UNIVERSIDAD DE COSTA RICA

SISTEMA DE ESTUDIOS DE POSGRADO

AUDITORÍA DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO DE LA ASOCIACIÓN.

Trabajo final de graduación sometido a la consideración de la Comisión del Programa de Estudios de Posgrado en Administración y Dirección de Empresas para optar al grado y título de Maestría Profesional en Auditoría de Tecnologías de Información y Comunicación

ALEXANDER JIMÉNEZ COTO

Ciudad Universitaria Rodrigo Facio, Costa Rica

2018

Dedicatoria

A Dios, por darme la vida y la salud.

A mis padres, José Ángel y Bernardita, que con su esfuerzo, amor y dedicación me dieron la oportunidad de estudiar y me inculcaron el valor del estudio en mi vida.

Alexander Jiménez Coto

Agradecimiento

Al profesor guía, el Doctor Sergio Espinoza y al Profesor lector; M.Sc Pedro Navarro Torres por la colaboración brindada y su ayuda en el desarrollo de la práctica profesional.

A los funcionarios de La Asociación, por brindar la oportunidad de realizar la práctica en la organización que tienen bajo su administración.

“Este trabajo final de investigación aplicada fue aceptado por la Comisión del Programa de Estudios de Posgrado en Administración y Dirección de Empresas de la Universidad de Costa Rica, como requisito parcial para optar al grado y título de Maestría Profesional en Auditoría de Tecnologías de Información y Comunicación.”

_____

Dr. Sergio Espinoza Guido

Profesor Guía

_____

M.Sc Pedro Navarro Torres

Lector

_____

Lic. Fabio Chávez Vargas

Lector de Empresa

_____

M.Sc Ridiguer Artavia Barboza

Director Programa de Posgrado en Administración y Dirección de Empresas

_____

Lic. Alexander Jiménez Coto

Sustentante

Tabla de Contenido

Resumen

La práctica profesional se realiza en una empresa de naturaleza solidarista, denominada de ahora en adelante La Asociación por temas de confidencialidad, por las características que tiene por su relación directa con la empresa de sus asociados y la identificación por parte del Gerente General de la exposición al riesgo de disponibilidad ante un evento o incidente, se decide evaluar la continuidad del negocio, tema primordial en la actualidad de la administración de La Asociación.

Para realizar la evaluación de la continuidad del negocio en La Asociación, se utiliza como base la guía de Auditoría de Gestión de Continuidad de Negocio emitida por ISACA, y se adapta realizando un cuestionario para aplicarlo en la organización.

De acuerdo a los resultados del cuestionario, se decide realizar o no pruebas de auditoría para validar las respuestas, sin embargo, la gran mayoría se responde con negación, identificando inmediatamente las áreas de mejora que tiene La Asociación en el área de la continuidad del negocio.

Al terminar la práctica, se comunican los resultados de la evaluación mediante un informe de auditoría, dirigido a la Gerencia General, que es el mayor órgano interno de La Asociación.

Lista de Tablas

Lista de Ilustraciones

Lista de Abreviaturas

ISACA: Acrónimo de Information Systems Audit and Control Association (Asociación de Auditoría y Control de Sistemas de Información).

COBIT: Acrónimo de Control Objectives for Information and related Technology (Objetivos de Control para Información y Tecnologías Relacionadas)

T.I.: Tecnología e Información

SLA: Acrónimo de Service Level Agreement (Acuerdo de nivel de servicio)

RTO: Acrónimo de Recovery Time Objective (Tiempo Objetivo de Recuperación)

RPO: Acrónimo de Recovery Point Objective (Punto Objetivo de Recuperación)

BCP: Acrónimo de Business Continuity Plan (Plan de Continuidad del Negocio)

BCM: Acrónimo de Business Continuity Management (Administración Continuidad del Negocio)

BIA: Acrónimo de Business Impact Analysis (Impacto al Negocio)

ERM: Acrónimo de (Impacto al Negocio)

Capítulo I: Aspectos Generales

Introducción

La Continuidad del Negocio es un tema que las organizaciones actualmente están dándole cada día más importancia, porque ya son conscientes de las repercusiones negativas que puede tener en sus operaciones, dejar de operar o funcionar, desde pérdida de credibilidad de sus clientes, asociados, acreedores, proveedores, hasta la quiebra, son consecuencias que pueden ir de la mano de una gestión deficiente de la continuidad del negocio.

Se aprecia fácilmente en la publicidad diaria la cantidad de empresas que ofrecen servicios de capacitaciones en el tema de continuidad, y las inversiones que realizan las empresas en planeaciones de cómo tratar incidentes de diferente tipo, son afirmaciones que reflejan que el tema de continuidad toma auge con el paso del tiempo, y las administraciones les brindan en las organizaciones el espacio que se merece, todo en pro de poder tener un manejo adecuado del negocio en marcha.

La capacidad que pueden tener las empresas para poder recuperarse ante un desastre y de re establecer el negocio de forma rápida sin mayores impactos para sus clientes, son puntos clave del análisis de continuidad que deben de realizar las organizaciones para poder tener planes que funcionen adecuadamente.

La importancia que tiene el tema de continuidad es lo que impulsa la selección del tema de la Práctica Profesional, y el desafío de poder aplicar las destrezas aprendidas en la Universidad en la evaluación de los controles, en una organización reafirma la selección del tema. Además, poder ejecutar herramientas de auditoría basados en guías diseñadas por ISACA es un aprendizaje bondadoso a nivel profesional de la Auditoría de Tecnologías de Información y Comunicación, siendo este el principal interés profesional al realizar la evaluación.

La finalidad de la evaluación es evaluar la gestión que tiene la organización para enfrentar incidentes o eventos que repercuten en la continuidad del negocio, examinarlos y emitir un informe que contenga las causas, criterios, efectos y recomendaciones de las áreas de mejora detectadas.

Objetivo General

Realizar una evaluación de la Gestión de la Continuidad del Negocio por medio de la aplicación de pruebas de auditoría para medir el grado de cumplimiento que tiene La Asociación con respecto a las buenas prácticas.

Objetivos Específicos

Diagnosticar la Gestión de la Continuidad del Negocio que tiene actualmente La Asociación, mediante cuestionarios para determinar el ambiente de control existente en la organización relacionado a la Continuidad del Negocio.

Evaluar la Gestión de la Continuidad del Negocio de La Asociación, mediante la aplicación de pruebas de auditoría para obtener el grado de cumplimiento con las buenas prácticas.

Comunicar los resultados de la evaluación de la Gestión de la Continuidad del Negocio de La Asociación, mediante un informe para trasmitir las áreas de mejora a la Gerencia General de la Organización.

Alcance de la revisión:

La auditoría tendrá un alcance sobre la Gestión de la Continuidad del Negocio de La Asociación, incluyendo políticas, normas, procedimientos, lineamientos, controles asociados y actividades que desarrollan sobre la continuidad de la operación.

Marco teórico

Las bases teóricas de la evaluación de la Continuidad del Negocio en La Asociación se basarán en el marco de control COBIT 4.1, y en la Guía de Continuidad del Negocio emitida por ISACA en el 2007. Se presenta un breve resumen de los principales conceptos a aplicar en la evaluación programada en La Asociación.

