestionar de una manera razonable, adecuada y eficiente los recursos financieros y de tecnología; asimismo realizando un debido proceso de gestión de riesgos para justificar o soportar las decisiones estratégicas en cuanto a la adquisición y uso de la tecnología, en este caso específico para justificar la decisión de diseñar, construir y mantener un centro de datos propio o bien arrendar este tipo de servicios a una empresa dedicada a este negocio. Otro beneficiado directo es la alta administración y la gerencia financiera ya que este tipo de proyectos buscan mejorar los niveles de rentabilidad de la cooperativa, dirigiendo los esfuerzos financieros y de negocio hacia la razón de ser de la empresa, en este caso hacia los servicios de ahorro y crédito. Además tenemos como beneficiario directo al departamento de Tecnologías de Información de COOPEALIANZA R.L, ya que el análisis producto de este proyecto busca además hacer que el personal de TI de la cooperativa se enfoque cada vez más en el negocio de la misma y de igual manera que se realice una adecuada gestión de los recursos de TI basados en una adecuada gestión del riesgo para soportar día con día los servicios financieros que ofrece la cooperativa a sus clientes y asociados. Un beneficiario indirecto son las empresas que ofrecen servicios subcontratados de arrendamiento de espacio físico, procesamiento y almacenamiento de información crítica; lo anterior se debe a que este tipo de análisis eventualmente puede generar un precedente para que otras entidades financieras justifiquen o sustenten el alquiler a arrendamiento de este tipo de servicios en lugar de destinar importantes recursos de personal, tecnológicos y financieros para diseñar, construir y mantener un centro de datos propio. Otro beneficiario indirecto son los proveedores de tecnología que a la fecha deben recorrer grandes distancias hasta el centro de datos de COOPEALIANZA R.L en Pérez Zeledón para poder ofrecer soporte y cumplir con los acuerdos de nivel de servicio pactados, en caso de justificarse la decisión de subcontratar un centro de datos, los tiempos de respuesta y las distancias se estarían acortando, viéndose beneficiados estos proveedores y traduciéndose además en un ahorro de costos para la cooperativa.
	Para realizar el siguiente proyecto será necesario tener acceso a los siguientes recursos:

Recursos necesarios	**Marcos de Gestión y Control / Estándares / Buenas Prácticas.** • Objetivos de Control para la Información y la Tecnología relacionada COBIT 4.0 • ISO 27001 • ISO 31000 y AS/NZs 4360 **Fuentes de Información.** • Personal de Tecnologias de Informacion de COOPEALIANZA R.L • Personal de Seguridad de Informacion de COOPEALIANZA R.L • Personal de Continuidad del Negocio de COOPEALIANZA R.L • Personal de Unidad Corporativa de Riesgos de COOPEALIANZA R.L • Personal de Gerencia Financiera de de COOPEALIANZA R.L • Personal Servicios Generales de COOPEALIANZA R.L • Personal de Proveeduria Corporativa de COOPEALIANZA R.L • Personal clave de Centros de Datos Subcontratados. **Otros recursos.** • Acceso al sitio web del *UpTime Institute*. • Acceso a los sitios web de empresas que subcontraten centros de datos y/o servicios ligados a este tipo de negocio. • Acceso a otra literatura referente al tema por medio de Internet.
Alcances y Limitaciones	Los eventuales riesgos que se identifican son: que el tiempo requerido para la realización de este proyecto se exceda debido a una mala definición del alcance o que la información requerida de las fuentes no sea obtenida de una manera oportuna. El análisis financiero incluirá los costos iniciales y de mantenimiento más representativo al construir un nuevo centro de datos; entre estos están metros cuadrados de construcción, diseño e implementación eléctrica, sistemas de respaldo eléctrico, sistema de enfriamiento, gabinetes para equipos, sistema de prevención temprana de incendio. El análisis financiero no incluye costos iniciales y de mantenimiento para el equipamiento del centro de datos, es decir servidores, almacenamiento, equipo de comunicación, por mencionar algunos. Además podría ocurrir que los costos enviados por los proveedores para la realización de este trabajo no muestren descuentos importantes ya que no

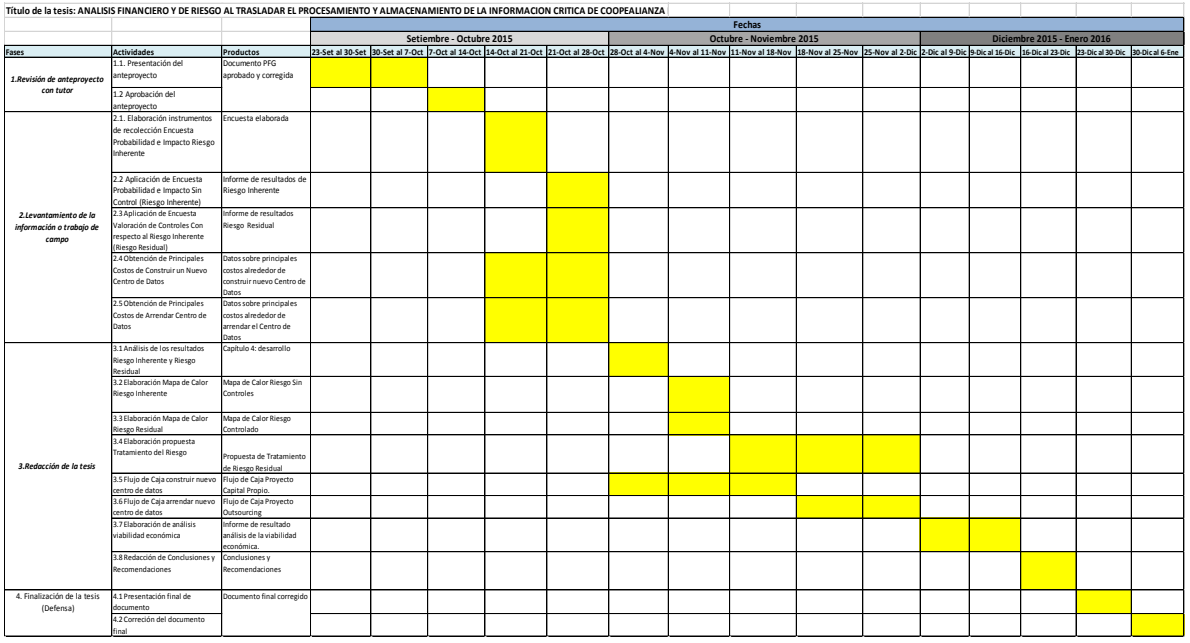
	se trata de una compra inmediata donde se puede obtener un descuento relevante, sino más bien de una estimación de costos. El proceso de gestión de riesgos de acuerdo al marco ISO 31000 que tiene como alcance este trabajo incorpora: establecer el contexto, identificación de riesgos, análisis de riesgos, evaluación de riesgos. El entregable “Tratamiento del riesgo” va a ofrecer una propuesta de controles para los riesgos identificados y que minimicen en un rango aceptable por COOPEALIANZA R.L cualquier impacto negativo, para efectos de este trabajo dichos controles no serán evaluados ni implementados. El alcance de este proyecto es contar con el análisis financiero y de riesgo al trasladar el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica; dentro del alcance además se incluye proporcionar a la alta administración de COOPEALIANZA R.L de conclusiones y recomendaciones producto del análisis efectuado; es por lo anterior que se excluye del alcance de este trabajo la implementación de las recomendaciones producto de este proyecto, lo anterior queda como una decisión a lo interno de la cooperativa.
Objetivos del proyecto	• ***General****:* Realizar un análisis financiero y de riesgo al trasladar el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica. • ***Específicos****:* o Elaborar un análisis financiero del costo inicial y de mantenimiento anual estimado de construir un nuevo centro de datos para COOPEALIANZA R.L que soporte el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L para los próximos 10 años. o Desarrollar un análisis financiero de los costos anuales de arrendamiento y servicios complementarios de centros de datos subcontratados para soportar el procesamiento y almacenamiento de la información crítica de

	COOPEALIANZA R.L para los próximos 10 años. o Ejecutar el proceso de gestión de riesgos de acuerdo al marco ISO 31000 a la actividad de trasladar el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica. o Proporcionar a la alta administración de COOPEALIANZA R.L de recomendaciones que contribuyan con la decisión estratégica en función de la operación del nuevo centro de datos.
Resumen Ejecutivo del Proyecto	En el año 2004 la cooperativa de ahorro y crédito y servicios múltiples COOPEALIANZA R.L decide destinar recursos financieros al diseño e implementación de un centro de datos de su propiedad, con dicha decisión todo el personal de Tecnologías de Información debió involucrarse ya que al tener una estructura organizacional limitada cada miembro tendría que responsabilizarse por mantener en operación dicho centro de datos. Con lo anterior el personal de Administración de Base de Datos, Sistemas de Información, Soporte Técnico, Mesa de Servicio tendrían que cumplir alguna función de soporte y/o monitoreo de algún componente crítico del centro de datos, todo lo anterior sin descuidar las funciones principales y acordes al área de tecnología para la cual fueron contratados. Por otra parte la cooperativa tuvo que destinar en dicho periodo de tiempo, recursos financieros por más de dos millones y medio de dólares, lo anterior sin considerar el costo total anual de propiedad en los que se incurre con un centro de datos de este tipo y que al estar en una zona alejada (Pérez Zeledón) con respecto a la concentración de proveedores que ofrecen soporte a este tipo de infraestructura, el costo se incrementa de manera considerable. También es relevante indicar que en el año 2004 las alternativas existentes en cuanto a subcontratar un centro de datos eran inexistentes o muy limitadas, y por otra parte existía una especie de monopolio y control de los

	precios, lo que hacía que se convirtiera en un servicio excesivamente costoso; por otra parte la infraestructura de telecomunicaciones estaba muy limitada y se contaba con un único proveedor de servicio, en este caso propiedad del estado donde no había opción de exigir un acuerdo de nivel de servicio acorde a la criticidad del servicio que la cooperativa requería. Es importante indicar además que en el año 2016 el centro de datos principal de COOPEALIANZA R.L ubicado en Pérez Zeledón, cumplirá más de diez años de haber entrado en operación, es así como todos los principales componentes de infraestructura, eléctricos, mecánicos, físicos y de seguridad de igual manera deben ser renovados; por otra parte la cooperativa requiere analizar si en lugar de construir un nuevo centro de datos más bien aprovecha las oportunidades que ofrecen los centros de datos subcontratados que cumplen con certificaciones tales como *COBIT*, *ITIL*, ISO 27000 y certificaciones *TIER* del *Up Time Institute*, por mencionar algunas. Con este proyecto se pretende realizar un análisis financiero y de riesgo al trasladar el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica; con lo anterior obtener una justificación o sustento a la hora de decidir diseñar y construir un nuevo centro de datos o bien subcontratar dicho servicio. Para una entidad financiera como COOPELIANZA R.L, donde su principal negocio es la colocación de crédito, el ahorro y los servicios financieros múltiples se convierte en una importante decisión estratégica no sólo redirigir recursos financieros hacia su principal negocio sino que además se vuelve relevante que el personal de Tecnologías de Información se enfoque más al giro de negocio principal y traslade la operativa actual de mantener el centro de datos hacia una empresa especializada en dicho campo, con lo anterior contribuir con el negocio de la cooperativa en gestionar de una manera eficiente y razonable los recursos de Tecnologías de Información. Como principal beneficiario del proyecto se encuentra la cooperativa de

	ahorro y crédito y servicios múltiples COOPEALIANZA R.L, debido a que se busca elegir una opción que le garantice a dicha cooperativa gestionar de una manera razonable, adecuada y eficiente los recursos financieros y de tecnología; asimismo realizando un debido proceso de gestión de riesgos para justificar o soportar las decisiones estratégicas en cuanto a la adquisición y uso de la tecnología, en este caso específico para justificar la decisión de diseñar, construir y mantener un centro de datos propio o bien arrendar este tipo de servicios a una empresa dedicada a este negocio. Además tenemos como beneficiario directo al departamento de Tecnologías de Información de COOPEALIANZA R.L, ya que el análisis producto de este proyecto busca además hacer que el personal de TI de la cooperativa se enfoque cada vez más en el negocio de la misma y de igual manera que se realice una adecuada gestión de los recursos de TI basados en una adecuada gestión del riesgo para soportar día con día los servicios financieros que ofrece la cooperativa a sus clientes y asociados; por otra parte se visualizan algunos beneficiarios indirectos tales como las empresas que se dedican a este tipo de servicios de arrendamiento de espacio y de procesamiento y almacenamiento de información crítica, ya que con este análisis eventualmente otras entidades financieras podrían considerar como sustento o justificación este trabajo para tomar una decisión de esta índole. El resultado del análisis va a proporcionar a la alta administración de COOPEALIANZA R.L de conclusiones y recomendaciones relevantes a la hora de decidir entre diseñar y construir un nuevo centro de datos o bien tomar la importante decisión de subcontratar los servicios a una empresa dedicada a este tipo de servicios.		
Nombre completo y Firma del estudiante	NORBERTO RODRIGUEZ MADRIGAL	**Fecha:**	_26-07-2015__

Nombre completo y firma del profesor (a) que aprueba el PFG	SUYEN ALONSO UBIETA	**Fecha:**	26-08-2015



Título de la tesis: ANALISIS FINANCIERO Y DE RIESGO AL TRASLADAR EL PROCESAMIENTO Y ALMACENAMIENTO DE LA INFORMACION CRITICA DE COOPEALIANZA

			Fechas																
			Setiembre - Octubre 2015					Octubre - Noviembre 2015					Diciembre 2015 - Enero 2016						
Fases	Actividades	Productos	23-Set al 30-Set	30-Set al 7-Oct	7-Oct al 14-Oct	14-Oct al 21-Oct	21-Oct al 28-Oct	28-Oct al 4-Nov	4-Nov al 11-Nov	11-Nov al 18-Nov	18-Nov al 25-Nov	25-Nov al 2-Dic	2-Dic al 9-Dic	9-Dic al 16-Dic	16-Dic al 23-Dic	23-Dic al 30-Dic	30-Dic al 6-Ene
1.Revisión de anteproyecto con tutor	1.1. Presentación del anteproyecto	Documento PFG aprobado y corregida															
	1.2 Aprobación del anteproyecto																
2.Levantamiento de la información o trabajo de campo	2.1. Elaboración instrumentos de recolección Encuesta Probabilidad e Impacto Riesgo Inherente	Encuesta elaborada															
	2.2 Aplicación de Encuesta Probabilidad e Impacto Sin Control (Riesgo Inherente)	Informe de resultados de Riesgo Inherente															
	2.3 Aplicación de Encuesta Valoración de Controles Con respecto al Riesgo Inherente (Riesgo Residual)	Informe de resultados Riesgo Residual															
	2.4 Obtención de Principales Costos de Construir un Nuevo Centro de Datos	Datos sobre principales costos alrededor de construir nuevo Centro de Datos															
	2.5 Obtención de Principales Costos de Arrendar Centro de Datos	Datos sobre principales costos alrededor de arrendar el Centro de Datos															
3.Redacción de la tesis	3.1 Análisis de los resultados Riesgo Inherente y Riesgo Residual	Capitulo 4: desarrollo															
	3.2 Elaboración Mapa de Calor Riesgo Inherente	Mapa de Calor Riesgo Sin Controles															
	3.3 Elaboración Mapa de Calor Riesgo Residual	Mapa de Calor Riesgo Controlado															
	3.4 Elaboración propuesta Tratamiento del Riesgo	Propuesta de Tratamiento de Riesgo Residual															
	3.5 Flujo de Caja construir nuevo centro de datos	Flujo de Caja Proyecto Capital Propio.															
	3.6 Flujo de Caja arrendar nuevo centro de datos	Flujo de Caja Proyecto Outsourcing															
	3.7 Elaboración de análisis viabilidad económica	Informe de resultado análisis de la viabilidad económica.															
	3.8 Redacción de Conclusiones y Recomendaciones	Conclusiones y Recomendaciones															
4. Finalización de la tesis (Defensa)	4.1 Presentación final de documento	Documento final corregido															
	4.2 Corrección del documento final																

Anexo 2: Riesgos identificados Actividad Subcontratar el Centro de Datos

No.	Proceso COBIT	Riesgo	Definición
1	AI3	Daño en los equipos de la plataforma tecnológica	Un funcionario de Tecnología de Información de la cooperativa o un empleado subcontratado al realizar mantenimiento, trabajos de actualización, instalaciones y/o mejoras, afecta de manera considerable equipamiento de tecnología crítico de la cooperativa tal como: servidores de datos, almacenamiento, equipo de comunicación; provocando que los servicios críticos de la cooperativa no puedan ser entregados a los clientes y asociados. También se

			considera afectaciones provocadas por terceros sin autorización o provocados por desastres naturales.
2	AI3	Inadecuada migración y/o traslado de datos al centro de datos	Un administrador de base de datos de la cooperativa o un empleado subcontratado al realizar una migración y/o traslado de datos, por inadecuado dimensionamiento del ancho de banda requerido o por daño en los equipos durante el traslado, o por negligencia provoca afectaciones importantes a la integridad, confidencialidad y disponibilidad de la información crítica de la cooperativa.
3	AI6	Inadecuada gestión de cambios	Un funcionario de Tecnología de Información de la cooperativa o un empleado subcontratado por la implementación de un cambio no aprobado o un cambio que no fue probado en un ambiente controlado de pruebas provoca degradación o no disponibilidad de servicios críticos de la cooperativa, pérdida de confianza y credibilidad del área de TI o incumplimiento de acuerdos de niveles de servicio.
4	DS4	Cierre de operaciones del proveedor del centro de datos	El proveedor del centro de datos por quiebra, embargo o desastre natural no puede ofrecer la entrega continua de los servicios pactados provocando a la cooperativa importantes pérdidas económicas, pérdida de oportunidades de negocio, pérdida de imagen, procesos legales y hasta un eventual cierre de operaciones.
5	DS2	Personal no calificado del proveedor del centro de datos	El personal del proveedor del centro de datos o el personal de otro tercero que contrata el proveedor del centro de datos por falta de conocimiento, habilidades, experiencia y/o rotación de personal no realiza las labores de una manera eficiente y segura provocando afectación a la integridad, confidencialidad y disponibilidad de la información, pérdidas económicas y/o pérdida de imagen de la cooperativa.
6	DS2	Inadecuado monitoreo del desempeño del proveedor del centro de datos	El Encargado de Gestión de Proveedores no establece formalmente en la cooperativa actividades de monitoreo periódicas del desempeño del proveedor del centro de datos provocando que

			exista incumplimiento de los acuerdos de niveles de servicio pactados y/o degradación o no disponibilidad del servicio contratado.
7	DS5	Operaciones ilícitas o fraudulentas desarrolladas por personal propio o externo	Un funcionario de Tecnología de Información de la cooperativa y/o personal del proveedor del centro de datos o el personal de otro tercero que contrata el proveedor del centro de datos realiza transacciones y/o operaciones ilícitas o fraudulentas por exceso de confianza, por ausencia de mecanismos de monitoreo a los accesos otorgados a personal interno o externo, por vulnerabilidades en los sistemas, por desmotivación o descontento provocando importantes pérdidas económicas, pérdida de imagen, afectación a la integridad y confidencialidad de la información, procesos legales e incremento de costos.
8	DS4	Imposibilidad de recuperarse ante un desastre en el centro de datos	La cooperativa y el proveedor del centro de datos no cuentan con un plan de continuidad que considere las acciones necesarias para soportar antes, durante y después un evento con un impacto significativo provocando importantes pérdidas económicas, degradación o no disponibilidad del servicio, pérdida de imagen, procesos legales y hasta el cierre de operaciones de la cooperativa.
9	DS5	Divulgación de información confidencial	Un funcionario de Tecnología de Información de la cooperativa y/o personal del proveedor del centro de datos o el personal de otro tercero que contrata el proveedor del centro de datos por dolo, negligencia, inexistencia o inapropiada clasificación de la información divulga información sensible y/o confidencial de la cooperativa o información clasificada del proveedor del centro de datos provocando sanciones por incumplimiento de normativa externa y/o leyes, pérdida de confianza en el negocio, pérdidas económicas y/o pérdida de imagen.
10	DS5	Pérdida de integridad de la información	Un funcionario de Tecnología de Información de la cooperativa y/o personal del proveedor del centro de

			datos o el personal de otro tercero que contrata el proveedor del centro de datos por dolo, negligencia, inadecuada administración de los datos altere/cambie sin autorización y justificación información sensible, crítica y/o relevante de la cooperativa provocando la transmisión y/o almacenamiento de datos que son incompletos o inexactos, pérdidas económicas, pérdida de imagen y/o pérdida de confianza en el negocio.
11	DS5	No disponibilidad de la información	Un funcionario de Tecnología de Información de la cooperativa y/o personal del proveedor del centro de datos o el personal de otro tercero que contrata el proveedor del centro de datos por dolo, negligencia, por inexistencia de mecanismos de alta disponibilidad en la infraestructura origina que información sensible, crítica y/o relevante de la cooperativa no esté disponible cuando la cooperativa lo requiere provocando sanciones por incumplimiento de normativa externa y/o leyes, pérdida de oportunidades de negocios, pérdida de imagen y/o pérdida de confianza en el negocio.
12	DS10	Inadecuada gestión de problemas, incidentes y eventos	Un funcionario de Tecnología de Información de la cooperativa y/o personal del proveedor del centro de datos o el personal de otro tercero que contrata el proveedor del centro de datos por deficiencias en el proceso de comunicación de incidentes, por poca disponibilidad de recurso humano, por ausencia de una área (*Help Desk*) especializada origina el no mantener formalmente actividades de gestión y control de problemas, incidentes y eventos que minimicen cualquier impacto negativo para la cooperativa provocando degradación o no disponibilidad del servicio, interrupciones en la continuidad del negocio, pérdida de imagen, pérdida económica y/o pérdida de clientes.
13	DS12	Afectaciones de instalaciones críticas por desastres naturales y/o ataques físicos	La cooperativa y el proveedor del centro de datos no cuentan con un plan de continuidad que considere las acciones necesarias para soportar antes, durante y después afectaciones ante desastres