La Continuidad del Negocio es un grupo de procesos en toda la empresa y las instrucciones para asegurar la continuación de los procesos de negocio, incluyendo, pero no limitado a, Tecnología de la información, en caso de una interrupción. Proporciona los planes de la empresa para recuperarse de incidentes menores (por ejemplo, las interrupciones localizadas de componentes de negocio) a perturbaciones importantes (por ejemplo, incendios, desastres naturales, fallas de energía extendidos, equipos y / o de telecomunicaciones de fallo). (ISACA, 2011)

Los planes de continuidad son vitales para cerciorarse un adecuado proceso de reanudación y de recuperación después de un evento, y minimizar los impactos, por estas afirmaciones, un plan de continuidad debe asegurar las siguientes premisas:

a. Los riesgos están adecuadamente identificados y evaluados, centrándose en el impacto de los riesgos conocidos y potenciales en los procesos de negocio.

b. Los costos de la implementación y gestión de la garantía de la continuidad son menos de las pérdidas esperadas y dentro de la tolerancia al riesgo de la gestión.

c. Las prioridades de la empresa se abordan: las aplicaciones críticas, los procesos intermedios, las actividades de restauración y plazos obligatorios.

d. Interfaces manuales a procesos automatizados, está la Identificación del valor de la exportación, el personal está capacitado y se llevan a cabo ejercicios de práctica

e. Las expectativas son manejadas con objetivos realistas

Si el plan de continuidad asegura estas premisas, se tendrá una seguridad razonable acerca del buen funcionamiento cuando se aplique en la práctica, contando la empresa con una herramienta sumamente valiosa para mantener su operatividad ante cualquier evento.

Además, la necesidad de brindar continuidad en los servicios de TI requiere desarrollar, mantener y probar planes de continuidad de TI, almacenar respaldos fuera de las instalaciones y entrenar de forma periódica sobre los planes de continuidad, según los menciona el dominio DS4 Garantizar la Continuidad del Servicio de COBIT 4.1, IT Gobernance Institute (2007). Este concepto repercute en la necesidad de organizaciones de contar con procesos que definan los recursos necesarios que deben tener para poder manejar incidentes de continuidad en la empresa, no solamente plasmar los planes, sino probarlos es sumamente importante para que sean exitosos cuando se deben emplear en la práctica. También, muestra la necesidad de llevar a cabo entrenamientos o prácticas de los planes de continuidad, la tarea no se termina con el desarrollo, a la vez, se deben de establecer un cronograma de ejecuciones que permita probar, capacitar y entrenar a los colaboradores responsables de poner en práctica los planes cuando suceda algún evento en la organización. La importancia para las empresas es poder tener herramientas que le permitan tener la menor cantidad de impactos cuando por algún incidente se interrumpa la operación, no cabe duda, que la intención de las instituciones es poder llegar a tener control sobre los incidentes con sus planes de continuidad, en pro, de no tener impactos en sus empresas, y para poder lograrlo, COBIT 4.1., en su dominio de Garantizar la Continuidad del Servicio brinda un gran apoyo, mostrando pilares fundamentales para poder implementar una cultura y conciencia de lo importante de la continuidad a nivel empresarial. El dominio hace mención de lo importante que es mantener actualizados los planes de continuidad, un cambio en las operaciones sin mejorar los planes existentes puede ser un error

garrafal para la empresa, y las repercusiones no se harían esperar, y es lo que menos desean los administradores, por esta razón, se debe tener una práctica de actualización que permita trasmitir los cambios necesarios para que los planes funcionen adecuadamente, según los requerimientos de la organización.

Los objetivos del Dominio Garantizar la Continuidad del Servicio de COBIT 4.1 son:

DS4.1 Marco de Continuidad de TI: La empresa debe desarrollar un marco de continuidad que le permita contar con las herramientas necesarias para poder llevar a cabo planes que le permitan contra restar los impactos de las interrupciones de servicios.

DS4.2 Planes de Continuidad de TI: Los planes desarrollados deben de responder al marco de continuidad y deben de incluir aspectos de recuperación, resistencia y alternativas.

DS4.3 Recursos Críticos de TI: Se debe definir los puntos críticos de los planes de continuidad para establecer prioridades y poder atender los críticos de una manera oportuna.

DS4.4 Mantenimiento del Plan de Continuidad de TI: La definición de un procedimiento de cambios que permita mantener actualizado el plan de continuidad es una medida que la organización debe implementar para que el plan responda a las exigencias del negocio.

DS4.5 Pruebas del Plan de Continuidad de TI: Las pruebas que se deben de ejecutar para probar el plan de continuidad son básicas para detectar debilidades o ineficiencias y poderlas corregir y evitar un mal funcionamiento cuando suceda un incidente.

DS4.6 Entrenamiento del Plan de Continuidad de TI: La capacitación de los colaboradores que tienen roles y responsabilidades en el plan de continuidad es esencial para que sea exitoso en su ejecución.

DS4.7 Distribución del Plan de Continuidad de TI: La comunicación de los planes de continuidad a todos los involucrados y su disponibilidad en los eventos es clave para un proceso eficiente.

DS4.8 Recuperación y Reanudación de los Servicios de TI: Durante el tiempo de reanudación y de recuperación se deben de ejecutar los planes previamente definidos, y los responsables deben de tener claro los tiempos de respuesta y los recursos requeridos para poder ejecutar los planes de continuidad. Entre las actividades que se desarrollan son, activar sitios de respaldo, procesamientos alternativos, procesos de reanudación, comunicación a clientes, etc.

DS4.9 Almacenamientos de Respaldos Fuera de las Instalaciones: El almacenamiento externo de los recursos críticos de la organización para realizar la reanudación y planes de continuidad es esencial en el éxito ante un evento. Los responsables deben de revisar periódicamente los acuerdos de servicios con los lugares externos de almacenamiento, y se deben apegar a la política de almacenamiento, clasificación de los datos, seguridad, protección ambiental.

DS4.10 Revisión Post Reanudación: Desarrollar una revisión luego de un incidente o desastre para aplicar las lecciones aprendidas en la ejecución de los planes de continuidad y si es el caso actualizarlos, es una actividad esencial en todo el proceso.

Los objetivos son importantes tenerlos claros a la hora de gestionar la continuidad de operación en la empresa, para poder desarrollar una base de calidad e implementar los procesos necesarios y actividades que lleven a la organización a tener buenos criterios en el diseño de los planes de continuidad que requiera.

También, el Dominio Garantizar la Continuidad del Servicio de COBIT 4.1 establece las siguientes metas y métricas:

En Tecnología e Información (TI):

a. Asegurar que los servicios de TI estén disponibles cuando se requieran.

b. Asegurar un mínimo impacto al negocio en caso de una interrupción o cambios en los servicios de TI.
c. Asegurar que los servicios y la infraestructura de TI puedan resistir y recuperarse de fallas originadas por un error, ataque deliberado o desastre.