			naturales y/o ataques físicos de cualquier instalación de la cooperativa propia o subcontratada que procese o almacene información crítica provocando importantes pérdidas económicas, degradación o no disponibilidad del servicio, pérdida de imagen, procesos legales y hasta el cierre de operaciones de la cooperativa.
14	DS12	Espacio físico insuficiente en el centro de datos subcontratado	La Gerencia de Tecnologías de Información y las Jefaturas de TI realizan un inadecuado dimensionamiento del espacio requerido en el centro de datos por la cooperativa tanto para las necesidades actuales como futuras, lo anterior por falta de un proceso de monitoreo de tendencias y/o nuevas tecnologías de la industria, por falta de alineamiento de TI con el negocio provocando pérdida de oportunidades de negocios, incremento de costos, pérdida de confianza entre las partes (TI, negocio y proveedor) y entrega del servicio no acorde a los requerimientos de la cooperativa.
15	ME2	Incumplimiento de normativas relacionadas con regulaciones y leyes	La Gerencia de Tecnologías de Información y las Jefaturas de TI por falta de divulgación de normativas, por falta de compromiso para aplicar las normativas, por un inadecuado proceso de inducción y capacitación, por negligencia se incumpla de manera parcial o total normativas de entes regulatorios tales como el acuerdo SUGEF 14-09, otra normativa de la SUGEF o normativa del Banco Central de Costa Rica (BCCR) con respecto al Sistema Nacional de Pagos Electrónicos (SINPE), así como leyes tales como Ley 8968 “Ley de protección de la persona frente al tratamiento de sus datos personales” provocando procesos legales, pérdida de imagen, sanciones de entes supervisores, pérdidas económicas u otras sanciones administrativas.
16	DS12	Dificultad para monitorear y verificar la administración sobre el ambiente físico subcontratado	La Gerencia de Tecnologías de Información, las Jefaturas de TI y Seguridad Corporativa por falta de dispositivos o herramientas que permitan el monitoreo del espacio físico contratado, por inadecuados

			procedimientos y acuerdos para tramitar accesos al centro de datos ante situaciones de emergencia, por restricciones del proveedor (acceso fuera de horario, uso de dispositivos de grabación, por falta de comunicación por parte del proveedor ante cambios en sus políticas internas se origina dificultad para ejercer el control sobre el ambiente físico administrado por el tercero provocando pérdida económica, no disponibilidad del servicio, pérdida de imagen, procesos legales, pérdida de confianza entre las partes (TI, negocio y proveedor) y/o la entrega del servicio no acorde a los requerimientos de la cooperativa.
17	DS9	Información documentada no refleja la arquitectura actual	El administrador de la configuración por la inexistencia de un repositorio actualizado de la configuración, por inexistencia de un proceso para administrar la configuración, por un inadecuado o inexistente proceso de gestión de cambios no mantiene actualizados los estándares, procedimientos, metodologías, directrices, políticas, repositorio de configuración acorde a la infraestructura actual de la cooperativa provocando dificultad para la toma de decisiones, incumplimiento de normativa interna y externa, la existencia de un plan de infraestructura tecnológica inconsistente, costos no contemplados, riesgos no mitigados, planes de contingencia mal diseñados.

Anexo 3: "Encuesta Evaluar Probabilidad e Impacto del Riesgo"

Probabilidad	Impacto
1. La probabilidad de que el evento de riesgo (Daño en los equipos de la plataforma tecnológica) se materialice es: **( ) Casi Cierta** **( ) Probable** **( ) Posible** **( ) Poco Probable** **( ) Remota**	1. Si el evento de riesgo (**Daño en los equipos de la plataforma tecnológica**) se materializa produciría un impacto: ( ) Crítico ( ) Significativo ( ) Moderado ( ) Bajo ( ) Insignificante
2. La probabilidad de que el evento de riesgo (Inadecuada migración y/o traslado de datos al centro de datos) se materialice es: **( ) Casi Cierta** **( ) Probable** **( ) Posible** **( ) Poco Probable** **( ) Remota**	2. Si el evento de riesgo (**Inadecuada migración y/o traslado de datos al centro de datos**) se materializa produciría un impacto: ( ) Crítico ( ) Significativo ( ) Moderado ( ) Bajo ( ) Insignificante
3. La probabilidad de que el evento de riesgo (Inadecuada gestión de cambios) se materialice es: **( ) Casi Cierta** **( ) Probable** **( ) Posible** **( ) Poco Probable** **( ) Remota**	3. Si el evento de riesgo (**Inadecuada gestión de cambios**) se materializa produciría un impacto: ( ) Crítico ( ) Significativo ( ) Moderado ( ) Bajo ( ) Insignificante
4. La probabilidad de que el evento de riesgo (Cierre de operaciones del proveedor del centro de datos) se materialice es: **( ) Casi Cierta** **( ) Probable** **( ) Posible** **( ) Poco Probable** **( ) Remota**	4. Si el evento de riesgo (**Cierre de operaciones del proveedor del centro de datos**) se materializa produciría un impacto: ( ) Crítico ( ) Significativo ( ) Moderado ( ) Bajo ( ) Insignificante
5. La probabilidad de que el evento de riesgo (Personal no calificado del proveedor del centro de datos) se materialice es: **( ) Casi Cierta** **( ) Probable** **( ) Posible** **( ) Poco Probable** **( ) Remota**	5. Si el evento de riesgo (**Personal no calificado del proveedor del centro de datos**) se materializa produciría un impacto: ( ) Crítico ( ) Significativo ( ) Moderado ( ) Bajo ( ) Insignificante
6. La probabilidad de que el evento de riesgo (Inadecuado monitoreo del desempeño del proveedor del centro de	6. Si el evento de riesgo (**Inadecuado monitoreo del desempeño del proveedor del centro de datos**) se materializa

datos) se materialice es: **( ) Casi Cierta** **( ) Probable** **( ) Posible** **( ) Poco Probable** **( ) Remota**	produciría un impacto: ( ) Crítico ( ) Significativo ( ) Moderado ( ) Bajo ( ) Insignificante
7. La probabilidad de que el evento de riesgo (Operaciones ilícitas o fraudulentas desarrolladas por personal propio o externo) se materialice es: **( ) Casi Cierta** **( ) Probable** **( ) Posible** **( ) Poco Probable** **( ) Remota**	7. Si el evento de riesgo (**Operaciones ilícitas o fraudulentas desarrolladas por personal propio o externo**) se materializa produciría un impacto: ( ) Crítico ( ) Significativo ( ) Moderado ( ) Bajo ( ) Insignificante
8. La probabilidad de que el evento de riesgo (Imposibilidad de recuperarse ante un desastre en el centro de datos) se materialice es: **( ) Casi Cierta** **( ) Probable** **( ) Posible** **( ) Poco Probable** **( ) Remota**	8. Si el evento de riesgo (**Imposibilidad de recuperarse ante un desastre en el centro de datos**) se materializa produciría un impacto: ( ) Crítico ( ) Significativo ( ) Moderado ( ) Bajo ( ) Insignificante
9. La probabilidad de que el evento de riesgo (Divulgación de información confidencial) se materialice es: **( ) Casi Cierta** **( ) Probable** **( ) Posible** **( ) Poco Probable** **( ) Remota**	9. Si el evento de riesgo (**Divulgación de información confidencial**) se materializa produciría un impacto: ( ) Crítico ( ) Significativo ( ) Moderado ( ) Bajo ( ) Insignificante
10. La probabilidad de que el evento de riesgo (Pérdida de integridad de la información) se materialice es: **( ) Casi Cierta** **( ) Probable** **( ) Posible** **( ) Poco Probable** **( ) Remota**	10. Si el evento de riesgo (**Pérdida de integridad de la información**) se materializa produciría un impacto: ( ) Crítico ( ) Significativo ( ) Moderado ( ) Bajo ( ) Insignificante
11. La probabilidad de que el evento de riesgo (No disponibilidad de la información) se materialice es: **( ) Casi Cierta** **( ) Probable** **( ) Posible** **( ) Poco Probable** **( ) Remota**	11. Si el evento de riesgo (**No disponibilidad de la información**) se materializa produciría un impacto: ( ) Crítico ( ) Significativo ( ) Moderado ( ) Bajo ( ) Insignificante
12. La probabilidad de que el evento de riesgo (Inadecuada gestión de	12. Si el evento de riesgo (**Inadecuada gestión de problemas, incidentes y eventos**) se

problemas, incidentes y eventos) se materialice es: **( ) Casi Cierta** **( ) Probable** **( ) Posible** **( ) Poco Probable** **( ) Remota**	materializa produciría un impacto: ( ) Crítico ( ) Significativo ( ) Moderado ( ) Bajo ( ) Insignificante
13. La probabilidad de que el evento de riesgo (Afectaciones de instalaciones críticas por desastres naturales y/o ataques físicos) se materialice es: **( ) Casi Cierta** **( ) Probable** **( ) Posible** **( ) Poco Probable** **( ) Remota**	13. Si el evento de riesgo (**Afectaciones de instalaciones críticas por desastres naturales y/o ataques físicos**) se materializa produciría un impacto: ( ) Crítico ( ) Significativo ( ) Moderado ( ) Bajo ( ) Insignificante
14. La probabilidad de que el evento de riesgo (Espacio físico insuficiente en el centro de datos subcontratado) se materialice es: **( ) Casi Cierta** **( ) Probable** **( ) Posible** **( ) Poco Probable** **( ) Remota**	14. Si el evento de riesgo (**Espacio físico insuficiente en el centro de datos subcontratado**) se materializa produciría un impacto: ( ) Crítico ( ) Significativo ( ) Moderado ( ) Bajo ( ) Insignificante
15. La probabilidad de que el evento de riesgo (Incumplimiento de normativas relacionadas con regulaciones y leyes) se materialice es: **( ) Casi Cierta** **( ) Probable** **( ) Posible** **( ) Poco Probable** **( ) Remota**	15. Si el evento de riesgo (**Incumplimiento de normativas relacionadas con regulaciones y leyes**) se materializa produciría un impacto: ( ) Crítico ( ) Significativo ( ) Moderado ( ) Bajo ( ) Insignificante
16. La probabilidad de que el evento de riesgo (Dificultad para monitorear y verificar la administración sobre el ambiente físico subcontratado) se materialice es: **( ) Casi Cierta** **( ) Probable** **( ) Posible** **( ) Poco Probable** **( ) Remota**	16. Si el evento de riesgo (**Dificultad para monitorear y verificar la administración sobre el ambiente físico subcontratado**) se materializa produciría un impacto: ( ) Crítico ( ) Significativo ( ) Moderado ( ) Bajo ( ) Insignificante
17. La probabilidad de que el evento de riesgo (Información documentada no refleja la arquitectura actual) se materialice es: **( ) Casi Cierta**	17. Si el evento de riesgo (**Información documentada no refleja la arquitectura actual**) se materializa produciría un impacto: ( ) Crítico ( ) Significativo

( ) Probable **( ) Posible** **( ) Poco Probable** **( ) Remota**	( ) Moderado ( ) Bajo ( ) Insignificante

Anexo 4: Minutas sesiones de trabajo Proceso Gestión del Riesgo

Unidad de Riesgos Corporativa	**UNIDAD DE RIESGOS CORPORATIVA RIESGO OPERATIVO Y TI MINUTA DE REUNIÓN**	**MIN-RO-060-2015**

FECHA REUNIÓN:	26 de Octubre 2015	**INICIO:**	08:20 a.m.	**FIN:**	05:00 p.m.

	NOMBRE	**PUESTO**
PRESENTES:	Norberto Rodríguez Madrigal	Gerente T.I.
	Tania Melissa Hidalgo Lopez	Oficial de Riesgo Operativo
	Cidar Rojas Santamaria	Coordinador de Sistemas de Información
	Víctor Hugo Mora Chaves	Encargado de Seguridad de la Información
	Julio Zeledón Zúñiga	Coordinador Soporte Técnico y Redes
	Jamesson Céspedes Barrantes	Encargado de Help Desk
	Karen Brenes Barrantes	Encargada de control de procesos de TI
	Ernesto Esquivel Sandí	Coordinador de Base de Datos
	Rony Gutiérrez Madrigal	Coordinador Unidad de Riesgos Corporativa
	Juan Padilla Porras	Asistente Gerencia de T.I.
	Javier Solís Solís	Encargado de Continuidad de las Operaciones
	Ligia Esquivel Castro	Encargado de Gestión de Proveedores
ASUNTO:	1º Sesión de trabajo 2015 con el proceso TI (Traslado el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica), aplicación de la Metodología Riesgo Operativo y TI.	

OBJETIVO DE LA REUNIÓN: Revisión por parte de los participantes de los subprocesos, riesgos, causas y consecuencias existentes para los riesgos de Riesgo Operativo y TI en Traslado el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica. Además de la valoración por parte de los participantes de la probabilidad de ocurrencia de los riesgos y el Impacto de los mismos.

AGENDA

Revisión de los subprocesos existentes de Riesgo Operativo y TI en el Traslado el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica.
Revisión de los riesgos existentes de Riesgo Operativo y TI en el Traslado el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica.
Revisión de las Causas existentes para los riesgos de Riesgo Operativo y TI en el Traslado el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica.
Revisión de las Consecuencias existentes para los riesgos de Riesgo Operativo y TI en el Traslado el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica.

Revisión de la valoración de la probabilidad de ocurrencia de los riesgos de Riesgo Operativo y TI identificados en el Traslado el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica.
Revisión de la valoración del impacto de los riesgos de Riesgo Operativo y TI identificados en el Traslado el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica.

ACUERDOS

#1 Se definen los siguientes subprocesos para el Traslado el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica:

Subproceso	ID Subproceso
Adquirir y mantener la infraestructura tecnológica	AI3
Administrar cambios	AI6
Administrar los problemas	DS10
Administrar el ambiente físico	DS12
Administrar servicios de terceros	DS2
Garantizar la continuidad del servicio	DS4
Garantizar la seguridad de los sistemas	DS5
Administrar la configuración	DS9
Garantizar el Cumplimiento Regulatorio	ME3

#2 Se definen los siguientes eventos de riesgo, causas y consecuencias:

Ref.	Riesgo	Causas	Consecuencias
1	**Daño en los equipos de la plataforma tecnológica**	-Dolo -Fallas o inadecuado funcionamiento del sistema eléctrico -Fallas o inadecuado funcionamiento del sistema de enfriamiento -Sabotaje -Desastres naturales -Defectos de fábrica -Negligencia -Vandalismo	-Pérdidas económicas -Incremento de costos -Pérdida de oportunidades de negocio -Degradación o no disponibilidad del servicio -Pérdida de imagen -Procesos legales
2	**Inadecuada migración y/o traslado de datos al centro de datos.**	-Inadecuado dimensionamiento del ancho de banda -Interrupción en la comunicación -Daño en los equipos durante el traslado -Imposibilidad de traslado físico de los datos -Negligencia -Inadecuada planificación en el proceso de migración -Pérdida de integridad de los datos durante el traslado	-Afectación a la integridad y confidencialidad de la información -Pérdidas económicas -Incremento de costos -Pérdida de oportunidades de negocio -Degradación o no disponibilidad del servicio -Pérdida de imagen -Procesos legales

3	**Inadecuada gestión de cambios**	-Cambios no cumplen con arquitectura de tecnología global -Cambios no documentados -Control y seguimiento insuficiente sobre los cambios -Falta de prioridades en la gestión de cambios según los requerimientos del negocio -Cambios no autorizados ni detectados al ambiente de producción -Inadecuada dirección tecnológica -Falta de estudios técnicos y funcionales -Falta de una visión integral del negocio -Ausencia de un Comité de Arquitectura y Comité de Gestión de Proyectos e Inversiones -Ausencia de un Gestor de Cambios -Falta de personal capacitado -Incumplimiento del marco normativo -Falta de integración con los procesos de administración de problemas y configuración -Inadecuada priorización de cambios según las necesidades del negocio -Mal manejo de versiones en el desarrollo de software -Ausencia de un asistente de Administración de Proyectos de TI	-Pérdidas económicas -Esfuerzos mal dirigidos -Dificultad de mantenimiento y pruebas -Problemas de integración -Pérdida de competitividad -TI no alineado con el negocio -Incapacidad para atender requerimientos -Problemas de compatibilidad -Incumplimiento de acuerdos de niveles de servicio -Degradación o no disponibilidad del servicio -Pérdida de oportunidades de negocios -Fraude -Pérdida de confianza y credibilidad
4	**Cierre de operaciones del proveedor del centro de datos**	-Imposibilidades legales para operar -Quiebras o embargos -Desastres naturales -Ataque externo (lógico o físico) -Incapacidad del proveedor del centro de datos de adaptarse a tendencias y/o nuevas tecnologías de la industria requeridas por la organización	-Afectación a la integridad y confidencialidad de la información -Pérdidas económicas -Incremento de costos -Pérdida de oportunidades de negocio -Degradación o no disponibilidad del servicio -Pérdida de imagen -Procesos legales -Cierre de operaciones
5	**Personal no calificado del proveedor del centro de datos**	-Acuerdos de nivel de servicio que no cumplen con los requerimientos de la cooperativa -Rotación de personal -Ausencia de un plan de capacitación y entrenamiento periódico -Inadecuada selección y reclutamiento del personal por parte del proveedor	-Afectación a la integridad y confidencialidad de la información -Pérdidas económicas -Incremento de costos -Pérdida de oportunidades de negocio -Degradación o no disponibilidad del servicio -Pérdida de imagen -Procesos legales
6	**Inadecuado monitoreo del desempeño del proveedor del centro de datos**	-Ausencia de un responsable de la relación con el proveedor del centro de datos -Ausencia de un marco normativo -Herramientas de monitoreo inadecuadas -Incumplimiento de los cronogramas de monitoreo -No disponibilidad de los responsables de los procesos requirentes	-Incumplimiento de los acuerdos de niveles de servicio -Afectación a la integridad y confidencialidad de la información -Pérdidas económicas -Incremento de costos -Pérdida de oportunidades de negocio -Degradación o no disponibilidad del servicio -Pérdida de imagen -Procesos legales

7	**Operaciones ilícitas o fraudulentas desarrolladas por personal propio o externo**	-Modificaciones de software no autorizadas -Negligencia de personal -Exceso de confianza -Ausencia de mecanismos de monitoreo a los accesos otorgados a personal interno o externo -Uso de herramientas de software no autorizadas -Inapropiado establecimiento de roles de acceso -Falta de aplicación de la política conozca a su empleado -Falta de especificaciones en los requerimientos de seguridad en los sistemas -Vulnerabilidades en los sistemas -Desmotivación o descontento del personal -Suplantación de personal -Inadecuado manejo de las claves a los sistemas -Falta de mecanismos en seguridad de redes -Extorción -Ineficientes medidas de prevención detección y corrección -Inexistencia o incumplimiento de la normativa -Falta de aplicación de la política conozca a su proveedor -Dolo -Negligencia	-Procesos legales -Pérdidas económicas -Pérdida de imagen -Rotación de personal -Sanciones a la Cooperativa -Afectación a la integridad y confidencialidad de la información -Incremento de costos -Pérdida de oportunidades de negocio -Degradación o no disponibilidad del servicio
8	**Imposibilidad de recuperarse ante un desastre en el centro de datos**	-Ausencia de un plan de continuidad del proveedor y/o de la cooperativa -El plan de recuperación del proveedor y/o TI no cumple con los requerimientos o infraestructura actuales del negocio -No idoneidad del personal a cargo en el momento del desastre -Ineficiente divulgación y disponibilidad del plan de continuidad	-Afectación a la integridad y confidencialidad de la información -Pérdidas económicas -Incremento de costos -Pérdida de oportunidades de negocio -Degradación o no disponibilidad del servicio -Pérdida de imagen -Procesos legales -Cierre de operaciones
9	**Divulgación de información confidencial**	-Inadecuada protección de datos sensibles en la transferencia, reproducción, eliminación, almacenamiento y actualización -Inexistencia o inapropiada clasificación de la información -Falta de monitoreo y restricción de aplicaciones no autorizadas -Dolo -Negligencia -Falta de cultura de seguridad de la información -Inexistente o inapropiado marco normativo -Violaciones a la seguridad lógica de la información -Inadecuada administración de los datos	-Procesos legales -Sanciones por incumplimiento de normativa externa y/o leyes -Pérdida de oportunidades de negocios -Pérdidas económicas -Pérdida de imagen -Pérdida de confianza en el negocio
10	**Pérdida de integridad de la información**	-Cambios aplicados directamente a los datos -Negligencia -Dolo -Inexistente o inapropiado marco normativo -Violaciones a la seguridad lógica de la información -Fallas en las comunicaciones -Inadecuada administración de los datos	-Datos transmitidos que son incompletos o inexactos -Procesos legales -Sanciones por incumplimiento de normativa externa y/o leyes -Pérdida de oportunidades de negocios -Pérdidas económicas -Pérdida de imagen -Pérdida de confianza en el negocio