Métricas:

a. N° de horas perdidas por usuario por mes debido a interrupciones no planeadas.

En procesos:

a. Establecer un plan de continuidad de TI que soporte los planes de continuidad de negocio.
b. Desarrollar planes de continuidad de TI que puedan ejecutarse, probarse y mantenerse.
c. Minimizar la posibilidad de interrupción de los servicios de T.I.

Métricas:

a. % de SLAs de disponibilidad que se cumplen
b. N° de procesos críticos del negocio que dependen de T.I., no cubiertos por un plan de continuidad.
c. % de pruebas para lograr los objetivos de recuperación.
d. Frecuencia en la interrupción de servicios de sistemas críticos.

En actividades:

a. Desarrollar y mantener (mejorar) los planes de contingencia de T.I.
b. Entrenamiento y pruebas de los planes de contingencia.
c. Almacenamiento de copias de los planes de contingencia fuera de las instalaciones.

Métricas:

a. Tiempo trascurrido entre las pruebas de cualquier elemento dado del plan de continuidad de T.I.
b. N° de horas de entrenamiento por año de cada empleado relevante de T.I.
c. % de componentes de infraestructura críticos con monitoreo de disponibilidad automatizado.
d. Frecuencia de revisión del plan de continuidad de T.I.

En las empresas tiene importancia conocer las métricas y metas para poder auto evaluarse y poder determinar qué madurez tiene la gestión de continuidad del negocio que realizan, y así, poder valorar si deben invertir o qué cambios realizar para asegurarse que la empresa está preparada para enfrentar incidentes o eventos que requieran un proceso de reanudación y recuperación para poder seguir operando sin impactos significativos.

A la vez, COBIT 4.1 define 5 etapas de madurez, para que las empresas puedan clasificarse según el desarrollo que tenga en el tema de continuidad del negocio, y poder compararse con las buenas prácticas y de esta manera, se podrá diagnosticar en qué etapa se ubican y poder realizar medidas correctivas para mejorar. También, el auditor puede determinar el grado de madurez después de finalizada su evaluación, y se puede asignar el nivel de madurez de la organización.

Las etapas de madurez son:

0: No existe: No hay conciencia de la necesidad de tener una gestión de continuidad en la empresa.

1: Inicial / Ad Hoc: El reconocimiento de la necesidad de la gestión de continuidad del negocio es baja.

2: Repetible pero Intuitivo: Existen controles, pero sin documentar, hay debilidades y no se enfrenta adecuadamente.

3: Definido: Existen controles y documentados, se revisa la efectividad de forma periódica pero las evaluaciones no se documentan. Se revisan los controles y se documenta.

4: Administrado y Medible: Existe un entorno de control interno y de riesgos adecuado, sin embargo, no todos los problemas se detectan de forma frecuente.

5: Optimizado: Los programas de riesgos y control son eficaces y se evalúan de forma automatizada, la evaluación continua basada en autoevaluaciones, y hay una participación activa de los colaboradores en mejorar los controles.

Es importante definir el grado de madurez para tener claro el punto donde se ubica la organización en términos de continuidad del negocio, de esta manera puede planear acciones para mejorarlo si es el caso.

Un grado de madurez bajo, puede generar problemas en las empresas a la hora de desarrollar un plan de continuidad que cumpla con lo requerido para poder operar después de un incidente, y las causas que provoca que los planes no funcionen eficientemente son: (ISACA, 2011)

a. El fracaso de los planes para reflejar los cambios en las necesidades del negocio, cartera de aplicaciones, los requisitos de cumplimiento o de la tecnología.
b. Planificación y consideración de riesgo empresarial significativo inadecuada.
c. El no planificar o incapacidad para evaluar la situación e implementar procesos.
d. Los planes y procesos de recuperación inadecuados o incompletos, lo que resulta retraso en la restauración de la función empresarial.
e. Planes logísticos intermedios incompletos o no probados.
f. Formación y / o personal inadecuada no preparados para ejecutar el plan con eficacia y rapidez.
g. Recursos inadecuados o no disponibles de dotación de personal para restaurar los procesos de negocio para cumplir con los objetivos de tiempo de recuperación o de punto de recuperación (RTO, RPO).
h. La falta de control de cambio de plan, resultando en los planes de continuidad fuera de la fecha.
i. Incumplimientos regulatorios resultantes de multas o la censura.

j. El riesgo de reputación que resulta en la pérdida de confianza de los clientes.
k. Incapacidad para cumplir con el descubrimiento electrónico legal.
l. Aumento de los costos de gestión de la continuidad debido a enfoque ineficaz sobre los riesgos y costos o el fracaso de dar prioridad a la recuperación de los servicios basados en las necesidades de negocio.
m. La falta de desarrollo de escenarios de amenaza realistas que pueden potencialmente alterar los procesos de negocio.
n. La falta de consideración de todos los posibles escenarios de amenaza sobre la base de circunstancias y eventos potenciales.

Otros conceptos importantes de conocer son:

RTO: es el número máximo de horas o días en los que el sistema debe estar preparado para ejecutarlo (disponible para los negocios) después de un desastre. (ISACA, 2014)

RPO: Determina con base en la pérdida de datos aceptable en caso de una interrupción de las operaciones. Indica el punto más temprano en el tiempo que sea aceptable para recuperar los datos. El RPO cuantifica de manera efectiva la cantidad permisible de pérdida de datos en caso de interrupción. (ISACA, 2014)

BCP: Son las siglas con que se identifica el Plan de Continuidad de Negocios.

Procedimientos metodológicos

Los procedimientos metodológicos que se utilizarán incluyen la aplicación de cuestionarios cerrados, entrevistas, aplicación de pruebas de auditorías de cumplimiento, sustantivas y analíticas, según se requieran en el desarrollo de la evaluación. Además, el método de observación se utilizará si es necesario en el plan de la revisión y la recolección de datos.

Se utilizará como base la guía de evaluación de la Continuidad del Negocio emitida por ISACA.

Capítulo II:Planificación Preliminar y Diagnóstico de la Continuidad del Negocio en La Asociación

Descripción de la organización

La práctica profesional se realiza en una asociación solidarista, denominada en ahora en adelante La Asociación por confidencialidad de la información o datos que se describen y analizan en el trabajo. La organización administra los recursos de sus asociados, con un patrimonio que supera los 14 millones de dólares y más de 1 400 colaboradores activos, y con múltiples líneas de crédito y de ahorro, siendo una entidad consolidada y de un tamaño considerable.

Según la Ley de Asociaciones Solidaristas No. 6970 de Costa Rica, las Asociaciones Solidaristas son: *organizaciones sociales que se inspiran en una actitud humana, por medio de la cual el hombre se identifica con las necesidades y aspiraciones de sus semejantes, comprometiendo el aporte de los recursos y esfuerzos para satisfacer esas necesidades y aspiraciones de manera justa y pacífica. Su gobierno y su administración competen exclusivamente a los trabajadores afiliados a ellas.*

Por ser conformada La Asociación por trabajadores de una empresa, la unión entre la organización en que laboren los afiliados y La Asociación se vuelve muy fuerte, y el intercambio de actividades entre ambas instituciones es muy frecuente y constante, y en ocasiones se vuelve normal en el giro habitual de la Asociación. La facilidad de recursos que le da la empresa de los afiliados a La Asociación para que funcione por la estreches de sus lazos operacionales, por lo general de forma informal, hace que la organización no tenga respaldos sólidos a la hora de solicitar o requerir alguna actividad en especial, pero por el ahorro de costos que tiene, asumen el riesgo de esta decisión, sin embargo, más adelante analizaremos que para poder asegurar los servicios que brinda a sus asociados es importante respaldarse a nivel contractual o por medio de acuerdos de servicio (SLA) por posibles inconvenientes inesperados.

Ilustración 1 Organigrama de La Asociación

Tomado de la página de intranet de La Asociación

Valores de La Asociación

Los valores que tiene La Asociación y que replican en la cultura organizacional y por ende de primordial valor en el ambiente de control de la organización son los siguientes:

a. Servicio al cliente
b. Compromiso con el asociado
c. Amplia participación
d. Disciplina
e. Trabajo en equipo
f. Mejoramiento continuo
g. Calidad y oportunidad de servicios
h. Legalidad y moralidad en todas sus actividades
i. Respeto y trato digno al asociado

Descripción de los procesos

Los principales servicios que brinda La Asociación son relacionados a actividades financieras y sus clientes son los asociados que componen la organización, además, de administrar los recursos pertenecientes a los asociados, teniendo la necesidad de tener estados de cuenta actualizados para brindar información y datos cuando sean requeridos por sus asociados. Los principales servicios que brinda La Asociación a sus afiliados son los siguientes:

a. Líneas crediticias de diferente tipo
b. Líneas de ahorro o inversión
c. Convenios con instituciones de enseñanza, recreativas y comerciales
d. Opción de integrarse a diferentes fondos de inversión
e. Venta de artículos y diferentes productos
f. Página de Intranet que brinda al asociado información sobre su estado de cuenta, cambio de información, tramitar solicitudes de ahorro y préstamo, estatus de solicitudes.

Para poder cumplir con los servicios que brinda La Asociación es imprescindible poder contar con la disponibilidad de los recursos tecnológicos que tiene, una interrupción ante un evento es algo probable, pero la manera con que pueda volver a la normalidad y el tiempo que dure sin poder brindar el servicio es algo sumamente importante en la operación de la organización. La organización es responsable de la administración de importes significativos de sus asociados, y no poder darle datos oportunos y exactos generaría desconfianza que perjudicaría a la empresa de forma importante, efecto que no quiere asumir la Gerencia General, y para poder evitarlo, debe contar con planes de acción que le permitan asegurar razonablemente la prestación de sus servicios de forma eficiente.

Planificación preliminar

Se realiza una planeación preliminar para determinar las principales actividades que se deben de realizar en la etapa de conocimiento del negocio y generales, para obtener una comprensión general de la organización.

Programa de auditoría preliminar

AUDITOREXTERNO	**PROGRAMA DE AUDITORÍA PRELIMINAR**	Código: PA-1 Página 17 de 2 Versión: 1.0

Tipo de Auditoría: Auditoría por riesgos

Proceso a auditar: Continuidad del Negocio

Objetivo General:

Obtener información general preliminar para desarrollar un conocimiento y comprensión general de La Asociación y la Continuidad de Negocio

Tomar las principales decisiones que regirán el trabajo en la fase planificación detallada de la auditoría de Continuidad de Negocio

Definir el objetivo general de la auditoría que sea realista y alcanzable.

Tabla 1 Procedimientos Preliminares de Auditoría

No.	Procedimiento	Resultado	Referencia
1	Obtener o actualizar el conocimiento de las operaciones de La Asociación e indague sobre aspectos generales y servicios que presta la organización.	**Realizado**	Ver anexo N° 3
2	Obtener un organigrama de La Asociación.	**Realizado**	Ver Ilustración N° 1

No.	Procedimiento	Resultado	Referencia
3	Definir los objetivos de la auditoría.	**Realizado**	Ver programa de auditoría, página 20
4	Definir el alcance de la auditoría.	**Realizado**	Ver programa de auditoría página 20
5	Identificar las limitaciones y / o restricciones que afectan a la capacidad de auditar los departamentos específicos, ubicaciones o entidades.	**Realizado**	Ver anexo N° 3
6	Averiguar si el área auditada se le ha aplicado auditorías en periodos anteriores.	**Realizado**	Ver anexo N° 3
7	Entrevistar al Gerente General de La Asociación para indagar sobre el conocimiento que tiene sobre la Continuidad del Negocio, y si esta concientizado de su importancia en la organización.	**Realizado**	Ver anexo N° 3
8	Identificar si hay consciencia de la existencia del riesgo relacionado a continuidad del negocio	**Realizado**	Ver anexo N° 3
9	Preparar un cuestionario de control sobre los temas de continuidad de negocio que debe de tener La Asociación.	**Realizado**	Ver tablas de la N° 3 a la N° 10

Capítulo III: Programa de Auditoría y Aplicación de cuestionarios de la Continuidad del Negocio en La Asociación

Programa de auditoría de la continuidad de negocio

Objetivo general: Realizar una evaluación de la Gestión de la Continuidad del Negocio por medio de la aplicación de pruebas de auditoría para medir el grado de cumplimiento que tiene La Asociación con respecto a las buenas prácticas

Alcance: La auditoría comprenderá la evaluación de la razonabilidad y efectividad de los controles internos, conforme las mejores prácticas aplicables según la guía de auditoría de la continuidad del negocio.
La auditoría tendrá un alcance sobre la Gestión de la Continuidad del Negocio de La Asociación, incluyendo políticas, normas, procedimientos, lineamientos, controles asociados y actividades que desarrollan sobre la continuidad de la operación.

Riesgos y objetivos específicos asociados:

1. Disponibilidad

Factores/Eventos:

Afectación de uno o varios servicios de TI

Problemas de capacidad de tecnológica

Fallas en los procesos operativos

Fallas en los servicios de comunicación

Pérdida de información o datos históricos

Eventos por desastres naturales

Fallas por software o hardware

Fallas en la plataforma tecnológica por siniestros, accidentes

Objetivos específicos:

Determinar la existencia de un comité de continuidad de negocios con roles y responsabilidades definidas para tratar los temas de continuidad de negocios.

Validar la existencia de políticas, normas y procedimientos de continuidad del negocio.

Determinar la existencia y aplicación de un plan de continuidad de negocio que permita restaurar los sistemas de manera óptima.

Validar la existencia de una evaluación de riesgos asociados a la continuidad del negocio.

Validar si La Asociación ha definido los impactos mediante el cálculo del RTO y RPO de la organización.

Determinar la existencia de acuerdos de servicio (SLA) con los proveedores que ejecutan actividades relacionadas a la continuidad del negocio de La Asociación.