11	**No disponibilidad de la información**	-Incapacidad para restaurar información o volver a un estado anterior provocado por un incidente o desastre -Inexistencia de mecanismos de alta disponibilidad en la infraestructura -Negligencia -Dolo -Inexistente o inapropiado marco normativo -Violaciones a la seguridad lógica de la información -Fallas en las comunicaciones -Ausencia de un plan de continuidad del proveedor y/o de la cooperativa -El plan de recuperación del proveedor y/o TI no cumple con los requerimientos o infraestructura actuales del negocio -Inadecuada administración de los datos -No idoneidad del personal a cargo en el momento del desastre -Ineficiente divulgación y disponibilidad del plan de continuidad -Dificultad para acceder físicamente a la infraestructura instalada en el centro de datos subcontratado	-Procesos legales -Sanciones por incumplimiento de normativa externa y/o leyes -Pérdida de oportunidades de negocios -Pérdidas económicas -Pérdida de imagen -Pérdida de confianza en el negocio -Falta de información para tomar medidas defensivas
12	**Inadecuada gestión de problemas, incidentes y eventos**	-Recurrencia de problemas e incidentes -Falta de pistas de auditoría de los problemas, incidentes y sus soluciones para un manejo proactivo -Deficiencias en el proceso de comunicación de incidentes -Poca disponibilidad de recurso humano -Inexistencia de una base de datos de conocimiento -Ausencia de una área (HelpDesk) especializada -Inapropiada inversión del tiempo -La magnitud o complejidad del incidente supera la capacidad de respuesta -Incumplimiento de la normativa externa e interna	-Afectación de la disponibilidad, integridad y confidencialidad de la información -Pérdida de imagen -Pérdida económica -Pérdida de asociados y clientes -Rotación de personal -Pérdida de oportunidades de negocios -Interrupciones en la continuidad del negocio -Degradación o no disponibilidad del servicio -Sanciones a la Cooperativa -Procesos legales
13	**Afectaciones de instalaciones críticas por desastres naturales y/o ataques físicos**	-Falta de planificación en la ubicación de las instalaciones -Falta de implementar las medidas de protección -Falta de un análisis de riesgos antes de la planificación de los proyectos de selección y/o construcción -Negligencia -Afectación por factores externos(huelgas, terremotos, incendios, tormentas eléctricas, huracanes, inundaciones, actividad volcánica, cyberterrorismo) -Incumplimiento de normativa externa y/o leyes	-Pérdida económica -Daños en equipos -Pérdida información -No disponibilidad del servicio -Pérdida de imagen -Pérdida de productividad -Afectación de la integridad física y psicológica de las personas -Cierre parcial o total de las operaciones -Procesos legales
14	**Espacio físico insuficiente en el centro de datos subcontratado**	-TI no alineado con el negocio -Falta de un proceso de monitoreo de tendencias y/o nuevas tecnologías de la industria -Requerimientos regulatorios -Inadecuado dimensionamiento del espacio requerido en el centro de datos	-Procesos legales -Pérdida de oportunidades de negocios -Pérdidas económicas -Pérdida de imagen -Incremento de costos -Pérdida de confianza entre las partes(TI, negocio y proveedor) -Entrega del servicio no acorde a los requerimientos del negocio
15	**Incumplimiento de normativas relacionadas con regulaciones y leyes**	-Falta de divulgación de normativas -Falta de compromiso para aplicar las normativas -Inadecuado proceso de inducción y capacitación -Desconocimiento de las normas -Falta de seguimiento y monitoreo del cumplimiento de la normativa -Rotación de personal -Negligencia -Dolo -Ambigüedad de las normas	-Procesos legales -Pérdida de imagen -Sanciones de entes supervisores -Pérdidas económicas -Sanciones administrativas

16	**Dificultad para monitorear y verificar la administración sobre el ambiente físico subcontratado**	-Falta de dispositivos o herramientas que permitan el monitoreo del espacio físico contratado -Inadecuados procedimientos y acuerdos para tramitar accesos al centro de datos ante situaciones de emergencia o inusuales -Restricciones del proveedor (acceso fuera de horario, uso de dispositivos de grabación, etc.) -Falta de comunicación por parte del proveedor ante cambios en sus políticas internas	-Pérdida económica -No disponibilidad del servicio -Pérdida de imagen -Procesos legales -Pérdida de confianza entre las partes(TI, negocio y proveedor) -Entrega del servicio no acorde a los requerimientos del negocio
17	**Información documentada no refleja la arquitectura actual**	-Inexistencia de repositorio actualizado de la configuración -No existe un proceso para administrar la configuración -Falta de personal -Complejidad de la infraestructura y su documentación -Inadecuado o inexistente gestión de cambios -Inadecuado funcionamiento del software -Incumplimiento de la normativa interna y/o externa -Inexistencia de normativa	-Dificultad para la toma de decisiones -Incumplimiento de normativa interna y externa -Plan de infraestructura tecnológica inconsistente -TI no alineado con el negocio -Costos no contemplados -Riesgos no mitigados -Planes de contingencia mal diseñados -Documentación de la arquitectura critica inconsistente -Imposibilidad de restaurar un elemento de configuración a un estado anterior -Degradación o no disponibilidad de los servicios

#3 Se valora la probabilidad de ocurrencia y el impacto de los riesgos de Riesgo Operativo y TI para el Traslado el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica con el siguiente resultado:

A) Valoración probabilidad e impacto de los riesgos quedando de la siguiente forma:

N°	Subproceso	ID Subproceso	Riesgo	PROBABILIDAD DE OCURRENCIA	IMPACTO
1	Adquirir y mantener la infraestructura tecnológica	AI3	Daño en los equipos de la plataforma tecnológica	Probable (1 a 3 meses)	Crítico
2	Adquirir y mantener la infraestructura tecnológica	AI3	Inadecuada migración y/o traslado de datos al centro de datos.	Casi cierta (1 al mes)	Crítico
3	Administrar cambios	AI6	Inadecuada gestión de cambios	Probable (1 a 3 meses)	Moderado
4	Garantizar la continuidad del servicio	DS4	Cierre de operaciones del proveedor del centro de datos	Remota (1 al año)	Crítico
5	Administrar servicios de terceros	DS2	Personal no calificado del proveedor del centro de datos	Probable (1 a 3 meses)	Significativo
6	Administrar servicios de terceros	DS2	Inadecuado monitoreo del desempeño del proveedor del centro de datos	Casi cierta (1 al mes)	Significativo
7	Garantizar la seguridad de los sistemas	DS5	Operaciones ilícitas o fraudulentas desarrolladas por personal propio o externo	Casi cierta (1 al mes)	Crítico
8	Garantizar la continuidad del servicio	DS4	Imposibilidad de recuperarse ante un desastre en el centro de datos	Casi cierta (1 al mes)	Crítico
9	Garantizar la seguridad de los sistemas	DS5	Divulgación de información confidencial	Casi cierta (1 al mes)	Crítico
10	Garantizar la seguridad de los sistemas	DS5	Pérdida de integridad de la información	Probable (1 a 3 meses)	Crítico
11	Garantizar la seguridad de los sistemas	DS5	No disponibilidad de la información	Probable (1 a 3 meses)	Crítico

12	Administrar los problemas	DS10	Inadecuada gestión de problemas, incidentes y eventos	Probable (1 a 3 meses)	Significativo
13	Administrar el ambiente físico	DS12	Afectaciones de instalaciones críticas por desastres naturales y/o ataques físicos	Posible (3 a 5 meses)	Crítico
14	Administrar el ambiente físico	DS12	Espacio físico insuficiente en el centro de datos subcontratado	Posible (3 a 5 meses)	Significativo
15	Garantizar el Cumplimiento Regulatorio	ME3	Incumplimiento de normativas relacionadas con regulaciones y leyes	Casi cierta (1 al mes)	Significativo
16	Administrar el ambiente físico	DS12	Dificultad para monitorear y verificar la administración sobre el ambiente físico subcontratado	Probable (1 a 3 meses)	Moderado
17	Administrar la configuración	DS9	Información documentada no refleja la arquitectura actual	Casi cierta (1 al mes)	Moderado

FIRMAS

Tania Hidalgo López
Oficial de Riesgo Operativo

Norberto Rodriguez Madrigal
Gerente de TI

Rony Gutierrez Madrigal
Coordinador Unidad de Riesgos Corporativa

Juan Vacha Porras
Asistente Gerencia de T.I.

Javier Solís Solís
Encargado Continuidad de las Operaciones

Julio Zeledón Zúñiga
Coordinador Soporte Técnico y Redes

Víctor Hugo Mora Chaves
Encargado de Seguridad de la Información

Ligia Esquivel Castro
Encargado de Gestión de Proveedores

Cidar Rojas Santamaria
Coordinador de Sistemas de Información

Ernesto Esquivel Sandí
Coordinador de Base de Datos

Jamesson Céspedes Barrantes
Encargado de Help Desk

Karen Brenes Barrantes
Encargada de Control de Procesos de TI

Unidad de Riesgos Corporativa	**UNIDAD DE RIESGOS CORPORATIVA RIESGO OPERATIVO Y TI MINUTA DE REUNIÓN**	**MIN-RO-061-2015**

FECHA REUNIÓN:	27 de Octubre 2015	**INICIO:**	08:15 a.m.	**FIN:**	05:00 p.m.

	NOMBRE	**PUESTO**
PRESENTES:	Norberto Rodríguez Madrigal	Gerente T.I.
	Tania Melissa Hidalgo Lopez	Oficial de Riesgo Operativo
	Cidar Rojas Santamaria	Coordinador de Sistemas de Información
	Víctor Hugo Mora Chaves	Encargado de Seguridad de la Información
	Julio Zeledón Zúñiga	Coordinador Soporte Técnico y Redes
	Jamesson Céspedes Barrantes	Encargado de Help Desk
	Karen Brenes Barrantes	Encargada de control de procesos de TI
	Ernesto Esquivel Sandí	Coordinador de Base de Datos
	Rony Gutiérrez Madrigal	Coordinador Unidad de Riesgos Corporativa
	Juan Padilla Porras	Asistente Gerencia de T.I.
	Javier Solís Solís	Encargado de Continuidad de las Operaciones
	Ligia Esquivel Castro	Encargado de Gestión de Proveedores
ASUNTO:	2º Sesión de trabajo 2015 con el proceso TI (Traslado el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica), aplicación de la Metodología Riesgo Operativo y TI.	

OBJETIVO DE LA REUNIÓN: Revisión por parte de los participantes de los controles existentes para los riesgos de Riesgo Operativo y TI en el Traslado el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica. Además de la valoración de la calidad de los controles existentes.

AGENDA

Revisión de los controles existentes para los riesgos de Riesgo Operativo y TI en el Traslado el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica.

Revisión de la valoración de la calidad de los controles para los riesgos de Riesgo Operativo y TI identificados en el Traslado el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica.

ACUERDOS

#1 Se definen los siguientes controles para los riesgos en el Traslado el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica:

N°	Riesgo	Controles
1	**Daño en los equipos de la plataforma tecnológica**	-Aplicación integral de la "Parte A Asignación de Recursos Tecnológicos, Parte B Uso de Recursos Tecnológicos" de la DI-074 "Administración, asignación y seguridad de los recursos y servicios de TI" - Incorporación de "Responsabilidades sobre los recursos" en el perfil del puesto - Aplicación integral del procedimiento PR-TI-OPE-002 "Administración del desempeño y la capacidad" - Establecimiento y aplicación integral de los estándares tecnológicos - Establecimiento de mecanismos de seguridad física
2	**Inadecuada migración y/o traslado de datos al centro de datos.**	-Aplicación del procedimiento PR-TI-BD-032 "Migración de base datos Oracle" -Aplicación de la ME-AP-001 " Metodología para la administración de proyectos"
3	**Inadecuada gestión de cambios**	Aplicación del PR-TI-OPE-004 "Control de cambios en aplicaciones e infraestructura de TI" (todo el procedimiento). -Aplicación de la Directriz DI-120 "Funcionamiento de los comités administrativos y grupos de apoyo" PARTE D: Comité de Arquitectura y PARTE G: Comité de Gestión de Proyectos y Cambios de TI. -Aplicación de la Directriz DI-025 "Administración y control de tecnologías de información, punto 3 Administración de cambios. -Uso de la herramienta de software de administración de cambios
4	**Cierre de operaciones del proveedor del centro de datos**	-Se cuenta con una ubicación geográficamente alejada para procesamiento y almacenamiento alternativo documentado en el plan de continuidad del negocio PL-SG-CO-001 -Se cuenta con un diseño de red que permite que la información sea distribuida entre diferentes centros de datos documentado en el plan de continuidad del negocio PL-SG-CO-001 -Se cuenta con una solución de replicación de base de datos documentado en el plan de continuidad del negocio PL-SG-CO-001
5	**Personal no calificado del proveedor del centro de datos**	-Aplicación del procedimiento PR-LEG-002 "Requerimiento de contrato" paso 2 -Aplicación integral PR-SG-GPP-001 "Acreditación de proveedores de Coopealianza R.L y Subsidiarias" -Aplicación integral PR-SG-GPP-003 "Evaluación de proveedores críticos e importantes" -Aplicación de ME-SG-GPP-001 "Administración de servicios de terceros" en su punto 5.6 "Monitorear el desempeño de proveedores"
6	**Inadecuado monitoreo del desempeño del proveedor del centro de datos**	-Aplicación de ME-SG-GPP-001 "Administración de servicios de terceros" en su punto 5.6 "Monitorear el desempeño de proveedores" -Aplicación integral PR-SG-GPP-003 "Evaluación de proveedores críticos e importantes" -Aplicación del procedimiento PR-LEG-002 "Requerimiento de contrato" paso 2
7	**Operaciones ilícitas o fraudulentas desarrolladas por personal propio o externo**	-Estándar #7 " Estándares y reglas de seguridad para aplicaciones y sistemas donde se establece la aplicación de mecanismos de autenticación de acceso al sistema. -Aplicación del Plan de Seguridad de la Información donde se definen las revisiones que debe realizar el área de seguridad de la información. -Ejecución de un mecanismo formal para la creación de usuarios, entrega de permisos y dada de baja de usuarios según procedimientos: PR-SG-SI-001 Inclusión de formas nuevas y registro y modificación de parámetros(integral), PR-SG-SI-002 Solicitud, creación e inactivación usuarios; creación, modificación, asignación y derogación de roles de acceso (integral), PR-SG-SI-003 Creación de usuarios en el dominio y los sistemas(integral), PR-SG-SI-004 Inactivación de usuarios en los sistemas(integral), PR-SG-SI-005 Creación de roles en los sistemas(integral), PR-SG-SI-006 Asignación de roles de acceso a los usuarios (integral), PR-SG-SI-007 Derogación de roles en los sistemas(integral), PR-SG-SI-008 Modificación de roles de acceso(integral), PR-SG-SI-009 Activación de usuarios en los sistemas(integral), PR-TI-BD-002 Mantenimiento de usuarios en las Bases de Datos (integral) -Aplicación de la directriz DI-113 donde se norma la gestión de Seguridad de la Información capítulo 5. -Aplicación de la Directriz DI-025 "Administración y control de tecnologías de información(Puntos 4 y 7 del CAPÍTULO III ENTREGA Y SOPORTE) -Se efectúan pruebas en conformidad con los procedimientos: PR-TI-SI-013 "Cambios: Mantenimiento-corrección y mantenimiento de mejoras" (integral), y PR-TI-SI-015 "Proyectos"(integral) y PR-TI-SI-021 "Aprobación, publicación y eliminación de archivos en el servidor de aplicaciones" -Ejecución del procedimiento PR-SG-SI-017 Monitoreo de actividades de los usuarios en los sistemas utilizados en COOPEALIANZA (Paso 4), aplica para personal interno.

8	**Imposibilidad de recuperarse ante un desastre en el centro de datos**	-Se cuenta con una ubicación geográficamente alejada para procesamiento y almacenamiento alternativo documentado en el plan de continuidad del negocio PL-SG-CO-001 -Se cuenta con un diseño de red que permite que la información sea distribuida entre diferentes centros de datos documentado en el plan de continuidad del negocio PL-SG-CO-001 -Se cuenta con una solución de replicación de base de datos documentado en el plan de continuidad del negocio PL-SG-CO-001 -Se cuenta con un plan de continuidad que contiene una estrategia de recuperación de TI -Aplicación del procedimiento PR-LEG-002 "Requerimiento de contrato" paso 2 -Aplicación integral PR-SG-GPP-001 "Acreditación de proveedores de Coopealianza R.L y Subsidiarias"
9	**Divulgación de información confidencial**	-Se cuenta con acuerdos de confidencialidad con los proveedores normado en el procedimiento PR-SG-GPP-001 "Acreditación de proveedores de Coopealianza R.L y Subsidiarias" en el apartado observaciones -Aplicación del procedimiento PR-LEG-002 "Requerimiento de contrato" paso 7 -Aplicación de la metodología ME-SG-SI-001 "METODOLOGÍA CLASIFICACIÓN Y ETIQUETADO DE INFORMACIÓN EN COOPEALIANZA R.L. Y SUBSIDIARIAS" (integral), -DI-113 "Directriz de seguridad de la información en COOPEALIANZA R.L. y Subsidiarias integral. -Aplicación integral del Procedimiento PR-SG-SI-018 "Atención de requerimientos Corporativos" -Aplicación del procedimiento PR-SG-SI-013 Administración de la seguridad de TI. (Paso número 3) -Se efectúan pruebas en conformidad con los procedimientos: PR-TI-SI-013 "Cambios: Mantenimiento-corrección y mantenimiento de mejoras" (integral), y PR-TI-SI-015 "Proyectos"(integral) -Ejecución de un mecanismo formal para la creación de usuarios, entrega de permisos y dada de baja de usuarios según procedimientos: PR-SG-SI-001 Inclusión de formas nuevas y registro y modificación de parámetros(integral), PR-SG-SI-002 Solicitud, creación e inactivación usuarios; creación, modificación, asignación y derogación de roles de acceso (integral), PR-SG-SI-003 Creación de usuarios en el dominio y los sistemas(integral), PR-SG-SI-004 Inactivación de usuarios en los sistemas(integral), PR-SG-SI-005 Creación de roles en los sistemas(integral), PR-SG-SI-006 Asignación de roles de acceso a los usuarios (integral), PR-SG-SI-007 Derogación de roles en los sistemas(integral), PR-SG-SI-008 Modificación de roles de acceso(integral), PR-SG-SI-009 Activación de usuarios en los sistemas(integral), PR-TI-BD-002 Mantenimiento de usuarios en las Bases de Datos (integral) -Ejecución del procedimiento PR-SG-SI-014 Entrega de Información Clasificada (Paso 4) -Ejecución del procedimiento PR-SG-SI-016 Reporte, registro, categorización de incidentes que afecten la Seguridad de la Información paso 3 -Ejecución del procedimiento PR-SG-SI-017 Monitoreo de actividades de los usuarios en los sistemas utilizados en COOPEALIANZA (Paso 4) -Aplicación de la Directriz DI-025 "Administración y control de tecnologías de información (Puntos 4 y 7 del CAPÍTULO III ENTREGA Y SOPORTE)
10	**Pérdida de integridad de la información**	-Se efectúan pruebas técnicas del sistema y de usuarios en conformidad con los procedimientos: PR-TI-SI-013 "Cambios: Mantenimiento-corrección y mantenimiento de mejoras" (integral), y PR-TI-SI-015 "Proyectos"(integral) -Ejecución del procedimiento PR-SG-SI-016 Reporte, registro, categorización de incidentes que afecten la Seguridad de la Información paso 3 -Ejecución del procedimiento PR-SG-SI-017 Monitoreo de actividades de los usuarios en los sistemas utilizados en COOPEALIANZA (Paso 4) -Aplicación de la Directriz DI-025 "Administración y control de tecnologías de información (Puntos 4 y 7 del CAPÍTULO III ENTREGA Y SOPORTE) -DI-113 "Directriz de seguridad de la información en COOPEALIANZA R.L. y Subsidiarias integral. -Ejecutar el cronograma de pruebas del plan de continuidad PL-SG-CO-001, "Prueba de integridad y disponibilidad de los datos"
11	**No disponibilidad de la información**	-Aplicación del procedimiento PR-SG-SI-013 Administración de la seguridad de TI. (Paso número 3) -Ejecución del procedimiento PR-SG-SI-016 Reporte, registro, categorización de incidentes que afecten la Seguridad de la Información paso 3 -Aplicación de la Directriz DI-025 "Administración y control de tecnologías de información (Puntos 4 y 7 del CAPÍTULO III ENTREGA Y SOPORTE) -Aplicación del Plan de capacidad y desempeño PL-TI-001 -Aplicación del Plan de continuidad del negocio PL-SG-CO-001

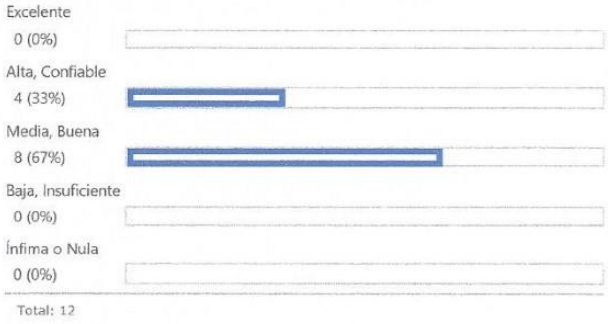
12	**Inadecuada gestión de problemas, incidentes y eventos**	-Aplicación del PR-SI-CO-001 "Atenc. escalabilidad y notific. por interrup. de servic. crítico T.I" pasos del 1 al 13 -Aplicación del PR-TI-011 "Análisis de cambios y problemas relacionados y su afectación a la CMBD" pasos del 1 al 13. -Aplicación del PR-TI-007 "Atención de incidentes y problemas que afecten servicios críticos TI" pasos del 1 al 34. -Aplicación del PR-TI-006 "Reporte de incidentes a proveedores de TI" pasos del 1 al 19.
13	**Afectaciones de instalaciones críticas por desastres naturales y/o ataques físicos**	-Evaluación y verificación de la aplicación del estándar Tecnológico de Coopealianza R.L y Subsidiarias
14	**Espacio físico insuficiente en el centro de datos subcontratado**	-Aplicación del Plan de capacidad y desempeño PL-TI-001
15	**Incumplimiento de normativas relacionadas con regulaciones y leyes**	-Revisión de Auditoria Externa e interna -Aplicación de la ME-SCI-CI-003 " Autoevaluación de la Gestión y el Control de Coopealianza R.L"
16	**Dificultad para monitorear y verificar la administración sobre el ambiente físico subcontratado**	-No existe
17	**Información documentada no refleja la arquitectura actual**	-Para el proceso de administración de la configuración se cuentan con herramientas como metrix (administración de licencias) y RCM (Remote Condition Management Configuration Manager -equipos de comunicación) de GCI, que suministran información al repositorio central de configuración (CMDB) -El Repositorio Central de Configuración contiene: hardware, software, middleware, parámetros, documentación, los procedimientos, nombre, número de versión y detalles de licenciamiento. - Envío anual del Perfil Tecnológico, Acuerdo SUGEF 14-09. - Aplicación de forma integral del Procedimiento PR-TI-OPE-001 Admin. de la configuración y revisión de la infraestructura de forma integral. - Aplicación del Procedimiento PR-TI-011 Análisis de cambios y problemas relacionados y su afectación a la CMBD en sus pasos 4, 5 y 7. - Auditorías Externas (Seguimiento oportunidades de mejora, Acuerdo SUGEF 14-09) -Aplicación del PR-TI-OPE-004 "CONTROL DE CAMBIOS EN APLICACIONES E INFRAESTRUCTURA SOPORTADA POR TECNOLOGÍAS DE INFORMACIÓN" en sus pasos 12,13 y 14. -Autoevaluación del proceso según metodología ME-SCI-CI-002 "Evaluación del marco de control de Tecnologías de Información", Capitulo VIII. RECURSOS/ 2. RECURSOS TECNOLÓGICOS/ Capitulo IX. AUTOEVALUACIÓN DE LOS CONTROLES INTERNOS DE TECNOLOGÍAS DE INFORMACIÓN.