Tabla 2 Procedimientos de Auditoría

No.	Procedimientos a realizar	Resultado	Referencia
1	Aplicar los cuestionarios de la evaluación de los controles relacionados a la Continuidad de Negocio de La Asociación.	**Deficiente**	Ver tablas de la N° 3 a la N° 8
2	Aplicar el cuestionario sobre respaldo, y restauración.	**Deficiente**	Ver tablas de la N° 9 a la N° 10

Cuestionarios de Continuidad del Negocio aplicados en La Asociación

Se aplica el cuestionario diseñado para evaluar la continuidad del negocio en La Asociación, se diseña basado en la guía de auditoría emitida por ISACA, y extrayendo los puntos aplicables a La Asociación según la información que se recopila en el avance de la práctica. Se divide en varios cuestionarios según las secciones de la revisión de la continuidad de negocio. Se adjunta el resultado obtenido al aplicar los cuestionarios.

Cuestionario del Plan de Gestión de Continuidad del Negocio

Tabla 3 Cuestionario del Plan de Gestión de Continuidad del Negocio

1. Plan De Gestión de Continuidad del Negocio	Normativa referencia	Cumplimiento SÍ/ NO
1.1Organización de Gestión de la Continuidad del Negocio Objetivo: El equipo del plan de gestión de la continuidad del negocio debe estar organizado para representar a todas las funciones empresariales		**NO**
1.1.1 Organización de Gestión de la Continuidad del Negocio Control: El equipo de Continuidad del Negocio tiene un líder designado, reportando a un alto ejecutivo de organización.	**PO4.6** **DS4.1**	**NO**
1.1.1.1 ¿La Asociación tiene una comisión que se encargue de los temas de Continuidad del Negocio?		**NO**

1.1.1.2 La Asociación tiene documentos relacionados con los procesos y procedimientos a seguir por el Comité de Continuidad del Negocio (BCM)por una contingencia, la composición del grupo, la frecuencia de las reuniones, y los requisitos de comunicaciones.		**NO**
1.1.1.3 La Asociación tiene por escrito las funciones del Comité de Continuidad del Negocio, que abarquen: Gestión de equipos, Instalaciones, Tecnología, Operaciones, Comunicaciones, Terceros críticos, por ejemplo, proveedores de tecnología.		**NO**
1.1.1.4. En la Asociación existen actas de las reuniones, organigramas y otra documentación como prueba de la participación en reuniones sobre la Continuidad del Negocio.		**NO**

Cuestionario Políticas, Normas y Procedimientos de Continuidad del Negocio

Tabla 4 Cuestionario Políticas, Normas y Procedimientos

2. Políticas, Normas Y Procedimientos	Normativa referencia	Cumplimiento SÍ / NO
2.1 Política y Estándares Objetivo: Las políticas que afectan la continuidad del negocio se implementan para garantizar la integridad y cobertura adecuada de los riesgos de negocio.		**NO**
2.1.1 Definición de la Política Control: Determinar si la función del Comité de Continuidad del Negocio (BCM) participa activamente en el establecimiento de la política de continuidad de negocio.	**PO6.3** **DS4.1** **DS4.2**	**NO**
2.1.1.1 La Asociación tiene políticas y normas de la continuidad del negocio?		**NO**
2.1.1.1.1 El Comité de Continuidad del Negocio (BCM) se basa en los estándares o marcos reconocidos?		**NO**
2.1.1.1.2 Existen actas de las reuniones del Comité de Continuidad del Negocio (BCM) para verificar la participación y la comprensión de las políticas y normas de La Asociación.		**NO**
2.1.1.1.4 El Comité de Continuidad del Negocio de La Asociación ¿está involucrado en el desarrollo de políticas y normas?		**NO**

2.1.1.1.5 En La Asociación ¿existen procedimientos de aprobación y revisión de la política de Continuidad del Negocio y el Comité de Continuidad participa?		**NO**
2.2 Procedimientos Comité de Continuidad de Negocio. Objetivo: Los procedimientos de Comité de Continuidad de Negocio se definen, aplican y controlan.		**NO**
2.2.1 Procedimientos Control: Los procedimientos del Comité de Continuidad de Negocio incluyen el alcance y los objetivos.		**NO**
2.2.1.1 El Comité de Continuidad del Negocio tiene definido su alcance y objetivos.		**NO**
2.2.2 Políticas de Personal Control: Las políticas de personal se establecen y se incluyen la evaluación de habilidades y programas de capacitación para las funciones del Comité de Continuidad de Negocio.	**PO7** **DS4.3** **DS7**	**NO**
2.2.2.1 La Asociación brinda los recursos para que el Comité de Continuidad de Negocio cumpla sus funciones y tiene las competencias adecuadas para desempeñar sus tareas.		**NO**
2.2.2.2 La Asociación tiene recursos asignados a las funciones de Comité de Continuidad del Negocio para que las capacitaciones que brinda cumplan		**NO**

requisitos, horarios de entrenamiento, monitoreo y seguimiento de finalización.		
2.2.2.2.1 La Asociación ¿tiene respaldos de las capacitaciones brindadas al Comité de Continuidad de Negocio?		**NO**
2.2.2.2.2 En los respaldos de las capacitaciones se evidencia que se enfocan a las competencias deficientes del Comité de Continuidad?		**NO**
2.2.3 Respuesta a Incidentes Control: Las responsabilidades de respuesta a incidentes están claramente definidos y los ejercicios se ejecutan de forma rutinaria.	**DS4.1** **DS8.3** **DS8.4** **DS10**	**NO**
2.2.3.1 La Asociación tiene políticas y procedimientos de respuesta a incidentes?		**NO**
2.2.3.2 La Asociación ¿tiene las responsabilidades de los incidentes claramente identificadas?		**NO**
2.2.3.3 La Asociación ¿realiza simulacros de incidentes y se programan regularmente? .		**NO**
2.2.3.4Los procedimientos y políticas de Continuidad de Negocio ¿están al día y se revisan con regularidad?		**NO**

Cuestionario Evaluación de Impacto de Negocio

Tabla 5 Cuestionario Evaluación de Impacto de Negocio

3.Evaluación De Impacto de Negocios(BIA)	**Normativa referencia**	**Cumplimiento SÍ / NO**
3.1El plan de continuidad de negocio define las necesidades de La Asociación Objetivo: Un análisis exhaustivo del impacto empresariales la base para las decisiones de continuidad del negocio.		**NO**
3.1.1El plan de continuidad de negocio tiene la metodología definida. Control: Una metodología de plan de continuidad de negocio se define y ejecuta.	**DS4.1 DS4.2**	**NO**
3.1.1.1 La Asociación tiene un plan de continuidad de negocio?		**NO**
3.1.1.2Se revisan los procesos para implementar modificaciones para reflejarlos cambios en el ambiente de negocios y de procesamiento.		**NO**
3.1.1.3 La Asociación tiene definido el RTO (tiempo de recuperación) y el RPO (Objetivo de recuperación) para cada aplicación crítica.		**NO**
3.1.1.4 La Asociación evalúa si las RTO y RPO son prácticos y razonables para cada aplicación y línea de negocio o función.		**NO**