#2 Se valora la calidad de los controles para los riesgos de Riesgo Operativo y TI identificados en el Traslado el procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica:

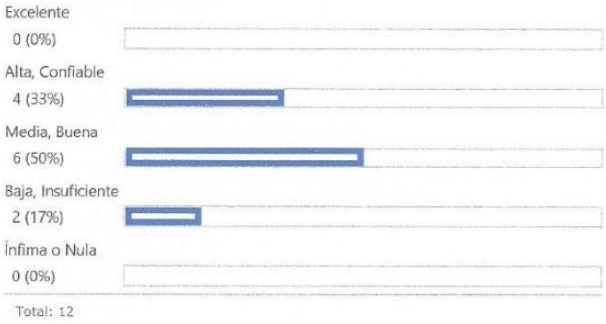
Votación de calidad(centro Datos TI)

Responder a esta encuesta Acciones Configuración Ver: Resumen gráfico

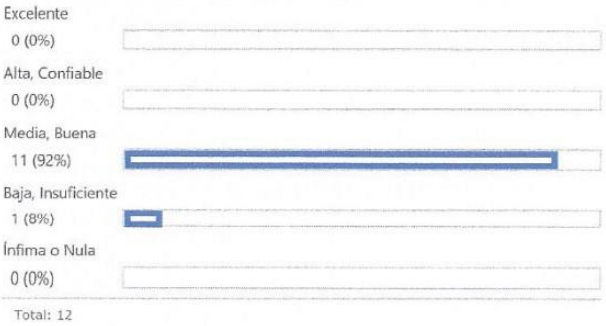
1. 1. En el evento de riesgo (Daño en los equipos de la plataforma tecnológica) la calidad del control (Aplicación integral de la "Parte A Asignación de Recursos Tecnológicos, Parte B Uso de Recursos Tecnológicos" de la DI-074 "Administración, asignación y seguridad de los recursos y servicios de TI") es:



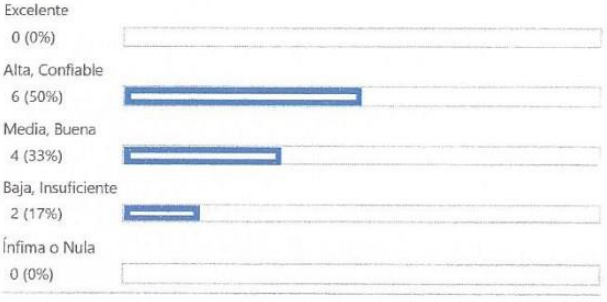
2. 2. En el evento de riesgo (Daño en los equipos de la plataforma tecnológica) la calidad del control (Incorporación de "Responsabilidades sobre los recursos" en el perfil del puesto) es:



3. 3. En el evento de riesgo (Daño en los equipos de la plataforma tecnológica) la calidad del control (Aplicación integral del procedimiento PR-TI-OPE-002 "Administración del desempeño y la capacidad") es:



4. 4. En el evento de riesgo (Daño en los equipos de la plataforma tecnológica) la calidad del control (Establecimiento y aplicación integral de los estándares tecnológicos) es:



Total: 12

5. 5. En el evento de riesgo (Daño en los equipos de la plataforma tecnológica) la calidad del control (Establecimiento de mecanismos de seguridad física) es:

Excelente
0 (0%)
Alta, Confiable
10 (83%)

Media, Buena
1 (8%)

Baja, Insuficiente
1 (8%)

Ínfima o Nula
0 (0%)

Total: 12

6. 6. En el evento de riesgo (Inadecuada migración y/o traslado de datos al centro de datos.) la calidad del control (Aplicación del procedimiento PR-TI-BD-032 "Migración de base datos Oracle") es:

Excelente
0 (0%)
Alta, Confiable
0 (0%)
Media, Buena
12 (100%)

Baja, Insuficiente
0 (0%)
Ínfima o Nula
0 (0%)

Total: 12

7. 7. En el evento de riesgo (Inadecuada migración y/o traslado de datos al centro de datos.) la calidad del control (Aplicación de la ME-AP-001 " Metodología para la administración de proyectos") es:

Excelente
0 (0%)
Alta, Confiable
0 (0%)
Media, Buena
11 (92%)

Baja, Insuficiente
1 (8%)

Ínfima o Nula
0 (0%)

Total: 12

8. 8. En el evento de riesgo (Inadecuada gestión de cambios) la calidad del control (Aplicación del PR-TI-OPE-004 "Control de cambios en aplicaciones e infraestructura de TI" (todo el procedimiento).) es:

Excelente
0 (0%)
Alta, Confiable
10 (83%)

Media, Buena
2 (17%)

Baja, Insuficiente
0 (0%)
Ínfima o Nula
0 (0%)

Total: 12

9. 9. En el evento de riesgo (Inadecuada gestión de cambios) la calidad del control (Aplicación de la Directriz DI-120 "Funcionamiento de los comités administrativos y grupos de apoyo" PARTE D: Comité de Arquitectura y PARTE G: Comité de Gestión de Proyectos y Cambios de TI.) es:

Excelente
0 (0%)
Alta, Confiable
0 (0%)
Media, Buena
10 (83%)

Baja, Insuficiente
2 (17%)

Ínfima o Nula

0 (0%)

Total: 12

10. 10. En el evento de riesgo (Inadecuada gestión de cambios) la calidad del control (Aplicación de la Directriz DI-025 "Administración y control de tecnologías de información, punto 3 Administración de cambios.) es:

Excelente
0 (0%)

Alta, Confiable
0 (0%)

Media, Buena
10 (83%)

Baja, Insuficiente
2 (17%)

Ínfima o Nula
0 (0%)

Total: 12

11. 11. En el evento de riesgo (Inadecuada gestión de cambios) la calidad del control (Uso de la herramienta de software de administración de cambios) es:

Excelente
0 (0%)

Alta, Confiable
7 (58%)

Media, Buena
4 (33%)

Baja, Insuficiente
1 (8%)

Ínfima o Nula
0 (0%)

Total: 12

12. 12. En el evento de riesgo (Cierre de operaciones del proveedor del centro de datos) la calidad del control (Se cuenta con una ubicación geográficamente alejada para procesamiento y almacenamiento alternativo documentado en el plan de continuidad del negocio PL-SG-CO-001) es:

Excelente
1 (8%)

Alta, Confiable
8 (67%)

Media, Buena
3 (25%)

Baja, Insuficiente
0 (0%)

Ínfima o Nula
0 (0%)

Total: 12

13. 13. En el evento de riesgo (Cierre de operaciones del proveedor del centro de datos) la calidad del control (Se cuenta con un diseño de red que permite que la información sea distribuida entre diferentes centros de datos documentado en el plan de continuidad del negocio PL-SG-CO-001) es:

Excelente
2 (17%)

Alta, Confiable
7 (58%)

Media, Buena
3 (25%)

Baja, Insuficiente
0 (0%)

Ínfima o Nula
0 (0%)

Total: 12

14. 14. En el evento de riesgo (Cierre de operaciones del proveedor del centro de datos) la calidad del control (Se cuenta con una solución de replicación de base de datos documentado en el plan de continuidad del negocio PL-SG-CO-001) es:

Excelente
2 (17%)

Alta, Confiable
10 (83%)

Media, Buena
0 (0%)

Baja, Insuficiente
0 (0%)

Ínfima o Nula

0 (0%)

Total: 12

15. 15. En el evento de riesgo (Personal no calificado del proveedor del centro de datos) la calidad del control (Aplicación del procedimiento PR-LEG-002 "Requerimiento de contrato" paso 2) es:

Excelente
0 (0%)

Alta, Confiable
0 (0%)

Media, Buena
12 (100%)

Baja, Insuficiente
0 (0%)

Ínfima o Nula
0 (0%)

Total: 12

16. 16. En el evento de riesgo (Personal no calificado del proveedor del centro de datos) la calidad del control (Aplicación integral PR-SG-GPP-001 "Acreditación de proveedores de Coopealianza R.L y Subsidiarias") es:

Excelente
0 (0%)

Alta, Confiable
7 (58%)

Media, Buena
5 (42%)

Baja, Insuficiente
0 (0%)

Ínfima o Nula
0 (0%)

Total: 12

17. 17. En el evento de riesgo (Personal no calificado del proveedor del centro de datos) la calidad del control (Aplicación integral PR-SG-GPP-003 "Evaluación de proveedores críticos e importantes") es:

Excelente
0 (0%)

Alta, Confiable
7 (58%)

Media, Buena
5 (42%)

Baja, Insuficiente
0 (0%)

Ínfima o Nula
0 (0%)

Total: 12

18. 18. En el evento de riesgo (Personal no calificado del proveedor del centro de datos) la calidad del control (Aplicación de ME-SG-GPP-001 "Administración de servicios de terceros" en su punto 5.6 "Monitorear el desempeño de proveedores") es:

Excelente
0 (0%)

Alta, Confiable
8 (67%)

Media, Buena
3 (25%)

Baja, Insuficiente
1 (8%)

Ínfima o Nula
0 (0%)

Total: 12

19. 19. En el evento de riesgo (Inadecuado monitoreo del desempeño del proveedor del centro de datos) la calidad del control (Aplicación de ME-SG-GPP-001 "Administración de servicios de terceros" en su punto 5.6 "Monitorear el desempeño de proveedores") es:

Excelente
0 (0%)

Alta, Confiable
8 (67%)

Media, Buena
3 (25%)

Baja, Insuficiente
1 (8%)

Ínfima o Nula
0 (0%)

Total: 12

20. 20. En el evento de riesgo (Inadecuado monitoreo del desempeño del proveedor del centro de datos) la calidad del control (Aplicación integral PR-SG-GPP-003 "Evaluación de proveedores críticos e importantes") es:

Excelente
0 (0%)

Alta, Confiable
10 (83%)

Media, Buena
2 (17%)

Baja, Insuficiente
0 (0%)

Ínfima o Nula
0 (0%)

Total: 12

21. 21. En el evento de riesgo (Inadecuado monitoreo del desempeño del proveedor del centro de datos) la calidad del control (Aplicación del procedimiento PR-LEG-002 "Requerimiento de contrato" paso 2) es:

Excelente
0 (0%)

Alta, Confiable
5 (42%)

Media, Buena
7 (58%)

Baja, Insuficiente
0 (0%)

Ínfima o Nula
0 (0%)

Total: 12

22. 22. En el evento de riesgo (Operaciones ilícitas o fraudulentas desarrolladas por personal propio o externo) la calidad del control (Estándar #7 " Estándares y reglas de seguridad para aplicaciones y sistemas donde se establece la aplicación de mecanismos de autenticación de acceso al sistema.) es:

Excelente
0 (0%)

Alta, Confiable
11 (92%)

Media, Buena
1 (8%)

Baja, Insuficiente
0 (0%)

Ínfima o Nula
0 (0%)

Total: 12

23. 23. En el evento de riesgo (Operaciones ilícitas o fraudulentas desarrolladas por personal propio o externo) la calidad del control (Aplicación del Plan de Seguridad de la Información donde se definen las revisiones que debe realizar el área de seguridad de la información.) es:

Excelente
0 (0%)

Alta, Confiable
0 (0%)

Media, Buena
12 (100%)

Baja, Insuficiente
0 (0%)

Ínfima o Nula
0 (0%)

Total: 12

24. 24. En el evento de riesgo (Operaciones ilícitas o fraudulentas desarrolladas por personal propio o externo) la calidad del control (Ejecución de un mecanismo formal para la creación de usuarios, entrega de permisos y dada de baja de usuarios según procedimientos: PR-SG-SI-001 Inclusión de formas nuevas y registro y modificación de parámetros(integral), PR-SG-SI-002 Solicitud, creación e inactivación usuarios; creación, modificación, asignación y derogación de roles de acceso (integral), PR-SG-SI-003 Creación de usuarios en el dominio y los sistemas(integral), PR-SG-SI-004 Inactivación de usuarios en los sistemas(integral), PR-SG-SI-005 Creación de roles en los sistemas(integral), PR-SG-SI-006 Asignación de roles de acceso a los usuarios (integral), PR-SG-SI-007 Derogación de roles en los sistemas(integral), PR-SG-SI-008 Modificación de roles de acceso(integral), PR-SG-SI-009 Activación de usuarios en los sistemas(integral), PR-TI-BD-002 Mantenimiento de usuarios en las Bases de Datos (integral)) es:

Excelente
0 (0%)

Alta, Confiable
8 (67%)

Media, Buena
4 (33%)

Baja, Insuficiente
0 (0%)

Ínfima o Nula
0 (0%)

Total: 12

25. 25. En el evento de riesgo (Operaciones ilícitas o fraudulentas desarrolladas por personal propio o externo) la calidad del control (Aplicación de la directriz DI-113 donde se norma la gestión de Seguridad de la Información capítulo 5.) es:

Excelente
0 (0%)

Alta, Confiable
0 (0%)

Media, Buena
9 (75%)

Baja, Insuficiente
3 (25%)

Ínfima o Nula
0 (0%)

Total: 12

26. 26. En el evento de riesgo (Operaciones ilícitas o fraudulentas desarrolladas por personal propio o externo) la calidad del control (Aplicación de la Directriz DI-025 "Administración y control de tecnologías de información(Puntos 4 y 7 del CAPÍTULO III ENTREGA Y SOPORTE)) es:

Excelente
0 (0%)

Alta, Confiable
3 (25%)

Media, Buena
6 (50%)

Baja, Insuficiente
3 (25%)

Ínfima o Nula
0 (0%)

Total: 12

27. 27. En el evento de riesgo (Operaciones ilícitas o fraudulentas desarrolladas por personal propio o externo) la calidad del control (Se efectúan pruebas en conformidad con los procedimientos: PR-TI-SI-013 "Cambios: Mantenimiento-corrección y mantenimiento de mejoras" (integral), y PR-TI-SI-015 "Proyectos"(integral) y PR-TI-SI-021 "Aprobación, publicación y eliminación de archivos en el servidor de aplicaciones") es:

Excelente
0 (0%)

Alta, Confiable
9 (75%)

Media, Buena
3 (25%)

Baja, Insuficiente
0 (0%)

Ínfima o Nula
0 (0%)

Total: 12

28. 28. En el evento de riesgo (Operaciones ilícitas o fraudulentas desarrolladas por personal propio o externo) la calidad del control (Ejecución del procedimiento PR-SG-SI-017 Monitoreo de actividades de los usuarios en los sistemas utilizados en COOPEALIANZA (Paso 4), aplica para personal interno.) es:

Excelente
0 (0%)

Alta, Confiable
0 (0%)

Media, Buena
1 (8%)

Baja, Insuficiente
11 (92%)

Ínfima o Nula
0 (0%)

Total: 12

29. 29. En el evento de riesgo (Imposibilidad de recuperarse ante un desastre en el centro de datos) la calidad del control (Se cuenta con una ubicación geográficamente alejada para procesamiento y almacenamiento alternativo documentado en el plan de continuidad del negocio PL-SG-CO-001) es:

Excelente
2 (17%)

Alta, Confiable
9 (75%)

Media, Buena
1 (8%)

Baja, Insuficiente
0 (0%)

Ínfima o Nula
0 (0%)

Total: 12

30. 30. En el evento de riesgo (Imposibilidad de recuperarse ante un desastre en el centro de datos) la calidad del control (Se cuenta con un diseño de red que permite que la información sea distribuida entre diferentes centros de datos documentado en el plan de continuidad del negocio PL-SG-CO-001) es:

Excelente
1 (8%)

Alta, Confiable
9 (75%)

Media, Buena
2 (17%)

Baja, Insuficiente
0 (0%)

Ínfima o Nula
0 (0%)

Total: 12

31. 31. En el evento de riesgo (Imposibilidad de recuperarse ante un desastre en el centro de datos) la calidad del control (Se cuenta con una solución de replicación de base de datos documentado en el plan de continuidad del negocio PL-SG-CO-001) es:

Excelente
2 (17%)

Alta, Confiable
6 (50%)

Media, Buena
4 (33%)

Baja, Insuficiente
0 (0%)

Ínfima o Nula
0 (0%)

Total: 12

32. 32. En el evento de riesgo (Imposibilidad de recuperarse ante un desastre en el centro de datos) la calidad del control (Se cuenta con un plan de continuidad que contiene una estrategia de recuperación de TI) es:

Excelente
0 (0%)

Alta, Confiable
8 (67%)

Media, Buena
4 (33%)

Baja, Insuficiente
0 (0%)

Ínfima o Nula
0 (0%)

Total: 12

33. 33. En el evento de riesgo (Imposibilidad de recuperarse ante un desastre en el centro de datos) la calidad del control (Aplicación del procedimiento PR-LEG-002 "Requerimiento de contrato" paso 2) es:

Excelente
0 (0%)

Alta, Confiable
2 (17%)

Media, Buena
8 (67%)

Baja, Insuficiente
2 (17%)

Ínfima o Nula
0 (0%)

Total: 12

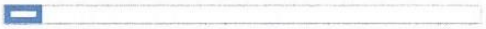
34. 34. En el evento de riesgo (Imposibilidad de recuperarse ante un desastre en el centro de datos) la calidad del control (Aplicación integral PR-SG-GPP-001 "Acreditación de proveedores de Coopealianza R.L y Subsidiarias") es:

Excelente
0 (0%)

Alta, Confiable
3 (25%)

Media, Buena
8 (67%)

Baja, Insuficiente
1 (8%)



Ínfima o Nula
0 (0%)

Total: 12

35. 35. En el evento de riesgo (Divulgación de información confidencial) la calidad del control (Se cuenta con acuerdos de confidencialidad con los proveedores normado en el procedimiento PR-SG-GPP-001 "Acreditación de proveedores de Coopealianza R.L y Subsidiarias" en el apartado observaciones) es:

Excelente
0 (0%)

Alta, Confiable
7 (58%)

Media, Buena
4 (33%)

Baja, Insuficiente
1 (8%)

Ínfima o Nula
0 (0%)

Total: 12

36. 36. En el evento de riesgo (Divulgación de información confidencial) la calidad del control (Aplicación del procedimiento PR-LEG-002 "Requerimiento de contrato" paso 7) es:

Excelente
0 (0%)

Alta, Confiable
7 (58%)

Media, Buena
4 (33%)

Baja, Insuficiente
1 (8%)

Ínfima o Nula
0 (0%)

Total: 12

37. 37. En el evento de riesgo (Divulgación de información confidencial) la calidad del control (Aplicación de la metodología ME-SG-SI-001 "METODOLOGÍA CLASIFICACIÓN Y ETIQUETADO DE INFORMACIÓN EN COOPEALIANZA R.L. Y SUBSIDIARIAS" (integral),) es:

Excelente
0 (0%)

Alta, Confiable
0 (0%)

Media, Buena
12 (100%)

Baja, Insuficiente
0 (0%)

Ínfima o Nula
0 (0%)

Total: 12

38. 38. En el evento de riesgo (Divulgación de información confidencial) la calidad del control (DI-113 "Directriz de seguridad de la información en COOPEALIANZA R.L. y Subsidiarias integral.) es:

Excelente
0 (0%)

Alta, Confiable
2 (17%)

Media, Buena
8 (67%)

Baja, Insuficiente
2 (17%)

Ínfima o Nula
0 (0%)

Total: 12

39. 39. En el evento de riesgo (Divulgación de información confidencial) la calidad del control (Aplicación integral del Procedimiento PR-SG-SI-018 "Atención de requerimientos Corporativos") es:

Excelente
0 (0%)

Alta, Confiable
7 (58%)

Media, Buena
4 (33%)

Baja, Insuficiente
1 (8%)

Ínfima o Nula
0 (0%)

Total: 12

40. 40. En el evento de riesgo (Divulgación de información confidencial) la calidad del control (Aplicación del procedimiento PR-SG-SI-013 Administración de la seguridad de TI. (Paso número 3)) es:

Excelente
0 (0%)

Alta, Confiable
2 (17%)

Media, Buena
10 (83%)

Baja, Insuficiente
0 (0%)

Ínfima o Nula
0 (0%)

Total: 12

41. 41. En el evento de riesgo (Divulgación de información confidencial) la calidad del control (Se efectúan pruebas en conformidad con los procedimientos: PR-TI-SI-013 "Cambios: Mantenimiento-corrección y mantenimiento de mejoras" (integral), y PR-TI-SI-015 "Proyectos"(integral)) es:

Excelente
0 (0%)

Alta, Confiable
8 (67%)

Media, Buena
3 (25%)

Baja, Insuficiente
1 (8%)

Ínfima o Nula
0 (0%)

Total: 12

42. 42. En el evento de riesgo (Divulgación de información confidencial) la calidad del control (Ejecución de un mecanismo formal para la creación de usuarios, entrega de permisos y dada de baja de usuarios según procedimientos: PR-SG-SI-001 Inclusión de formas nuevas y registro y modificación de parámetros(integral), PR-SG-SI-002 Solicitud, creación e inactivación usuarios; creación, modificación, asignación y derogación de roles de acceso (integral), PR-SG-SI-003 Creación de usuarios en el dominio y los sistemas(integral), PR-SG-SI-004 Inactivación de usuarios en los sistemas(integral), PR-SG-SI-005 Creación de roles en los sistemas(integral), PR-SG-SI-006 Asignación de roles de acceso a los usuarios (integral), PR-SG-SI-007 Derogación de roles en los sistemas(integral), PR-SG-SI-008 Modificación de roles de acceso(integral), PR-SG-SI-009 Activación de usuarios en los sistemas(integral), PR-TI-BD-002 Mantenimiento de usuarios en las Bases de Datos (integral)) es:

Excelente
0 (0%)

Alta, Confiable
9 (75%)

Media, Buena
2 (17%)

Baja, Insuficiente
1 (8%)

Ínfima o Nula
0 (0%)

Total: 12

43. 43. En el evento de riesgo (Divulgación de información confidencial) la calidad del control (Ejecución del procedimiento PR-SG-SI-014 Entrega de Información Clasificada (Paso 4)) es:

Excelente
0 (0%)

Alta, Confiable

0 (0%)

Media, Buena

2 (17%)

Baja, Insuficiente

10 (83%)

Ínfima o Nula

0 (0%)

Total: 12

44. 44. En el evento de riesgo (Divulgación de información confidencial) la calidad del control (Ejecución del procedimiento PR-SG-SI-016 Reporte, registro, categorización de incidentes que afecten la Seguridad de la Información paso 3) es:

Excelente

0 (0%)

Alta, Confiable

0 (0%)

Media, Buena

1 (8%)

Baja, Insuficiente

11 (92%)

Ínfima o Nula

0 (0%)

Total: 12

45. 45. En el evento de riesgo (Divulgación de información confidencial) la calidad del control (Ejecución del procedimiento PR-SG-SI-017 Monitoreo de actividades de los usuarios en los sistemas utilizados en COOPEALIANZA (Paso 4)) es:

Excelente

0 (0%)

Alta, Confiable

7 (58%)

Media, Buena

4 (33%)

Baja, Insuficiente

1 (8%)

Ínfima o Nula

0 (0%)

Total: 12

46. 46. En el evento de riesgo (Divulgación de información confidencial) la calidad del control (Aplicación de la Directriz DI-025 "Administración y control de tecnologías de información (Puntos 4 y 7 del CAPÍTULO III ENTREGA Y SOPORTE)) es:

Excelente

0 (0%)

Alta, Confiable

2 (17%)

Media, Buena

7 (58%)

Baja, Insuficiente

3 (25%)

Ínfima o Nula

0 (0%)

Total: 12

47. 47. En el evento de riesgo (Pérdida de integridad de la información) la calidad del control (Se efectúan pruebas técnicas del sistema y de usuarios en conformidad con los procedimientos: PR-TI-SI-013 "Cambios: Mantenimiento-corrección y mantenimiento de mejoras" (integral), y PR-TI-SI-015 "Proyectos"(integral)) es:

Excelente

0 (0%)

Alta, Confiable

8 (67%)

Media, Buena

4 (33%)

Baja, Insuficiente

0 (0%)

Ínfima o Nula

0 (0%)

Total: 12

48. 48. En el evento de riesgo (Pérdida de integridad de la información) la calidad del control (Ejecución del procedimiento PR-SG-SI-016 Reporte, registro, categorización de incidentes que afecten la Seguridad de la Información paso 3) es:

Excelente

0 (0%)

Alta, Confiable

0 (0%)

Media, Buena

1 (8%)

Baja, Insuficiente

11 (92%)

Ínfima o Nula

0 (0%)

Total: 12

49. 49. En el evento de riesgo (Pérdida de integridad de la información) la calidad del control (Ejecución del procedimiento PR-SG-SI-017 Monitoreo de actividades de los usuarios en los sistemas utilizados en COOPEALIANZA (Paso 4)) es:

Excelente

0 (0%)

Alta, Confiable

8 (67%)

Media, Buena

2 (17%)

Baja, Insuficiente

2 (17%)

Ínfima o Nula

0 (0%)

Total: 12

50. 50. En el evento de riesgo (Pérdida de integridad de la información) la calidad del control (Aplicación de la Directriz DI-025 "Administración y control de tecnologías de información (Puntos 4 y 7 del CAPÍTULO III ENTREGA Y SOPORTE)) es:

Excelente

0 (0%)

Alta, Confiable

3 (25%)

Media, Buena

6 (50%)

Baja, Insuficiente

3 (25%)

Ínfima o Nula

0 (0%)

Total: 12

51. 51. En el evento de riesgo (Pérdida de integridad de la información) la calidad del control (DI-113 "Directriz de seguridad de la información en COOPEALIANZA R.L. y Subsidiarias integral.) es:

Excelente

0 (0%)

Alta, Confiable

6 (50%)

Media, Buena

3 (25%)

Baja, Insuficiente

3 (25%)

Ínfima o Nula

0 (0%)

Total: 12

52. 52. En el evento de riesgo (Pérdida de integridad de la información) la calidad del control (Ejecutar el cronograma de pruebas del plan de continuidad PL-SG-CO-001, "Prueba de integridad y disponibilidad de los datos") es:

Excelente

0 (0%)

Alta, Confiable

9 (75%)

Media, Buena

3 (25%)

Baja, Insuficiente

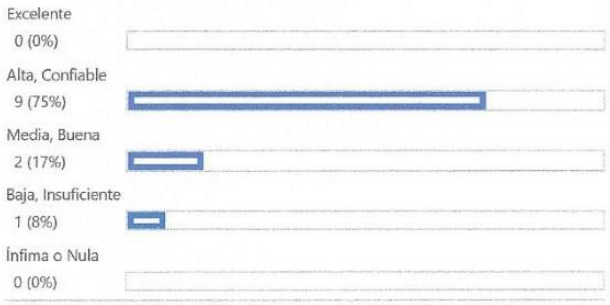
0 (0%)

Ínfima o Nula

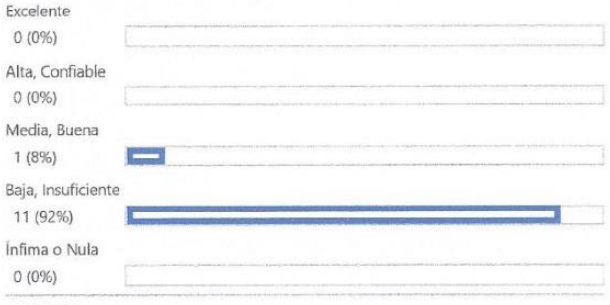
0 (0%)

Total: 12

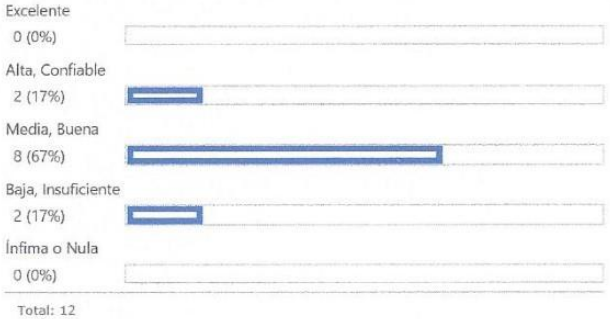
53. 53. En el evento de riesgo (No disponibilidad de la información) la calidad del control (Aplicación del procedimiento PR-SG-SI-013 Administración de la seguridad de TI. (Paso número 3)) es:



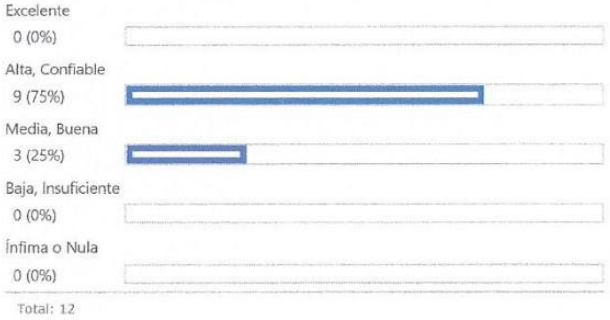
54. 54. En el evento de riesgo (No disponibilidad de la información) la calidad del control (Ejecución del procedimiento PR-SG-SI-016 Reporte, registro, categorización de incidentes que afecten la Seguridad de la Información paso 3) es:



55. 55. En el evento de riesgo (No disponibilidad de la información) la calidad del control (Aplicación de la Directriz DI-025 "Administración y control de tecnologías de información (Puntos 4 y 7 del CAPÍTULO III ENTREGA Y SOPORTE)) es:

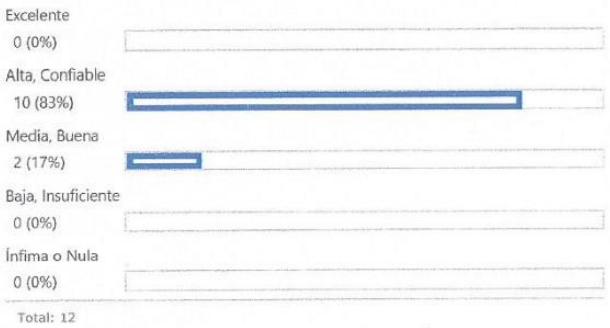


56. 56. En el evento de riesgo (No disponibilidad de la información) la calidad del control (Aplicación del Plan de capacidad y desempeño PL-TI-001) es:



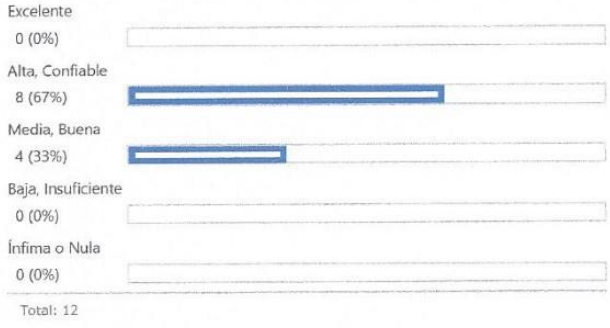
57. 57. En el evento de riesgo (No disponibilidad de la información) la calidad del control (Aplicación del Plan de continuidad del negocio PL-SG-CO-001) es:

58. 58. En el evento de riesgo (Inadecuada gestión de problemas, incidentes y eventos) la calidad del control (Aplicación del PR-SI-CO-001 "Atenc. escalabilidad y notific. por interrup. de servic. crítico T.I." pasos del 1 al 13) es:

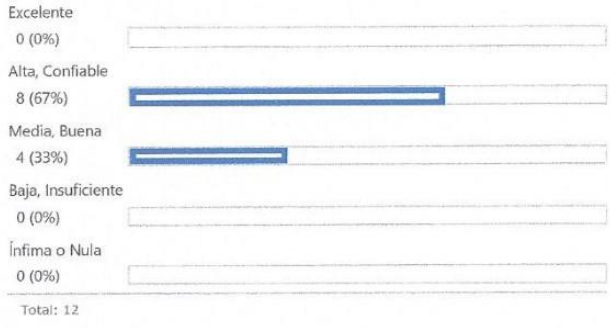


59. 59. En el evento de riesgo (Inadecuada gestión de problemas, incidentes y eventos) la calidad del control (Aplicación del PR-TI-011 "Análisis de cambios y problemas relacionados y su afectación a la CMBD."pasos del 1 al 13.) es:

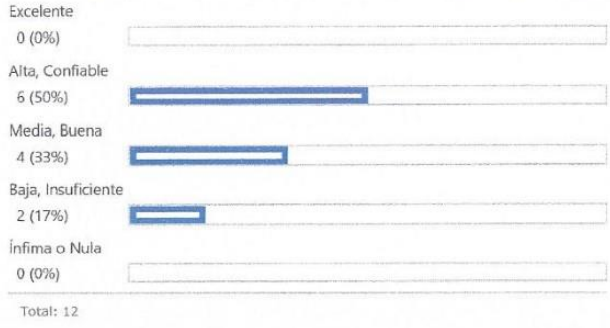
60. 60. En el evento de riesgo (Inadecuada gestión de problemas, incidentes y eventos) la calidad del control (Aplicación del PR-TI-007 "Atención de incidentes y problemas que afecten servicios críticos TI."pasos del 1 al 34.) es:



61. 61. En el evento de riesgo (Inadecuada gestión de problemas, incidentes y eventos) la calidad del control (Aplicación del PR-TI-006 "Reporte de incidentes a proveedores de TI."pasos del 1 al 19.) es:



62. 62. En el evento de riesgo (Afectaciones de instalaciones críticas por desastres naturales y/o ataques físicos) la calidad del control (Evaluación y verificación de la aplicación del estándar Tecnológico de Coopealianza R.L y Subsidiarias) es:



63. 63. En el evento de riesgo (Espacio físico insuficiente en el centro de datos subcontratado) la calidad del control (Aplicación del Plan de capacidad y desempeño PL-TI-001) es:

Excelente
0 (0%)
Alta, Confiable
1 (8%)
Media, Buena
0 (0%)
Baja, Insuficiente
11 (92%)
Ínfima o Nula
0 (0%)
Total: 12

64. 64. En el evento de riesgo (Incumplimiento de normativas relacionadas con regulaciones y leyes) la calidad del control (Revisión de Auditoria Externa e interna) es:

Excelente
0 (0%)
Alta, Confiable
8 (67%)
Media, Buena
4 (33%)
Baja, Insuficiente
0 (0%)
Ínfima o Nula
0 (0%)
Total: 12

65. 65. En el evento de riesgo (Incumplimiento de normativas relacionadas con regulaciones y leyes) la calidad del control (Aplicación de la ME-SCI-CI-003 " Autoevaluación de la Gestión y el Control de Coopealianza R.L") es:

Excelente
0 (0%)
Alta, Confiable
2 (17%)
Media, Buena
9 (75%)
Baja, Insuficiente
1 (8%)
Ínfima o Nula
0 (0%)
Total: 12

66. 66. En el evento de riesgo (Dificultad para monitorear y verificar la administración sobre el ambiente físico subcontratado) la calidad del control (No existe) es:

Excelente
0 (0%)
Alta, Confiable
0 (0%)
Media, Buena
0 (0%)
Baja, Insuficiente
0 (0%)
Ínfima o Nula
12 (100%)
Total: 12

67. 67. En el evento de riesgo (Información documentada no refleja la arquitectura actual) la calidad del control (Para el proceso de administración de la configuración se cuentan con herramientas como metrix (administración de licencias) y RCM (Remote Condition Management Configuration Manager -equipos de comunicación) de GCI, que suministran información al repositorio central de configuración (CMDB)) es:

Excelente
0 (0%)
Alta, Confiable
6 (50%)
Media, Buena
4 (33%)
Baja, Insuficiente
2 (17%)
Ínfima o Nula

0 (0%)

Total: 12

68. 68. En el evento de riesgo (Información documentada no refleja la arquitectura actual) la calidad del control (El Repositorio Central de Configuración contiene: hardware, software, middleware, parámetros, documentación, los procedimientos, nombre, numero de versión y detalles de licenciamiento.) es:

Excelente
0 (0%)

Alta, Confiable
8 (67%)

Media, Buena
4 (33%)

Baja, Insuficiente
0 (0%)

Ínfima o Nula
0 (0%)

Total: 12

69. 69. En el evento de riesgo (Información documentada no refleja la arquitectura actual) la calidad del control (Envío anual del Perfil Tecnológico, Acuerdo SUGEF 14-09.) es:

Excelente
0 (0%)

Alta, Confiable
9 (75%)

Media, Buena
1 (8%)

Baja, Insuficiente
2 (17%)

Ínfima o Nula
0 (0%)

Total: 12

70. 70. En el evento de riesgo (Información documentada no refleja la arquitectura actual) la calidad del control (Aplicación de forma integral del Procedimiento PR-TI-OPE-001 Admin. de la configuración y revisión de la infraestructura de forma integral.) es:

Excelente
0 (0%)

Alta, Confiable
11 (92%)

Media, Buena
1 (8%)

Baja, Insuficiente
0 (0%)

Ínfima o Nula
0 (0%)

Total: 12

71. 71. En el evento de riesgo (Información documentada no refleja la arquitectura actual) la calidad del control (Aplicación del Procedimiento PR-TI-011 Análisis de cambios y problemas relacionados y su afectación a la CMBD en sus pasos 4, 5 y 7.) es:

Excelente
0 (0%)

Alta, Confiable
7 (58%)

Media, Buena
5 (42%)

Baja, Insuficiente
0 (0%)

Ínfima o Nula
0 (0%)

Total: 12

72. 72. En el evento de riesgo (Información documentada no refleja la arquitectura actual) la calidad del control (Auditorias Externas (Seguimiento oportunidades de mejora, Acuerdo SUGEF 14-09)) es:

Excelente
1 (8%)

Alta, Confiable
8 (67%)

Media, Buena
2 (17%)

Baja, Insuficiente
1 (8%)

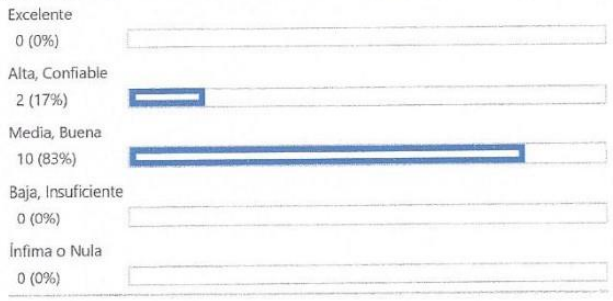
Ínfima o Nula
0 (0%)

Total: 12

73. 73. En el evento de riesgo (Información documentada no refleja la arquitectura actual) la calidad del control (Aplicación del PR-TI-OPE-004 "CONTROL DE CAMBIOS EN APLICACIONES E INFRAESTRUCTURA SOPORTADA POR TECNOLOGÍAS DE INFORMACIÓN" en sus pasos 12,13 y 14.) es:

Total: 12

74. 74. En el evento de riesgo (Información documentada no refleja la arquitectura actual) la calidad del control (Autoevaluación del proceso segun metodología ME-SCI-CI-002 "Evaluación del marco de control de Tecnologías de Información", Capitulo VIII. RECURSOS/ 2. RECURSOS TECNOLÓGICOS/ Capitulo IX. AUTOEVALUACIÓN DE LOS CONTROLES INTERNOS DE TECNOLOGÍAS DE INFORMACIÓN.) es



Total: 12

FIRMAS

Tania Hidalgo López
Oficial de Riesgo Operativo

Norberto Rodriguez Madrigal
Gerente de TI

Rony Gutierrez Madrigal
Coordinador Unidad de Riesgos Corporativa

Juan [illegible]illa Porras
Asistente Gerencia de T.I.