Cuestionario Evaluación del riesgo

Tabla 6 Cuestionario Evaluación del riesgo

4. Evaluación del riesgo	**Normativa referencia**	**Cumplimiento SÍ / NO**
4.1Integracióncon la Gestión de Riesgos (ERM) Objetivo: El Comité de Continuidad de Negocio es un componente integral del programa de ERM.		**NO**
4.1.1GestiónRiesgo Control: La Gerencia General debe participar en un programa de gestión activa del riesgo.	**PO9**	**NO**
4.1.1.1El Comité de Continuidad de Negocio realiza evaluaciones de riesgos anuales o más frecuentes, con base en las condiciones de negocio actuales.		**NO**
4.1.1.2Las evaluaciones de riesgo ¿incluyen las relaciones con terceros críticos?		**NO**
4.1.1.3 La Asociación monitorea las amenazas identificadas.		**NO**
4.1.1.4El Comité de Continuidad de Negocio prepara un perfil de riesgo residual e identifica riesgos significativos, y revisar los documentos para determinar la gestión de seguimiento.		**NO**
4.1.1.5Existe actas de las reuniones en que se analizó el riesgo de gestión.		**NO**

4.1.1.6El Comité de Continuidad del Negocio ¿participa en la función de gestión de riesgos?		**NO**
4.1.2Gestión de Riesgos (ERM) Control: La gestión de continuidad del negocio es un proceso dentro del ERM.	**PO9**	**NO**
4.1.2.1 ¿Existen evaluaciones de riesgos que incluyan riesgos y factores relacionados a la Continuidad del Negocio?		**NO**
4.1.2.1.1 Existen documentos de evaluación de riesgos relacionados a la Continuidad del Negocio?		**NO**

Cuestionario Documentación

Tabla 7 Cuestionario Documentación

5.Documentación	**Normativa referencia**	**Cumplimiento SÍ / NO**
5.1Documentación apropiada Objetivo: El plan de continuidad del negocio está debidamente documentado para llevar a cabo actividades comerciales eficaces y procedimientos de recuperación provisional después de una interrupción de la actividad declarada.		**NO**
5.1.1La documentación es adecuada para apoyar la Continuidad del Negocio Control: El plan de toda la continuidad del negocio está documentado y disponible durante una emergencia declarada.	**PO8 AI4 DS4.4 DS4.7**	**NO**
5.1.1.1Existe documentación del plan de continuidad del negocio.		**NO**
5.1.1.2El plan de continuidad está vigente y refleja los cambios en los procesos de negocio, el medio ambiente, la tecnología, las relaciones con terceros, contratos y requisitos regulatorios y otros de cumplimiento.		**NO**
5.2La documentación es adecuada para apoyar la recuperación		**NO**
5.2.1Documentación del Plan de Recuperación Control: El plan de recuperación de toda	**DS4.4 DS4.7**	**NO**

empresa está documentado y disponible durante una emergencia declarada.		
5.2.1.1Existe un plan de recuperación y se archiva en un lugar adecuado.		**NO**
5.2.1.2Existe documentación del plan de recuperación.		**NO**
5.2.1.3El plan de recuperación está vigente y refleja los cambios relevantes en los procesos de negocio, medio ambiente, relaciones con terceros, contratos y requisitos regulatorios y otros de cumplimiento.		**NO**

Cuestionario Plan de Pruebas

Este cuestionario aplica solamente para la actividad de respaldos y restauración, porque es solamente lo que existe de manera informal que se puede contemplar dentro de un plan de continuidad del negocio, y se seleccionaron algunos puntos para validar si cumple con lo requerido para probar si los respaldos y la restauración funciona correctamente en La Asociación.

Tabla 8 Cuestionario Plan de Pruebas

6.Plan de Pruebas del Plan de Continuidad	**Normativa referencia**	**Cumplimiento SÍ / NO**
6.1Pruebas del Plan de Continuidad Objetivo: El plan debe ser probado con regularidad, y las pruebas debería incluir una	**DS11.5 DS4.5 DS4.6**	**NO**

verificación integral de los procesos de continuidad y ejercicios situacionales para poner a prueba los supuestos y procedimientos alternativos dentro del plan.		
6.1.1Políticas de pruebas Control: Existencia de Políticas de pruebas, que definen frecuencia de prueba, tipos de pruebas, el uso de ejercicios situacionales y otros procesos reconocidos.		**NO**
6.1.1.1Existe documento formal de políticas de pruebas.		**NO**
6.1.1.2Determinarque las siguientes políticas se expresan y se documentan: La frecuencia mínima de prueba Las condiciones que requieren pruebas más frecuentes. Tipos de escenarios a ensayar		**NO**
6.1.2Existen métodos de ensayo Control: Las pruebas incluyen tutoriales y ejercicios a gran escala de los planes de procesos y recuperación provisionales.		**NO**
6.1.3Gestiónde Pruebas Control: Las pruebas del Plan de Continuidad se documentan y proporcionan la estructura para identificarlas fallas.	**DS4** **DS5** **DS9**	**NO**
6.2Los planes de recuperación se prueban periódicamente.		**NO**

Aplicación cuestionario de respaldo y restauración

En el desarrollo de la práctica, se determina la existencia de un tercero que brinda el servicio de respaldo de datos de La Asociación, por lo que se decide aplicar un cuestionario para revisar el cumplimiento de los controles básicos que debe de tener la organización. Además, se aplica un cuestionario sobre restauración.

Cuestionario de respaldo de datos

Tabla 9 Cuestionario de Respaldo

N°	Cuestionario para respaldo	Cumplimiento SÍ/ NO
	Tercerización	
1	¿Se ha tercerizado el servicio de respaldos?	**SI**
2	¿Se estableció un contrato de confidencialidad?	**NO**
3	¿Se estableció un contrato que estipulara aspectos de seguridad y gestión de los respaldos?	**NO**
4	¿Se supervisa el cumplimiento de los aspectos pactados?	**NO**
5	¿Se ha definido acuerdos de servicio sobre la tolerancia a pérdida de información y recuperación de datos?	**NO**
6	¿Los acuerdos están formalmente documentados?	**NO**
7	¿Los acuerdos están formalmente aprobados y comunicados?	**NO**

8	¿Los acuerdos están asociados con el análisis de riesgo de la organización?	**NO**

Cuestionario de restauración

Tabla 10 Cuestionario de Restauración

N°	Cuestionario de restauración	Cumplimiento SÍ / NO
	Gestión de Restauración de Datos	
1	¿Se han establecido procedimientos formales de restauración de datos? Si se responde NO, pasar a la pregunta N° 9	**NO**
2	¿Los procedimientos se basan en escenarios de restauración?	**NO**
3	¿Se actualizan de forma permanente?	**NO**
4	¿Existe un responsable formalmente asignado para esta labor?	**NO**
5	¿Está aprobada por la persona o dependencia competente?	**NO**
6	¿Se ha comunicado a todos los participantes en el proceso?	**NO**
7	¿Están alineados con el plan de continuidad de TI y del negocio?	**NO**
8	¿Se tiene definido la capacidad de procesamiento y almacenamiento requerido para la restauración completa y exitosa de la base de datos principal?	**NO**