Javier Solís Solís
Encargado Continuidad de las Operaciones

Julio Zeledón Zúñiga
Coordinador Soporte Técnico y Redes

Víctor Hugo Mora Chaves
Encargado de Seguridad de la Información

Ligia Esquivel Castro
Encargado de Gestión de Proveedores

Cidar Rojas Santamaria
Coordinador de Sistemas de Información

Ernesto Esquivel Sandí
Coordinador de Base de Datos

Jamesson Céspedes Barrantes
Encargado de Help Desk

Karen Brenes Barrantes
Encargada de Control de Procesos de TI

Unidad de Riesgos Corporativa	UNIDAD DE RIESGOS CORPORATIVA RIESGO OPERATIVO Y TI MINUTA DE REUNIÓN	MIN-RO-063-2015

FECHA REUNIÓN:	03 de Noviembre 2015	INICIO:	01:45 p.m.	FIN:	05:00 p.m.

	NOMBRE	PUESTO
PRESENTES:	Norberto Rodríguez Madrigal	Gerente T.I.
	Tania Melissa Hidalgo Lopez	Oficial de Riesgo Operativo
	Cidar Rojas Santamaria	Coordinador de Sistemas de Información
	Víctor Hugo Mora Chaves	Encargado de Seguridad de la Información
	Julio Zeledón Zúñiga	Coordinador Soporte Técnico y Redes
	Jamesson Céspedes Barrantes	Encargado de Help Desk
	Karen Brenes Barrantes	Encargada de control de procesos de TI
	Ernesto Esquivel Sandí	Coordinador de Base de Datos
	Rony Gutiérrez Madrigal	Coordinador Unidad de Riesgos Corporativa
	Juan Padilla Porras	Asistente Gerencia de T.I.
	Javier Solís Solís	Encargado de Continuidad de las Operaciones
	Ligia Esquivel Castro	Encargado de Gestión de Proveedores

ASUNTO:	3º Sesión de trabajo 2015 con el proceso TI (Traslado del procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica), aplicación de la Metodología Riesgo Operativo y TI.

OBJETIVO DE LA REUNIÓN: Valoración por parte de los participantes de la frecuencia y ponderación de los controles existentes en el Traslado del procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica.

AGENDA

Revisión de la valoración la ponderación de los controles existentes para los riesgos de Riesgo Operativo y TI identificados en el Traslado del procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica.

Revisión de la valoración la frecuencia de los controles existentes para los riesgos de Riesgo Operativo y TI identificados en el Traslado del procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica.

ACUERDOS

#1 Se valora la ponderación y la frecuencia de los controles de los riesgos de Riesgo Operativo y TI para el Traslado del procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica con el siguiente resultado:

A) Valoración de la ponderación de los controles quedando de la siguiente forma:

N°	Subproceso	Riesgos	Controles	Ponderación
1	AI3	**Daño en los equipos de la plataforma tecnológica**	Aplicación integral de la "Parte A Asignación de Recursos Tecnológicos, Parte B Uso de Recursos Tecnológicos" de la DI-074 "Administración, asignación y seguridad de los recursos y servicios de TI"	30%
		Daño en los equipos de la plataforma tecnológica	Incorporación de "Responsabilidades sobre los recursos" en el perfil del puesto	20%
		Daño en los equipos de la plataforma tecnológica	Aplicación integral del procedimiento PR-TI-OPE-002 "Administración del desempeño y la capacidad"	5%
		Daño en los equipos de la plataforma tecnológica	Establecimiento y aplicación integral de los estándares tecnológicos	5%
		Daño en los equipos de la plataforma tecnológica	Establecimiento de mecanismos de seguridad física	40%
				100%
2	AI3	**Inadecuada migración y/o traslado de datos al centro de datos.**	Aplicación del procedimiento PR-TI-BD-032 "Migración de base datos Oracle"	30%
		Inadecuada migración y/o traslado de datos al centro de datos.	Aplicación de la ME-AP-001 " Metodología para la administración de proyectos"	70%
				100%
3	AI6	**Inadecuada gestión de cambios**	Aplicación del PR-TI-OPE-004 "Control de cambios en aplicaciones e infraestructura de TI" (todo el procedimiento).	40%
		Inadecuada gestión de cambios	Aplicación de la Directriz DI-120 "Funcionamiento de los comités administrativos y grupos de apoyo" PARTE D: Comité de Arquitectura y PARTE G: Comité de Gestión de Proyectos y Cambios de TI.	30%
		Inadecuada gestión de cambios	Aplicación de la Directriz DI-025 "Administración y control de tecnologías de información, punto 3 Administración de cambios.	20%
		Inadecuada gestión de cambios	Uso de la herramienta de software de administración de cambios	10%
				100%
4	DS4	**Cierre de operaciones del proveedor del centro de datos**	Se cuenta con una ubicación geográficamente alejada para procesamiento y almacenamiento alternativo documentado en el plan de continuidad del negocio PL-SG-CO-001	34%
		Cierre de operaciones del proveedor del centro de datos	Se cuenta con un diseño de red que permite que la información sea distribuida entre diferentes centros de datos documentado en el plan de continuidad del negocio PL-SG-CO-001	33%
		Cierre de operaciones del proveedor del centro de datos	Se cuenta con una solución de replicación de base de datos documentado en el plan de continuidad del negocio PL-SG-CO-001	33%
				100%
5	DS2	**Personal no calificado del proveedor del centro de datos**	Aplicación del procedimiento PR-LEG-002 "Requerimiento de contrato" paso 2	25%
		Personal no calificado del proveedor del centro de datos	Aplicación integral PR-SG-GPP-001 "Acreditación de proveedores de Coopealianza R.L y Subsidiarias"	25%
		Personal no calificado del proveedor del centro de datos	Aplicación integral PR-SG-GPP-003 "Evaluación de proveedores críticos e importantes"	25%
		Personal no calificado del proveedor del centro de datos	Aplicación de ME-SG-GPP-001 "Administración de servicios de terceros" en su punto 5.6 "Monitorear el desempeño de proveedores"	25%
				100%
6	DS2	**Inadecuado monitoreo del desempeño del proveedor del centro de datos**	Aplicación de ME-SG-GPP-001 "Administración de servicios de terceros" en su punto 5.6 "Monitorear el desempeño de proveedores"	50%

		Inadecuado monitoreo del desempeño del proveedor del centro de datos	Aplicación integral PR-SG-GPP-003 "Evaluación de proveedores críticos e importantes"	25%
		Inadecuado monitoreo del desempeño del proveedor del centro de datos	Aplicación del procedimiento PR-LEG-002 "Requerimiento de contrato" paso 2	25%
				100%
7	**DS5**	**Operaciones ilícitas o fraudulentas desarrolladas por personal propio o externo**	Estándar #7 " Estándares y reglas de seguridad para aplicaciones y sistemas donde se establece la aplicación de mecanismos de autenticación de acceso al sistema.	10%
		Operaciones ilícitas o fraudulentas desarrolladas por personal propio o externo	Aplicación del Plan de Seguridad de la Información donde se definen las revisiones que debe realizar el área de seguridad de la información.	20%
		Operaciones ilícitas o fraudulentas desarrolladas por personal propio o externo	Ejecución de un mecanismo formal para la creación de usuarios, entrega de permisos y dada de baja de usuarios según procedimientos: PR-SG-SI-001 Inclusión de formas nuevas y registro y modificación de parámetros(integral), PR-SG-SI-002 Solicitud, creación e inactivación usuarios; creación, modificación, asignación y derogación de roles de acceso (integral), PR-SG-SI-003 Creación de usuarios en el dominio y los sistemas(integral), PR-SG-SI-004 Inactivación de usuarios en los sistemas(integral), PR-SG-SI-005 Creación de roles en los sistemas(integral), PR-SG-SI-006 Asignación de roles de acceso a los usuarios (integral), PR-SG-SI-007 Derogación de roles en los sistemas(integral), PR-SG-SI-008 Modificación de roles de acceso(integral), PR-SG-SI-009 Activación de usuarios en los sistemas(integral), PR-TI-BD-002 Mantenimiento de usuarios en las Bases de Datos (integral)	15%
		Operaciones ilícitas o fraudulentas desarrolladas por personal propio o externo	Aplicación de la directriz DI-113 donde se norma la gestión de Seguridad de la Información capítulo 5.	15%
		Operaciones ilícitas o fraudulentas desarrolladas por personal propio o externo	Aplicación de la Directriz DI-025 "Administración y control de tecnologías de información(Puntos 4 y 7 del CAPÍTULO III ENTREGA Y SOPORTE)	10%
		Operaciones ilícitas o fraudulentas desarrolladas por personal propio o externo	Se efectúan pruebas en conformidad con los procedimientos: PR-TI-SI-013 "Cambios: Mantenimiento-corrección y mantenimiento de mejoras" (integral), y PR-TI-SI-015 "Proyectos"(integral) y PR-TI-SI-021 "Aprobación, publicación y eliminación de archivos en el servidor de aplicaciones"	10%
		Operaciones ilícitas o fraudulentas desarrolladas por personal propio o externo	Ejecución del procedimiento PR-SG-SI-017 Monitoreo de actividades de los usuarios en los sistemas utilizados en COOPEALIANZA (Paso 4), aplica para personal interno.	20%
				100%
8	**DS4**	**Imposibilidad de recuperarse ante un desastre en el centro de datos**	Se cuenta con una ubicación geográficamente alejada para procesamiento y almacenamiento alternativo documentado en el plan de continuidad del negocio PL-SG-CO-001	25%
		Imposibilidad de recuperarse ante un desastre en el centro de datos	Se cuenta con un diseño de red que permite que la información sea distribuida entre diferentes centros de datos documentado en el plan de continuidad del negocio PL-SG-CO-001	25%
		Imposibilidad de recuperarse ante un desastre en el centro de datos	Se cuenta con una solución de replicación de base de datos documentado en el plan de continuidad del negocio PL-SG-CO-001	25%

		Imposibilidad de recuperarse ante un desastre en el centro de datos	Se cuenta con un plan de continuidad que contiene una estrategia de recuperación de TI	15%
		Imposibilidad de recuperarse ante un desastre en el centro de datos	Aplicación del procedimiento PR-LEG-002 "Requerimiento de contrato" paso 2	5%
		Imposibilidad de recuperarse ante un desastre en el centro de datos	Aplicación integral PR-SG-GPP-001 "Acreditación de proveedores de Coopealianza R.L y Subsidiarias"	5%
				100%
9	**DS5**	**Divulgación de información confidencial**	Se cuenta con acuerdos de confidencialidad con los proveedores normado en el procedimiento PR-SG-GPP-001 "Acreditación de proveedores de Coopealianza R.L y Subsidiarias" en el apartado observaciones	10%
		Divulgación de información confidencial	Aplicación del procedimiento PR-LEG-002 "Requerimiento de contrato" paso 7	10%
		Divulgación de información confidencial	Aplicación de la metodología ME-SG-SI-001 "METODOLOGÍA CLASIFICACIÓN Y ETIQUETADO DE INFORMACIÓN EN COOPEALIANZA R.L. Y SUBSIDIARIAS" (integral),	10%
		Divulgación de información confidencial	DI-113 "Directriz de seguridad de la información en COOPEALIANZA R.L. y Subsidiarias integral.	15%
		Divulgación de información confidencial	Aplicación integral del Procedimiento PR-SG-SI-018 "Atención de requerimientos Corporativos"	10%
		Divulgación de información confidencial	Aplicación del procedimiento PR-SG-SI-013 Administración de la seguridad de TI. (Paso número 3)	5%
		Divulgación de información confidencial	Se efectúan pruebas en conformidad con los procedimientos: PR-TI-SI-013 "Cambios: Mantenimiento-corrección y mantenimiento de mejoras" (integral), y PR-TI-SI-015 "Proyectos"(integral)	5%
		Divulgación de información confidencial	Ejecución de un mecanismo formal para la creación de usuarios, entrega de permisos y dada de baja de usuarios según procedimientos: PR-SG-SI-001 Inclusión de formas nuevas y registro y modificación de parámetros(integral), PR-SG-SI-002 Solicitud, creación e inactivación usuarios; creación, modificación, asignación y derogación de roles de acceso (integral), PR-SG-SI-003 Creación de usuarios en el dominio y los sistemas(integral), PR-SG-SI-004 Inactivación de usuarios en los sistemas(integral), PR-SG-SI-005 Creación de roles en los sistemas(integral), PR-SG-SI-006 Asignación de roles de acceso a los usuarios (integral), PR-SG-SI-007 Derogación de roles en los sistemas(integral), PR-SG-SI-008 Modificación de roles de acceso(integral), PR-SG-SI-009 Activación de usuarios en los sistemas(integral), PR-TI-BD-002 Mantenimiento de usuarios en las Bases de Datos (integral)	15%
		Divulgación de información confidencial	Ejecución del procedimiento PR-SG-SI-014 Entrega de Información Clasificada (Paso 4)	5%
		Divulgación de información confidencial	Ejecución del procedimiento PR-SG-SI-016 Reporte, registro, categorización de incidentes que afecten la Seguridad de la Información paso 3	5%
		Divulgación de información confidencial	Ejecución del procedimiento PR-SG-SI-017 Monitoreo de actividades de los usuarios en los sistemas utilizados en COOPEALIANZA (Paso 4)	5%
		Divulgación de información confidencial	Aplicación de la Directriz DI-025 "Administración y control de tecnologías de información (Puntos 4 y 7 del CAPÍTULO III ENTREGA Y SOPORTE)	5%
				100%
10	**DS5**	**Pérdida de integridad de la información**	Se efectúan pruebas técnicas del sistema y de usuarios en conformidad con los procedimientos: PR-TI-SI-013 "Cambios:	30%

			Mantenimiento-corrección y mantenimiento de mejoras" (integral), y PR-TI-SI-015 "Proyectos"(integral)	
		Pérdida de integridad de la información	Ejecución del procedimiento PR-SG-SI-016 Reporte, registro, categorización de incidentes que afecten la Seguridad de la Información paso 3	10%
		Pérdida de integridad de la información	Ejecución del procedimiento PR-SG-SI-017 Monitoreo de actividades de los usuarios en los sistemas utilizados en COOPEALIANZA (Paso 4)	25%
		Pérdida de integridad de la información	Aplicación de la Directriz DI-025 "Administración y control de tecnologías de información (Puntos 4 y 7 del CAPÍTULO III ENTREGA Y SOPORTE)	10%
		Pérdida de integridad de la información	DI-113 "Directriz de seguridad de la información en COOPEALIANZA R.L. y Subsidiarias integral.	10%
		Pérdida de integridad de la información	Ejecutar el cronograma de pruebas del plan de continuidad PL-SG-CO-001, "Prueba de integridad y disponibilidad de los datos"	15%
				100%
11	**DS5**	**No disponibilidad de la información**	Aplicación del procedimiento PR-SG-SI-013 Administración de la seguridad de TI. (Paso número 3)	10%
		No disponibilidad de la información	Ejecución del procedimiento PR-SG-SI-016 Reporte, registro, categorización de incidentes que afecten la Seguridad de la Información paso 3	10%
		No disponibilidad de la información	Aplicación de la Directriz DI-025 "Administración y control de tecnologías de información (Puntos 4 y 7 del CAPÍTULO III ENTREGA Y SOPORTE)	10%
		No disponibilidad de la información	Aplicación del Plan de capacidad y desempeño PL-TI-001	30%
		No disponibilidad de la información	Aplicación del Plan de continuidad del negocio PL-SG-CO-001	40%
				100%
12	**DS10**	**Inadecuada gestión de problemas, incidentes y eventos**	Aplicación del PR-SI-CO-001 "Atenc. escalabilidad y notific. por interrup. de servic. crítico T.I." pasos del 1 al 13	30%
		Inadecuada gestión de problemas, incidentes y eventos	Aplicación del PR-TI-011 "Análisis de cambios y problemas relacionados y su afectación a la CMBD" pasos del 1 al 13.	20%
		Inadecuada gestión de problemas, incidentes y eventos	Aplicación del PR-TI-007 "Atención de incidentes y problemas que afecten servicios críticos TI" pasos del 1 al 34.	30%
		Inadecuada gestión de problemas, incidentes y eventos	Aplicación del PR-TI-006 "Reporte de incidentes a proveedores de TI" pasos del 1 al 19.	20%
				100%
13	**DS12**	**Afectaciones de instalaciones críticas por desastres naturales y/o ataques físicos**	Evaluación y verificación de la aplicación del estándar Tecnológico de Coopealianza R.L y Subsidiarias	100%
				100%
14	**DS12**	**Espacio físico insuficiente en el centro de datos subcontratado**	Aplicación del Plan de capacidad y desempeño PL-TI-001	100%
				100%
15	**ME3**	**Incumplimiento de normativas relacionadas con regulaciones y leyes**	Revisión de Auditoria Externa e interna	80%
		Incumplimiento de normativas relacionadas con regulaciones y leyes	Aplicación de la ME-SCI-CI-003 " Autoevaluación de la Gestión y el Control de Coopealianza R.L"	20%
				100%

16	DS12	**Dificultad para monitorear y verificar la administración sobre el ambiente físico subcontratado**	No existe	0%
				0%
17	DS9	**Información documentada no refleja la arquitectura actual**	Para el proceso de administración de la configuración se cuentan con herramientas como metrix (administración de licencias) y RCM (Remote Condition Management Configuration Manager -equipos de comunicación) de GCI, que suministran información al repositorio central de configuración (CMDB)	10%
		Información documentada no refleja la arquitectura actual	El Repositorio Central de Configuración contiene: hardware, software, middleware, parámetros, documentación, los procedimientos, nombre, número de versión y detalles de licenciamiento.	10%
		Información documentada no refleja la arquitectura actual	Envío anual del Perfil Tecnológico, Acuerdo SUGEF 14-09.	10%
		Información documentada no refleja la arquitectura actual	Aplicación de forma integral del Procedimiento PR-TI-OPE-001 Admin. de la configuración y revisión de la infraestructura de forma integral.	30%
		Información documentada no refleja la arquitectura actual	Aplicación del Procedimiento PR-TI-011 Análisis de cambios y problemas relacionados y su afectación a la CMBD en sus pasos 4, 5 y 7.	5%
		Información documentada no refleja la arquitectura actual	Auditorías Externas (Seguimiento oportunidades de mejora, Acuerdo SUGEF 14-09)	10%
		Información documentada no refleja la arquitectura actual	Aplicación del PR-TI-OPE-004 "CONTROL DE CAMBIOS EN APLICACIONES E INFRAESTRUCTURA SOPORTADA POR TECNOLOGÍAS DE INFORMACIÓN" en sus pasos 12,13 y 14.	20%
		Información documentada no refleja la arquitectura actual	Autoevaluación del proceso según metodología ME-SCI-CI-002 "Evaluación del marco de control de Tecnologías de Información", Capitulo VIII. RECURSOS/ 2. RECURSOS TECNOLÓGICOS/ Capitulo IX. AUTOEVALUACIÓN DE LOS CONTROLES INTERNOS DE TECNOLOGÍAS DE INFORMACIÓN.	5%
				100%

B) Votación de la frecuencia de los controles quedando de la siguiente forma:

Votaciónfrecuencia(centroDatosTI)

Responder a esta encuesta Acciones Configuración Ver: Resumen gráfico

1. 1. En el evento de riesgo (Daño en los equipos de la plataforma tecnológica) la frecuencia del control (Aplicación integral de la "Parte A Asignación de Recursos Tecnológicos, Parte B Uso de Recursos Tecnológicos" de la DI-074 "Administración, asignación y seguridad de los recursos y servicios de TI") es:

Permanente
12 (100%)
Habitual
0 (0%)
Ocasional
0 (0%)
Inexistente o Nula
0 (0%)
Total: 12

2. 2. En el evento de riesgo (Daño en los equipos de la plataforma tecnológica) la frecuencia del control (Incorporación de "Responsabilidades sobre los recursos" en el perfil del puesto) es:

Permanente
10 (83%)
Habitual
2 (17%)
Ocasional
0 (0%)
Inexistente o Nula
0 (0%)
Total: 12

3. 3. En el evento de riesgo (Daño en los equipos de la plataforma tecnológica) la frecuencia del control (Aplicación integral del procedimiento PR-TI-OPE-002 "Administración del desempeño y la capacidad") es:

Permanente
0 (0%)
Habitual
0 (0%)
Ocasional
0 (0%)
Inexistente o Nula
12 (100%)
Total: 12

4. 4. En el evento de riesgo (Daño en los equipos de la plataforma tecnológica) la frecuencia del control (Establecimiento y aplicación integral de los estándares tecnológicos) es:

Permanente
9 (75%)
Habitual
3 (25%)
Ocasional
0 (0%)
Inexistente o Nula
0 (0%)
Total: 12

5. 5. En el evento de riesgo (Daño en los equipos de la plataforma tecnológica) la frecuencia del control (Establecimiento de mecanismos de seguridad física) es:

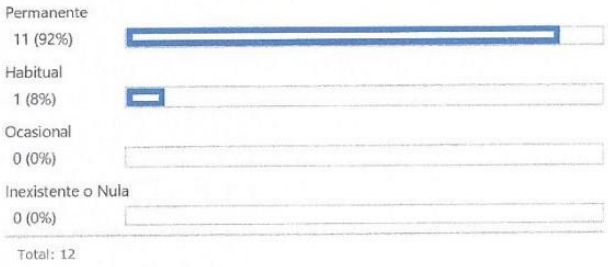
Permanente
5 (42%)
Habitual
7 (58%)