9	¿Se tiene definido el tiempo requerido para realizar una restauración completa y exitosa de la base de datos principal?	**NO**
10	¿Existe un responsable formalmente asignado para esta labor?	**NO**
	Pruebas de restauración	
11	¿Se realizan pruebas de restauración?	**NO**
12	¿Se registran los resultados positivos o negativos de las pruebas?	**NO**
13	¿Se ha definido la frecuencia para realizar las pruebas de restauración?	**NO**
14	¿Se cuenta con un historial de pruebas de restauración?	**NO**
15	¿Existe un responsable formalmente asignado para esta labor?	**NO**
	Tercerización	
17	¿Se ha tercerizado el servicio de restauración?	**NO**

Capítulo IV: Comunicación de resultados

Informe de Auditoría

PARA: La Gerencia General

EMPRESA: La Asociación

AREA DE GESTIÓN: Administración General

OBJETIVO DE AUDITORÍA: Realizar una evaluación de la Gestión de la Continuidad del Negocio por medio de la aplicación de pruebas de auditoría para medir el grado de cumplimiento que tiene La Asociación con respecto a las buenas prácticas.

OBJETIVOS ESPECÍFICOS:

Determinar la existencia de un comité de continuidad de negocios con roles y responsabilidades definidas para tratar los temas de continuidad de negocios.

Validar la existencia de políticas, normas y procedimientos de continuidad del negocio.

Determinar la existencia y aplicación de un plan de continuidad de negocio que permita restaurar los sistemas de manera óptima.

Validar la existencia de una evaluación de riesgos asociados a la continuidad del negocio.

Validar si La Asociación ha definido los impactos mediante el cálculo del RTO y RPO de la organización.

Determinar la existencia de acuerdos de servicio (SLA) con los proveedores que ejecutan actividades relacionadas a la continuidad del negocio de La Asociación.

ALCANCE: El alcance de la auditoría parte de los resultados obtenidos mediante la aplicación de un cuestionario de Continuidad de Negocio, además para su estudio el marco de referencia COBIT 4.1, durante el periodo marzo y abril del 2015.

CRITERIOS:

COBIT 4.1.: DS4 Garantizar la Continuidad del Servicio

La necesidad de brindar continuidad en los servicios de TI requiere desarrollar, mantener y probar planes de continuidad de TI, almacenar respaldos fuera de las instalaciones y entrenar de forma periódica sobre los planes de continuidad. Un proceso efectivo de continuidad de servicios, minimiza la probabilidad y el impacto de interrupciones mayores en los servicios de TI, sobre funciones y procesos claves del negocio.

COBIT 4.1.: PO6.3 Administración de Políticas para TI

Elaborar y dar mantenimiento a un conjunto de políticas que apoyen la estrategia de TI. Estas políticas deben incluir su intención, roles y responsabilidades, procesos de excepción, enfoque de cumplimiento y referencias a procedimientos, estándares y directrices. Su relevancia se debe confirmar y aprobar en forma regular.

COBIT 4.1.: PO9.4 Evaluación de Riesgos de TI

Evaluar de forma recurrente la probabilidad e impacto de todos los riesgos identificados, usando métodos cualitativos y cuantitativos. La probabilidad e impacto asociados a los riesgos inherentes y residuales se debe determinar de forma individual, por categoría y con base en el portafolio.

COBIT 4.1.: DS1.3 Acuerdos de Niveles de Servicio

Definir y acordar convenios de niveles de servicio para todos los procesos críticos de TI con base en los requerimientos del cliente y las capacidades en TI. Esto incluye los compromisos del cliente, los requerimientos de soporte para el servicio, métricas cualitativas y cuantitativas para la medición del servicio firmado por los interesados, en caso de aplicar, los arreglos comerciales y de financiamiento, y los roles y responsabilidades, incluyendo la revisión del SLA. Los puntos a considerar son disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, niveles de soporte, planeación de continuidad, seguridad y restricciones de demanda.

COBIT 4.1.: DS11.5 Respaldo y Restauración

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

Hallazgo N° 1: Inexistencia del Comité de Continuidad del Negocio

Condición: La Asociación no cuenta con un comité formal para gestionar los temas relacionados con la continuidad del negocio por la falta de interés de la Gerencia General

Causa: Falta de una estructura definida para atender los temas de Continuidad del Negocio

Criterio: COBIT 4.1.: DS4.1 Marco de Trabajo de Continuidad de TI

Desarrollar un marco de trabajo de continuidad de TI para soportar la continuidad del negocio con un proceso consistente a lo largo de toda la organización. El objetivo del marco de trabajo es ayudar en la determinación de la resistencia requerida de la infraestructura y de guiar el desarrollo de los planes de recuperación de desastres

y de contingencias. El marco de trabajo debe tomar en cuenta la estructura organizacional para administrar la continuidad, la cobertura de roles, las tareas y las responsabilidades de los proveedores de servicios internos y externos, su administración y sus clientes; así como las reglas y estructuras para documentar, probar y ejecutar la recuperación de desastres y los planes de contingencia de TI. El plan debe también considerar puntos tales como la identificación de recursos críticos, el monitoreo y reporte de la disponibilidad de recursos críticos, el procesamiento alternativo y los principios de respaldo y recuperación.

Efectos: Atrasos en la reanudación de los servicios ante eventualidades, que genera pérdida económica a La Asociación de ¢ 106,019 por cada hora, más, cada asociado que se retire de La Asociación por pérdida de confianza y credibilidad ¢ 5,900,000 La salida normal de asociados es de 10 al mes, ante un evento que supere las 48 horas, se puede duplicar la salida de asociados, y generaría una pérdida de ¢ 118,000,000, y puede aumentar si la cantidad de asociados incrementa. Se presenta los impactos económicos según la cantidad de horas de interrupción:

Cantidad de horas de interrupción	Importe ingreso	Costos	Total
1	81,019	25,000	106,019
2	162,037	50,000	212,037
4	324,074	100,000	424,074
8	648,148	200,000	848,148
16	1,296,296	400,000	1,696,296
24	1,944,444	800,000	2,744,444
48	3,888,889	1,600,000	5,488,889

Otros efectos: Carencia de políticas, normas y procedimientos de continuidad del negocio.

Carencia de un plan de continuidad.

Falta de planes para atender siniestros o eventos.

Recomendación

Para: La Gerencia General de La Asociación

Conformar un comité de continuidad del negocio y asignarle las responsabilidades y roles requeridos para que funcione adecuadamente, según las necesidades de la organización.

Hallazgo N° 2: Inexistencia de Políticas, Normas y Procedimientos de Continuidad del Negocio.

Condición: En La Asociación no existen políticas, normas y procedimientos que regulen temas relacionados a la continuidad del negocio, por la falta de interés de la Gerencia General.

Causa: Falta de una estructura definida para atender los temas de Continuidad del Negocio por la no definición y des interés que tiene la Gerencia General.