Ocasional
0 (0%)

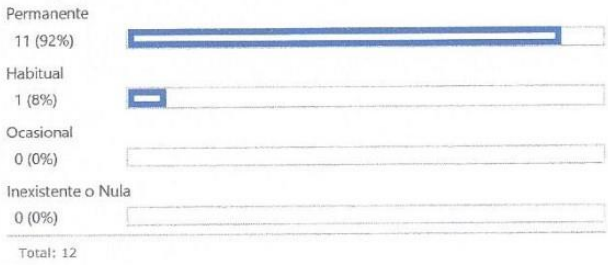
Inexistente o Nula
0 (0%)

Total: 12

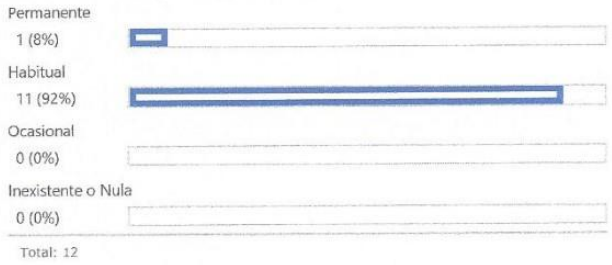
6. 6. En el evento de riesgo (Inadecuada migración y/o traslado de datos al centro de datos.) la frecuencia del control (Aplicación del procedimiento PR-TI-BD-032 "Migración de base datos Oracle") es:



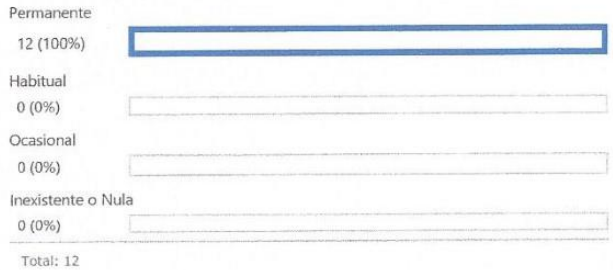
7. 7. En el evento de riesgo (Inadecuada migración y/o traslado de datos al centro de datos.) la frecuencia del control (Aplicación de la ME-AP-001 " Metodología para la administración de proyectos") es:



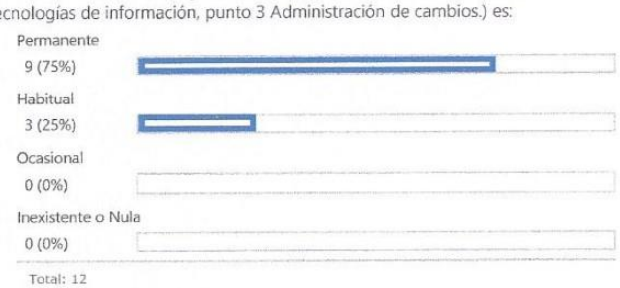
8. 8. En el evento de riesgo (Inadecuada gestión de cambios) la frecuencia del control (Aplicación del PR-TI-OPE-004 "Control de cambios en aplicaciones e infraestructura de TI" (todo el procedimiento).) es:



9. 9. En el evento de riesgo (Inadecuada gestión de cambios) la frecuencia del control (Aplicación de la Directriz DI-120 "Funcionamiento de los comités administrativos y grupos de apoyo" PARTE D: Comité de Arquitectura y PARTE G: Comité de Gestión de Proyectos y Cambios de TI.) es:



10. 10. En el evento de riesgo (Inadecuada gestión de cambios) la frecuencia del control (Aplicación de la Directriz DI-025 "Administración y control de tecnologías de información, punto 3 Administración de cambios.) es:



11. 11. En el evento de riesgo (Inadecuada gestión de cambios) la frecuencia del control (Uso de la herramienta de software de administración de cambios) es:

Permanente
5 (42%)
Habitual
7 (58%)
Ocasional
0 (0%)
Inexistente o Nula
0 (0%)
Total: 12

12. 12. En el evento de riesgo (Cierre de operaciones del proveedor del centro de datos) la frecuencia del control (Se cuenta con una ubicación geográficamente alejada para procesamiento y almacenamiento alternativo documentado en el plan de continuidad del negocio PL-SG-CO-001) es:

Permanente
12 (100%)
Habitual
0 (0%)
Ocasional
0 (0%)
Inexistente o Nula
0 (0%)
Total: 12

13. 13. En el evento de riesgo (Cierre de operaciones del proveedor del centro de datos) la frecuencia del control (Se cuenta con un diseño de red que permite que la información sea distribuida entre diferentes centros de datos documentado en el plan de continuidad del negocio PL-SG-CO-001) es:

Permanente
12 (100%)
Habitual
0 (0%)
Ocasional
0 (0%)
Inexistente o Nula
0 (0%)
Total: 12

14. 14. En el evento de riesgo (Cierre de operaciones del proveedor del centro de datos) la frecuencia del control (Se cuenta con una solución de replicación de base de datos documentado en el plan de continuidad del negocio PL-SG-CO-001) es:

Permanente
12 (100%)
Habitual
0 (0%)
Ocasional
0 (0%)
Inexistente o Nula
0 (0%)
Total: 12

15. 15. En el evento de riesgo (Personal no calificado del proveedor del centro de datos) la frecuencia del control (Aplicación del procedimiento PR-LEG-002 "Requerimiento de contrato" paso 2) es:

Permanente
9 (75%)
Habitual
3 (25%)
Ocasional
0 (0%)
Inexistente o Nula
0 (0%)
Total: 12

16. 16. En el evento de riesgo (Personal no calificado del proveedor del centro de datos) la frecuencia del control (Aplicación integral PR-SG-GPP-001 "Acreditación de proveedores de Coopealianza R.L y Subsidiarias") es:

Permanente
11 (92%)
Habitual
1 (8%)
Ocasional
0 (0%)
Inexistente o Nula

0 (0%)

Total: 12

17. 17. En el evento de riesgo (Personal no calificado del proveedor del centro de datos) la frecuencia del control (Aplicación integral PR-SG-GPP-003 "Evaluación de proveedores críticos e importantes") es:

Permanente
10 (83%)

Habitual
2 (17%)

Ocasional
0 (0%)

Inexistente o Nula
0 (0%)

Total: 12

18. 18. En el evento de riesgo (Personal no calificado del proveedor del centro de datos) la frecuencia del control (Aplicación de ME-SG-GPP-001 "Administración de servicios de terceros" en su punto 5.6 "Monitorear el desempeño de proveedores") es:

Permanente
11 (92%)

Habitual
1 (8%)

Ocasional
0 (0%)

Inexistente o Nula
0 (0%)

Total: 12

19. 19. En el evento de riesgo (Inadecuado monitoreo del desempeño del proveedor del centro de datos) la frecuencia del control (Aplicación de ME-SG-GPP-001 "Administración de servicios de terceros" en su punto 5.6 "Monitorear el desempeño de proveedores") es:

Permanente
10 (83%)

Habitual
2 (17%)

Ocasional
0 (0%)

Inexistente o Nula
0 (0%)

Total: 12

20. 20. En el evento de riesgo (Inadecuado monitoreo del desempeño del proveedor del centro de datos) la frecuencia del control (Aplicación integral PR-SG-GPP-003 "Evaluación de proveedores críticos e importantes") es:

Permanente
9 (75%)

Habitual
3 (25%)

Ocasional
0 (0%)

Inexistente o Nula
0 (0%)

Total: 12

21. 21. En el evento de riesgo (Inadecuado monitoreo del desempeño del proveedor del centro de datos) la frecuencia del control (Aplicación del procedimiento PR-LEG-002 "Requerimiento de contrato" paso 2) es:

Permanente
9 (75%)

Habitual
2 (17%)

Ocasional
1 (8%)

Inexistente o Nula
0 (0%)

Total: 12

22. 22. En el evento de riesgo (Operaciones ilícitas o fraudulentas desarrolladas por personal propio o externo) la frecuencia del control (Estándar #7 " Estándares y reglas de seguridad para aplicaciones y sistemas donde se establece la aplicación de mecanismos de autenticación de acceso al sistema.) es:

Permanente
11 (92%)

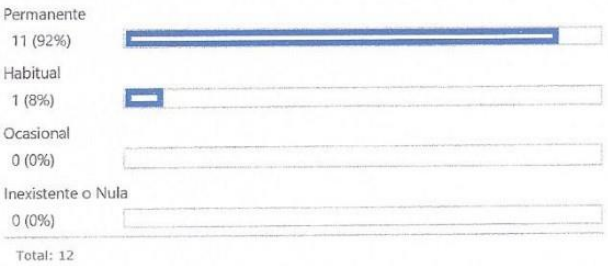
Habitual
1 (8%)

Ocasional
0 (0%)

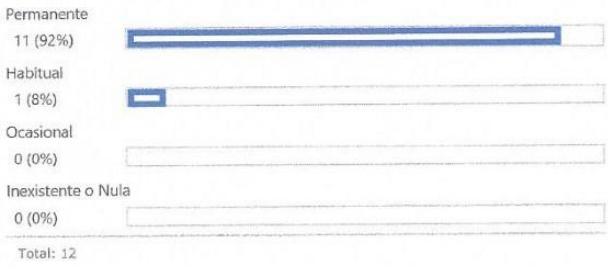
Inexistente o Nula
0 (0%)

Total: 12

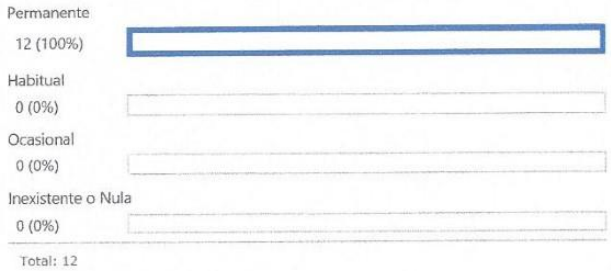
23. 23. En el evento de riesgo (Operaciones ilícitas o fraudulentas desarrolladas por personal propio o externo) la frecuencia del control (Aplicación del Plan de Seguridad de la Información donde se definen las revisiones que debe realizar el área de seguridad de la información.) es:



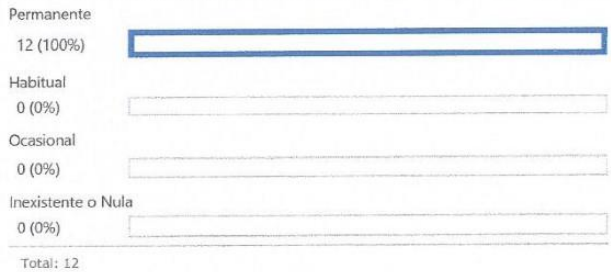
24. 24. En el evento de riesgo (Operaciones ilícitas o fraudulentas desarrolladas por personal propio o externo) la frecuencia del control (Ejecución de un mecanismo formal para la creación de usuarios, entrega de permisos y dada de baja de usuarios según procedimientos: PR-SG-SI-001 Inclusión de formas nuevas y registro y modificación de parámetros(integral), PR-SG-SI-002 Solicitud, creación e inactivación usuarios; creación, modificación, asignación y derogación de roles de acceso (integral), PR-SG-SI-003 Creación de usuarios en el dominio y los sistemas(integral), PR-SG-SI-004 Inactivación de usuarios en los sistemas(integral), PR-SG-SI-005 Creación de roles en los sistemas(integral), PR-SG-SI-006 Asignación de roles de acceso a los usuarios (integral), PR-SG-SI-007 Derogación de roles en los sistemas(integral), PR-SG-SI-008 Modificación de roles de acceso(integral), PR-SG-SI-009 Activación de usuarios en los sistemas(integral), PR-TI-BD-002 Mantenimiento de usuarios en las Bases de Datos (integral)) es:



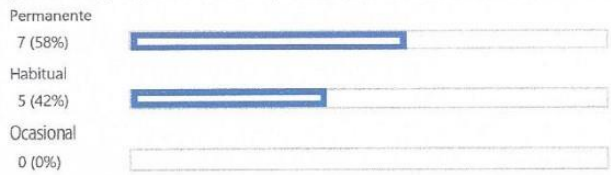
25. 25. En el evento de riesgo (Operaciones ilícitas o fraudulentas desarrolladas por personal propio o externo) la frecuencia del control (Aplicación de la directriz DI-113 donde se norma la gestión de Seguridad de la Información capítulo 5.) es:



26. 26. En el evento de riesgo (Operaciones ilícitas o fraudulentas desarrolladas por personal propio o externo) la frecuencia del control (Aplicación de la Directriz DI-025 "Administración y control de tecnologías de información(Puntos 4 y 7 del CAPÍTULO III ENTREGA Y SOPORTE)) es:



27. 27. En el evento de riesgo (Operaciones ilícitas o fraudulentas desarrolladas por personal propio o externo) la frecuencia del control (Se efectúan pruebas en conformidad con los procedimientos: PR-TI-SI-013 "Cambios: Mantenimiento-corrección y mantemiento de mejoras" (integral), y PR-TI-SI-015 "Proyectos"(integral) y PR-TI-SI-021 "Aprobación, publicación y eliminación de archivos en el servidor de aplicaciones") es:



Inexistente o Nula
0 (0%)

Total: 12

28. 28. En el evento de riesgo (Operaciones ilícitas o fraudulentas desarrolladas por personal propio o externo) la frecuencia del control (Ejecución del procedimiento PR-SG-SI-017 Monitoreo de actividades de los usuarios en los sistemas utilizados en COOPEALIANZA (Paso 4), aplica para personal interno.) es:

Permanente
8 (67%)

Habitual
3 (25%)

Ocasional
1 (8%)

Inexistente o Nula
0 (0%)

Total: 12

29. 29. En el evento de riesgo (Imposibilidad de recuperarse ante un desastre en el centro de datos) la frecuencia del control (Se cuenta con una ubicación geográficamente alejada para procesamiento y almacenamiento alternativo documentado en el plan de continuidad del negocio PL-SG-CO-001) es:

Permanente
12 (100%)

Habitual
0 (0%)

Ocasional
0 (0%)

Inexistente o Nula
0 (0%)

Total: 12

30. 30. En el evento de riesgo (Imposibilidad de recuperarse ante un desastre en el centro de datos) la frecuencia del control (Se cuenta con un diseño de red que permite que la información sea distribuida entre diferentes centros de datos documentado en el plan de continuidad del negocio PL-SG-CO-001) es:

Permanente
12 (100%)

Habitual
0 (0%)

Ocasional
0 (0%)

Inexistente o Nula
0 (0%)

Total: 12

31. 31. En el evento de riesgo (Imposibilidad de recuperarse ante un desastre en el centro de datos) la frecuencia del control (Se cuenta con una solución de replicación de base de datos documentado en el plan de continuidad del negocio PL-SG-CO-001) es:

Permanente
12 (100%)

Habitual
0 (0%)

Ocasional
0 (0%)

Inexistente o Nula
0 (0%)

Total: 12

32. 32. En el evento de riesgo (Imposibilidad de recuperarse ante un desastre en el centro de datos) la frecuencia del control (Se cuenta con un plan de continuidad que contiene una estrategia de recuperación de TI) es:

Permanente
12 (100%)

Habitual
0 (0%)

Ocasional
0 (0%)

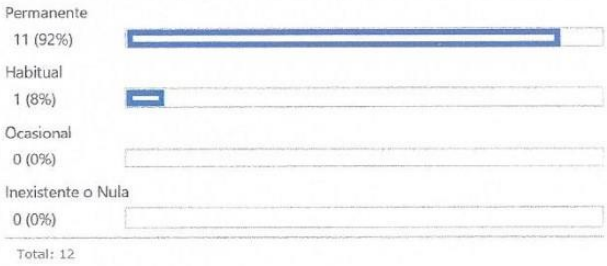
Inexistente o Nula
0 (0%)

Total: 12

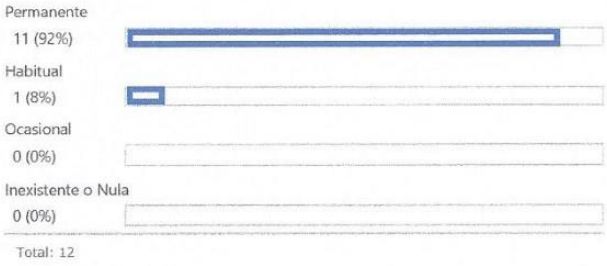
33. 33. En el evento de riesgo (Imposibilidad de recuperarse ante un desastre en el centro de datos) la frecuencia del control (Aplicación del procedimiento PR-LEG-002 "Requerimiento de contrato" paso 2) es:

Permanente
11 (92%)
Habitual
1 (8%)
Ocasional
0 (0%)
Inexistente o Nula
0 (0%)
Total: 12

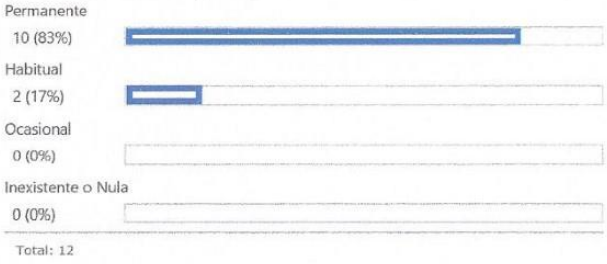
34. 34. En el evento de riesgo (Imposibilidad de recuperarse ante un desastre en el centro de datos) la frecuencia del control (Aplicación integral PR-SG-GPP-001 "Acreditación de proveedores de Coopealianza R.L y Subsidiarias") es:



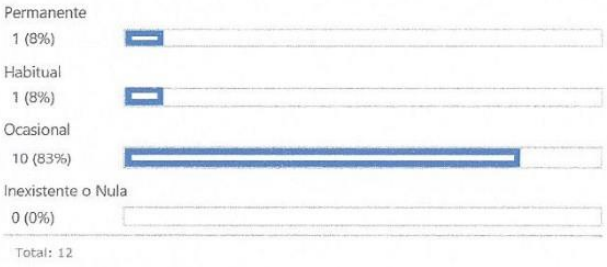
35. 35. En el evento de riesgo (Divulgación de información confidencial) la frecuencia del control (Se cuenta con acuerdos de confidencialidad con los proveedores normado en el procedimiento PR-SG-GPP-001 "Acreditación de proveedores de Coopealianza R.L y Subsidiarias" en el apartado observaciones) es:



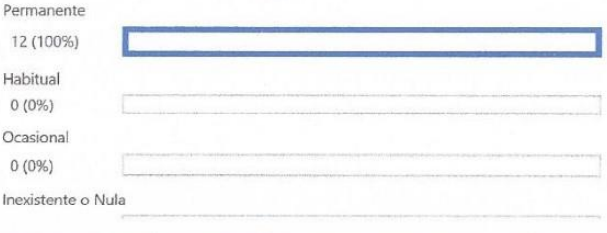
36. 36. En el evento de riesgo (Divulgación de información confidencial) la frecuencia del control (Aplicación del procedimiento PR-LEG-002 "Requerimiento de contrato" paso 7) es:



37. 37. En el evento de riesgo (Divulgación de información confidencial) la frecuencia del control (Aplicación de la metodología ME-SG-SI-001 "METODOLOGÍA CLASIFICACIÓN Y ETIQUETADO DE INFORMACIÓN EN COOPEALIANZA R.L. Y SUBSIDIARIAS" (integral),) es:



38. 38. En el evento de riesgo (Divulgación de información confidencial) la frecuencia del control (DI-113 "Directriz de seguridad de la información en COOPEALIANZA R.L. y Subsidiarias integral.) es:



0 (0%)

Total: 12

39. 39. En el evento de riesgo (Divulgación de información confidencial) la frecuencia del control (Aplicación integral del Procedimiento PR-SG-SI-018 "Atención de requerimientos Corporativos") es:

Permanente
10 (83%)

Habitual
2 (17%)

Ocasional
0 (0%)

Inexistente o Nula
0 (0%)

Total: 12

40. 40. En el evento de riesgo (Divulgación de información confidencial) la frecuencia del control (Aplicación del procedimiento PR-SG-SI-013 Administración de la seguridad de TI. (Paso número 3)) es:

Permanente
0 (0%)

Habitual
11 (92%)

Ocasional
1 (8%)

Inexistente o Nula
0 (0%)

Total: 12

41. 41. En el evento de riesgo (Divulgación de información confidencial) la frecuencia del control (Se efectúan pruebas en conformidad con los procedimientos: PR-TI-SI-013 "Cambios: Mantenimiento-corrección y mantemiento de mejoras" (integral), y PR-TI-SI-015 "Proyectos"(integral)) es:

Permanente
11 (92%)

Habitual
1 (8%)

Ocasional
0 (0%)

Inexistente o Nula
0 (0%)

Total: 12

42. 42. En el evento de riesgo (Divulgación de información confidencial) la frecuencia del control (Ejecución de un mecanismo formal para la creación de usuarios, entrega de permisos y dada de baja de usuarios según procedimientos: PR-SG-SI-001 Inclusión de formas nuevas y registro y modificación de parámetros(integral), PR-SG-SI-002 Solicitud, creación e inactivación usuarios; creación, modificación, asignación y derogación de roles de acceso (integral), PR-SG-SI-003 Creación de usuarios en el dominio y los sistemas(integral), PR-SG-SI-004 Inactivación de usuarios en los sistemas(integral), PR-SG-SI-005 Creación de roles en los sistemas(integral), PR-SG-SI-006 Asignación de roles de acceso a los usuarios (integral), PR-SG-SI-007 Derogación de roles en los sistemas(integral), PR-SG-SI-008 Modificación de roles de acceso(integral), PR-SG-SI-009 Activación de usuarios en los sistemas(integral), PR-TI-BD-002 Mantenimiento de usuarios en las Bases de Datos (integral)) es:

Permanente
12 (100%)

Habitual
0 (0%)

Ocasional
0 (0%)

Inexistente o Nula
0 (0%)

Total: 12

43. 43. En el evento de riesgo (Divulgación de información confidencial) la frecuencia del control (Ejecución del procedimiento PR-SG-SI-014 Entrega de Información Clasificada (Paso 4)) es:

Permanente
0 (0%)

Habitual
2 (17%)

Ocasional
10 (83%)

Inexistente o Nula
0 (0%)

Total: 12

44. 44. En el evento de riesgo (Divulgación de información confidencial) la frecuencia del control (Ejecución del procedimiento PR-SG-SI-016 Reporte, registro, categorización de incidentes que afecten la Seguridad de la Información paso 3) es:

Permanente
1 (8%)
Habitual
0 (0%)
Ocasional
11 (92%)
Inexistente o Nula
0 (0%)
Total: 12

45. 45. En el evento de riesgo (Divulgación de información confidencial) la frecuencia del control (Ejecución del procedimiento PR-SG-SI-017 Monitoreo de actividades de los usuarios en los sistemas utilizados en COOPEALIANZA (Paso 4)) es:

Permanente
11 (92%)
Habitual
1 (8%)
Ocasional
0 (0%)
Inexistente o Nula
0 (0%)
Total: 12

46. 46. En el evento de riesgo (Divulgación de información confidencial) la frecuencia del control (Aplicación de la Directriz DI-025 "Administración y control de tecnologías de información (Puntos 4 y 7 del CAPÍTULO III ENTREGA Y SOPORTE)) es:

Permanente
12 (100%)
Habitual
0 (0%)
Ocasional
0 (0%)
Inexistente o Nula
0 (0%)
Total: 12

47. 47. En el evento de riesgo (Pérdida de integridad de la información) la frecuencia del control (Se efectúan pruebas técnicas del sistema y de usuarios en conformidad con los procedimientos: PR-TI-SI-013 "Cambios: Mantenimiento-corrección y mantemiento de mejoras" (integral), y PR-TI-SI-015 "Proyectos"(integral)) es:

Permanente
12 (100%)
Habitual
0 (0%)
Ocasional
0 (0%)
Inexistente o Nula
0 (0%)
Total: 12

48. 48. En el evento de riesgo (Pérdida de integridad de la información) la frecuencia del control (Ejecución del procedimiento PR-SG-SI-016 Reporte, registro, categorización de incidentes que afecten la Seguridad de la Información paso 3) es:

Permanente
2 (17%)
Habitual
2 (17%)
Ocasional
8 (67%)
Inexistente o Nula
0 (0%)
Total: 12

49. 49. En el evento de riesgo (Pérdida de integridad de la información) la frecuencia del control (Ejecución del procedimiento PR-SG-SI-017 Monitoreo de actividades de los usuarios en los sistemas utilizados en COOPEALIANZA (Paso 4)) es:

Permanente
12 (100%)
Habitual
0 (0%)

Ocasional
0 (0%)

Inexistente o Nula
0 (0%)

Total: 12

50. 50. En el evento de riesgo (Pérdida de integridad de la información) la frecuencia del control (Aplicación de la Directriz DI-025 "Administración y control de tecnologías de información (Puntos 4 y 7 del CAPÍTULO III ENTREGA Y SOPORTE)) es:

Permanente
12 (100%)

Habitual
0 (0%)

Ocasional
0 (0%)

Inexistente o Nula
0 (0%)

Total: 12

51. 51. En el evento de riesgo (Pérdida de integridad de la información) la frecuencia del control (DI-113 "Directriz de seguridad de la información en COOPEALIANZA R.L. y Subsidiarias integral.) es:

Permanente
12 (100%)

Habitual
0 (0%)

Ocasional
0 (0%)

Inexistente o Nula
0 (0%)

Total: 12

52. 52. En el evento de riesgo (Pérdida de integridad de la información) la frecuencia del control (Ejecutar el conograma de pruebas del plan de continuidad PL-SG-CO-001, "Prueba de integridad y disponibilidad de los datos") es:

Permanente
12 (100%)

Habitual
0 (0%)

Ocasional
0 (0%)

Inexistente o Nula
0 (0%)

Total: 12

53. 53. En el evento de riesgo (No disponibilidad de la información) la frecuencia del control (Aplicación del procedimiento PR-SG-SI-013 Administración de la seguridad de TI. (Paso número 3)) es:

Permanente
3 (25%)

Habitual
2 (17%)

Ocasional
7 (58%)

Inexistente o Nula
0 (0%)

Total: 12

54. 54. En el evento de riesgo (No disponibilidad de la información) la frecuencia del control (Ejecución del procedimiento PR-SG-SI-016 Reporte, registro, categorización de incidentes que afecten la Seguridad de la Información paso 3) es:

Permanente
0 (0%)

Habitual
1 (8%)

Ocasional
11 (92%)

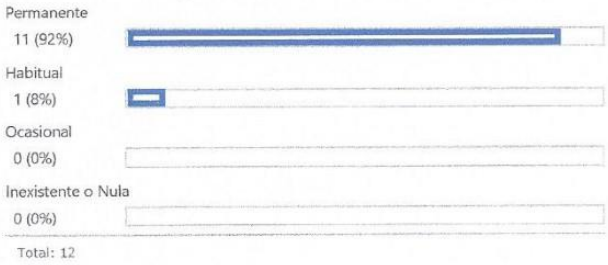
Inexistente o Nula
0 (0%)

Total: 12

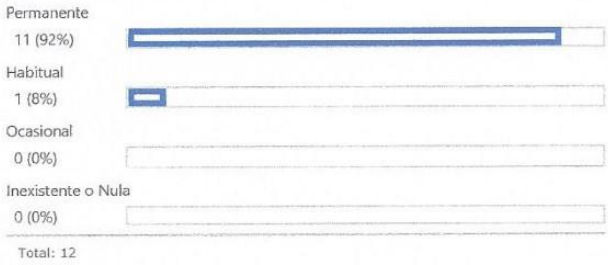
55. 55. En el evento de riesgo (No disponibilidad de la información) la frecuencia del control (Aplicación de la Directriz DI-025 "Administración y control de tecnologías de información (Puntos 4 y 7 del CAPÍTULO III ENTREGA Y SOPORTE)) es:

Permanente
12 (100%)
Habitual
0 (0%)
Ocasional
0 (0%)
Inexistente o Nula
0 (0%)
Total: 12

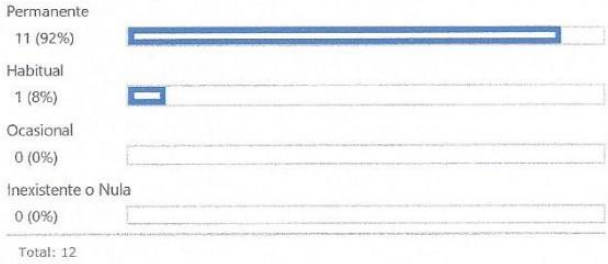
56. 56. En el evento de riesgo (No disponibilidad de la información) la frecuencia del control (Aplicación del Plan de capacidad y desempeño PL-TI-001) es:



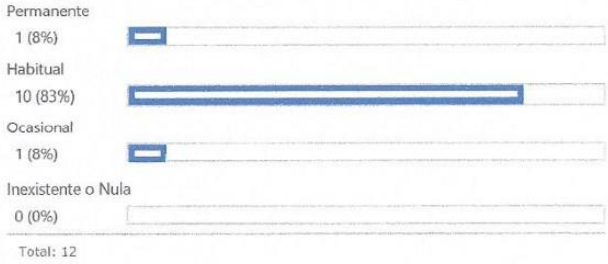
57. 57. En el evento de riesgo (No disponibilidad de la información) la frecuencia del control (Aplicación del Plan de continuidad del negocio PL-SG-CO-001) es:



58. 58. En el evento de riesgo (Inadecuada gestión de problemas, incidentes y eventos) la frecuencia del control (Aplicación del PR-SI-CO-001 "Atenc. escalabilidad y notific. por interrup. de servic. crítico T.I." pasos del 1 al 13) es:



59. 59. En el evento de riesgo (Inadecuada gestión de problemas, incidentes y eventos) la frecuencia del control (Aplicación del PR-TI-011 "Análisis de cambios y problemas relacionados y su afectación a la CMBD."pasos del 1 al 13.) es:



60. 60. En el evento de riesgo (Inadecuada gestión de problemas, incidentes y eventos) la frecuencia del control (Aplicación del PR-TI-007 "Atención de incidentes y problemas que afecten servicios críticos TI."pasos del 1 al 34.) es:

Total: 12

61. 61. En el evento de riesgo (Inadecuada gestión de problemas, incidentes y eventos) la frecuencia del control (Aplicación del PR-TI-006 "Reporte de incidentes a proveedores de TI."pasos del 1 al 19.) es:

Permanente
0 (0%)

Habitual
11 (92%)

Ocasional
1 (8%)

Inexistente o Nula
0 (0%)

Total: 12

62. 62. En el evento de riesgo (Afectaciones de instalaciones críticas por desastres naturales y/o ataques físicos) la frecuencia del control (Evaluación y verificación de la aplicación del estandar Tecnológico de Coopealianza R.L y Subsidiarias) es:

Permanente
12 (100%)

Habitual
0 (0%)

Ocasional
0 (0%)

Inexistente o Nula
0 (0%)

Total: 12

63. 63. En el evento de riesgo (Espacio físico insuficiente en el centro de datos subcontratado) la frecuencia del control (Aplicación del Plan de capacidad y desempeño PL-TI-001) es:

Permanente
1 (8%)

Habitual
0 (0%)

Ocasional
0 (0%)

Inexistente o Nula
11 (92%)

Total: 12

64. 64. En el evento de riesgo (Incumplimiento de normativas relacionadas con regulaciones y leyes) la frecuencia del control (Revisión de Auditoria Externa e interna) es:

Permanente
12 (100%)

Habitual
0 (0%)

Ocasional
0 (0%)

Inexistente o Nula
0 (0%)

Total: 12

65. 65. En el evento de riesgo (Incumplimiento de normativas relacionadas con regulaciones y leyes) la frecuencia del control (Aplicación de la ME-SCI-CI-003 " Autoevaluación de la Gestión y el Control de Coopealianza R.L") es:

Permanente
12 (100%)

Habitual
0 (0%)

Ocasional
0 (0%)

Inexistente o Nula
0 (0%)

Total: 12

66. 66. En el evento de riesgo (Dificultad para monitorear y verificar la administración sobre el ambiente físico subcontratado) la frecuencia del control (No Existe) es:

Permanente
0 (0%)

Habitual
0 (0%)

Ocasional
0 (0%)
Inexistente o Nula
12 (100%)

Total: 12

67. 67. En el evento de riesgo (Información documentada no refleja la arquitectura actual) la frecuencia del control (Para el proceso de administración de la configuración se cuentan con herramientas como metrix (administración de licencias) y RCM (Remote Condition Management Configuration Manager -equipos de comunicación) de GCI, que suministran información al repositorio central de configuración (CMDB)) es:

Permanente
12 (100%)

Habitual
0 (0%)
Ocasional
0 (0%)
Inexistente o Nula
0 (0%)
Total: 12

68. 68. En el evento de riesgo (Información documentada no refleja la arquitectura actual) la frecuencia del control (El Repositorio Central de Configuración contiene: hardware, software, middleware, parámetros, documentación, los procedimientos, nombre, numero de versión y detalles de licenciamiento.) es:

Permanente
12 (100%)

Habitual
0 (0%)
Ocasional
0 (0%)
Inexistente o Nula
0 (0%)
Total: 12

69. 69. En el evento de riesgo (Información documentada no refleja la arquitectura actual) la frecuencia del control (Envío anual del Perfil Tecnológico, Acuerdo SUGEF 14-09.) es:

Permanente
12 (100%)

Habitual
0 (0%)
Ocasional
0 (0%)
Inexistente o Nula
0 (0%)
Total: 12

70. 70. En el evento de riesgo (Información documentada no refleja la arquitectura actual) la frecuencia del control (Aplicación de forma integral del Procedimiento PR-TI-OPE-001 Admin. de la configuración y revisión de la infraestructura de forma integral.) es:

Permanente
11 (92%)

Habitual
1 (8%)

Ocasional
0 (0%)
Inexistente o Nula
0 (0%)
Total: 12

71. 71. En el evento de riesgo (Información documentada no refleja la arquitectura actual) la frecuencia del control (Aplicaciónción del Procedimiento PR-TI-011 Análisis de cambios y problemas relacionados y su afectación a la CMBD en sus pasos 4, 5 y 7.) es:

Permanente
1 (8%)

Habitual
10 (83%)

Ocasional
1 (8%)

Inexistente o Nula
0 (0%)
Total: 12

72. 72. En el evento de riesgo (Información documentada no refleja la arquitectura actual) la frecuencia del control (Auditorias Externas (Seguimiento oportunidades de mejora, Acuedo SUGEF 14-09)) es:

Permanente
10 (83%)
Habitual
2 (17%)
Ocasional
0 (0%)
Inexistente o Nula
0 (0%)
Total: 12

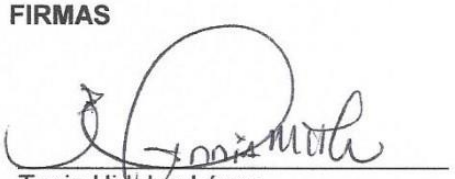
73. 73. En el evento de riesgo (Información documentada no refleja la arquitectura actual) la frecuencia del control (Aplicación del PR-TI-OPE-004 "CONTROL DE CAMBIOS EN APLICACIONES E INFRAESTRUCTURA SOPORTADA POR TECNOLOGÍAS DE INFORMACIÓN" en sus pasos 12,13 y 14.) es:

Permanente
1 (8%)
Habitual
11 (92%)
Ocasional
0 (0%)
Inexistente o Nula
0 (0%)
Total: 12

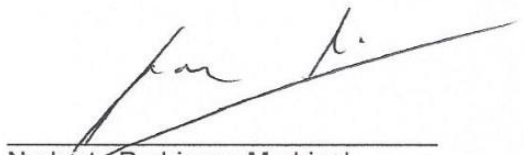
74. 74. En el evento de riesgo (Información documentada no refleja la arquitectura actual) la frecuencia del control (Autoevaluación del proceso segun metodología ME-SCI-CI-002 "Evaluación del marco de control de Tecnologías de Información", Capitulo VIII. RECURSOS/ 2. RECURSOS TECNOLÓGICOS/ Capitulo IX. AUTOEVALUACIÓN DE LOS CONTROLES INTERNOS DE TECNOLOGÍAS DE INFORMACIÓN.) es:

Permanente
11 (92%)
Habitual
1 (8%)
Ocasional
0 (0%)
Inexistente o Nula
0 (0%)
Total: 12

FIRMAS

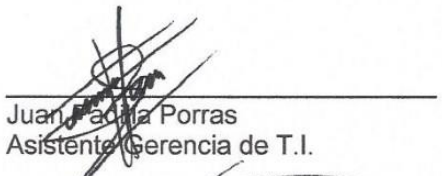


Tania Hidalgo López
Oficial de Riesgo Operativo

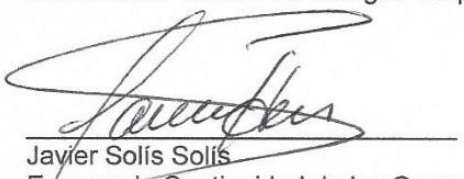


Norberto Rodriguez Madrigal
Gerente de TI

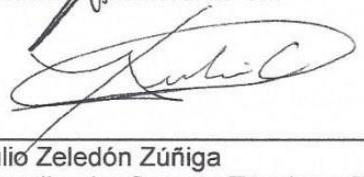
Rony Gutierrez Madrigal
Coordinador Unidad de Riesgos Corporativa



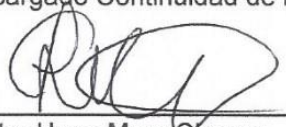
Juan Padilla Porras
Asistente Gerencia de T.I.



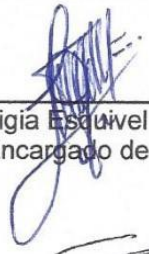
Javier Solís Solís
Encargado Continuidad de las Operaciones



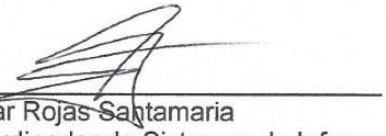
Julio Zeledón Zúñiga
Coordinador Soporte Técnico y Redes



Víctor Hugo Mora Chaves
Encargado de Seguridad de la Información

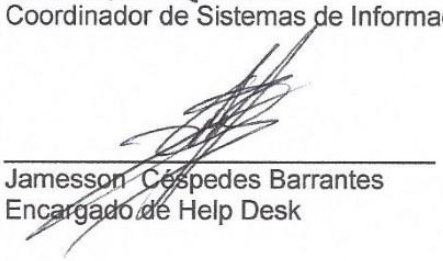


Ligia Esquivel Castro
Encargado de Gestión de Proveedores



Cidar Rojas Santamaria
Coordinador de Sistemas de Información

Ernesto Esquivel Sandí
Coordinador de Base de Datos



Jamesson Céspedes Barrantes
Encargado de Help Desk

Karen Brenes Barrantes
Encargada de Control de Procesos de TI

Unidad de Riesgos Corporativa	UNIDAD DE RIESGOS CORPORATIVA RIESGO OPERATIVO MINUTA DE REUNIÓN	MIN-RO-065-2015

FECHA REUNIÓN:	10 de Noviembre 2015	INICIO:	03:30 p.m.	FIN:	04:00 p.m.

	NOMBRE	PUESTO
PRESENTES:	Tania Hidalgo López	Oficial de Riego Operativo
	Norberto Rodríguez Madrigal	Gerente T.I.
ASUNTO:	Presentación Metodología Riesgo Operativo y TI (Traslado del procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica)	

OBJETIVO DE LA REUNIÓN: Determinación por parte del Gerente de T.I. la Naturaleza interna y/o externa, Naturaleza del impacto (+ -) y Medida a adoptar y dar a conocer los resultados de las sesiones de trabajo realizadas con el Proceso Traslado del procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica.

AGENDA

Determinación de la Naturaleza interna y/o externa
Determinación de la Naturaleza del impacto (+ -)
Determinación de la Medida a adoptar
Presentación del Mapa de Riesgos.
Presentación de la Nota obtenida por el proceso.

ACUERDOS

#1 Se definen las siguientes Naturaleza interna y/o externa, Naturaleza del impacto (+ -) y Medidas a adoptar con el proceso Traslado del procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica:

No.	RIESGO	NATURALEZA INTERNA Y/O EXTERNA	NATURALEZA DEL IMPACTO (+ -)	MEDIDA A ADOPTAR
1	Daño en los equipos de la plataforma tecnológica	Ambas	Negativo	Asumir
2	Inadecuada migración y/o traslado de datos al centro de datos.	Interna	Negativo	Asumir
3	Inadecuada gestión de cambios	Interna	Negativo	Asumir
4	Cierre de operaciones del proveedor del centro de datos	Externa	Negativo	Asumir
5	Personal no calificado del proveedor del centro de datos	Externa	Negativo	Asumir
6	Inadecuado monitoreo del desempeño del proveedor del centro de datos	Interna	Negativo	Asumir
7	Operaciones ilícitas o fraudulentas desarrolladas por personal propio o externo	Ambas	Negativo	Asumir
8	Imposibilidad de recuperarse ante un desastre en el centro de datos	Interna	Negativo	Asumir
9	Divulgación de información confidencial	Ambas	Negativo	Asumir
10	Pérdida de integridad de la información	Ambas	Negativo	Asumir
11	No disponibilidad de la información	Ambas	Negativo	Asumir
12	Inadecuada gestión de problemas, incidentes y eventos	Ambas	Negativo	Asumir
13	Afectaciones de instalaciones críticas por desastres naturales y/o ataques físicos	Externa	Negativo	Asumir
14	Espacio físico insuficiente en el centro de datos subcontratado	Ambas	Negativo	Reducir
15	Incumplimiento de normativas relacionadas con regulaciones y leyes	Ambas	Negativo	Asumir
16	Dificultad para monitorear y verificar la administración sobre el ambiente físico subcontratado	Ambas	Negativo	Reducir
17	Información documentada no refleja la arquitectura actual	Interna	Negativo	Asumir

#2 Como resultado de la aplicación de la Metodología de Riesgo Operativo y TI el proceso (Traslado del procesamiento y almacenamiento de la información crítica de COOPEALIANZA R.L a un centro de datos subcontratado en Costa Rica) obtuvo una calificación de 26.35% lo cual lo ubica en un riesgo residual Moderado.

FIRMAS

Tania Hidalgo López
Oficial de Riesgo Operativo

Norberto Rodríguez Madrigal
Gerente TI