Criterio: **COBIT 4.1.: PO6.3 Administración de Políticas para TI.**
Elaborar y dar mantenimiento a un conjunto de políticas que apoyen la estrategia de TI. Estas políticas deben incluir su intención, roles y responsabilidades, procesos de excepción, enfoque de cumplimiento y referencias a procedimientos, estándares y directrices. Su relevancia se debe confirmar y aprobar en forma regular.

Efecto: Materialización del riesgo de disponibilidad de los servicios de La Asociación por no poder gestionar adecuadamente la continuidad del negocio. La no disponibilidad de los servicios genera pérdida económica a La Asociación de ¢ 106,019 por cada hora, más, cada asociado que se retire de La Asociación por pérdida de confianza y credibilidad ¢ 5,900,000 La salida normal de asociados es

de 10 al mes, ante un evento que supere las 48 horas, se puede duplicar la salida de asociados, y generaría una pérdida de ¢ 118,000,000.

Recomendación

Para: La Gerencia General de La Asociación

Elaborar políticas, normas y procedimientos que regulen la continuidad del negocio de La Asociación, adaptados a la naturaleza de la organización y a los requerimientos diarios de operación.

Hallazgo N° 3: Carencia de un plan de continuidad de negocio.

Condición: La Asociación carece de un plan de continuidad del negocio documentado.

Causa: Falta de una estructura definida para atender los temas de Continuidad del Negocio, por el des interés de la Gerencia General sobre el tema.

Criterio: COBIT 4.1.: DS4.2 Planes de Continuidad de TI

Desarrollar planes de continuidad de TI con base en el marco de trabajo, diseñado para reducir el impacto de una interrupción mayor de las funciones y los procesos clave del negocio. Los planes deben considerar requerimientos de resistencia, procesamiento alternativo, y capacidad de recuperación de todos los servicios críticos de TI. También deben cubrir los lineamientos de uso, los roles y responsabilidades, los procedimientos, los procesos de comunicación y el enfoque de pruebas.

Efectos: Materialización del riesgo de disponibilidad de los servicios de La Asociación por no poder gestionar adecuadamente la continuidad del negocio. La no disponibilidad de los servicios genera pérdida económica a La Asociación de ¢ 106,019 por cada hora, más, cada asociado que se retire de La Asociación por pérdida de confianza y credibilidad ¢ 5,900,000 La salida normal de asociados es de 10 al mes, ante un evento que supere las 48 horas, se puede duplicar la salida de asociados, y generaría una pérdida de ¢ 118,000,000.

Otros efectos: Problemas para volver a su operación diaria después de un siniestro o evento.
Pérdida de confianza y reputación de La Asociación ante sus asociados.
Pérdida de datos e información relevante.

Recomendaciones

Para: La Gerencia General de La Asociación

Elaborar un plan de continuidad de negocios acorde a los requerimientos de la organización, que contemple lo necesario para poder enfrentar incidentes que aumenten la probabilidad de ocurrencia del riesgo de disponibilidad de los servicios de La Asociación.

Hallazgo N° 4: Sin evaluar los riesgos relacionados a la continuidad del negocio

Condición: La Asociación no evalúa los riesgos asociados a la continuidad del negocio.

Causa: Falta de una estructura definida para atender los temas de Continuidad del Negocio, por la falta de importancia e interés de la Gerencia General en la gestión de la Continuidad.

Criterio: COBIT 4.1.: PO9.4 Evaluación de Riesgos de TI

Evaluar de forma recurrente la probabilidad e impacto de todos los riesgos identificados, usando métodos cualitativos y cuantitativos. La probabilidad e impacto asociados a los riesgos inherentes y residuales se debe determinar de forma individual, por categoría y con base en el portafolio.

Efectos: Inexistencia de actividades de control para mitigar los riesgos

Falta de identificación de los factores que pueden disparar los riesgos

Falta de concientización de los colaboradores de los riesgos a que se expone La Asociación

Recomendación

Para: La Gerencia General de La Asociación

Implementar una evaluación de riesgos que permita identificar los factores que pueden llevar a materializar el riesgo o riesgos identificados en los procesos relacionados a la continuidad el negocio.

Hallazgo N° 5: Sin establecer el impacto del negocio: el objetivo de tiempo de recuperación (RTO) y el objetivo de pérdida de información (RPO) de la organización

Condición: En la organización no se definen los impactos de negocio por un problema de continuidad, no se establece el RTO ni los RPO de la organización,

que son el tiempo de recuperación que se coloca como objetivo la organización y la perdida de información que está dispuesta a perder la organización.

Causas:

Falta de una estructura definida para atender los temas de Continuidad del Negocio, por la falta de importancia y de interés de la Gerencia General en el tema de la Continuidad.

Falta de capacitación para definir los RTO y RPO de la organización.

Criterio: COBIT 4.1.: DS4.1 Marco de Trabajo de Continuidad de TI

Desarrollar un marco de trabajo de continuidad de TI para soportar la continuidad del negocio con un proceso consistente a lo largo de toda la organización. El objetivo del marco de trabajo es ayudar en la determinación de la resistencia requerida de la infraestructura y de guiar el desarrollo de los planes de recuperación de desastres y de contingencias. El marco de trabajo debe tomar en cuenta la estructura organizacional para administrar la continuidad, la cobertura de roles, las tareas y las responsabilidades de los proveedores de servicios internos y externos, su administración y sus clientes; así como las reglas y estructuras para documentar, probar y ejecutar la recuperación de desastres y los planes de contingencia de TI. El plan debe también considerar puntos tales como la identificación de recursos críticos, el monitoreo y reporte de la disponibilidad de recursos críticos, el procesamiento alternativo y los principios de respaldo y recuperación.

Efectos: Desconocimiento de los tiempos que La Asociación puede estar sin operar de sus servicios

Desconocimiento de la cantidad de datos o información que puede perder La Asociación ante un evento o siniestro.

Pérdidas económicas por interrupciones largas de la operación.

Recomendaciones

Para: La Gerencia General de La Asociación

La Asociación debe de capacitarse para poder calcular el impacto de negocio, incluyendo los RTO y RPO de la organización. Debe de comunicarlos a sus colaboradores para fomentar la concientización de la importancia de la continuidad de negocio en la organización.

Hallazgo N° 6: Carencia de acuerdos de servicio (SLA) con terceros que brindan el servicio de respaldo

Condición: Carencia de acuerdos de servicio o SLA formales con los terceros que brindan el servicio de respaldo de los datos, y con el tercero que custodia los respaldos.

Causa: Falta de una estructura definida para atender los temas de Continuidad del Negocio

Criterio: COBIT 4.1.: DS1.3 Acuerdos de Niveles de Servicio

Definir y acordar convenios de niveles de servicio para todos los procesos críticos de TI con base en los requerimientos del cliente y las capacidades en TI. Esto incluye los compromisos del cliente, los requerimientos de soporte para el servicio, métricas cualitativas y cuantitativas para la medición del servicio firmado por los interesados, en caso de aplicar, los arreglos comerciales y de financiamiento, y los roles y responsabilidades, incluyendo la revisión del SLA. Los puntos a considerar son disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, niveles de soporte, planeación de continuidad, seguridad y restricciones de demanda.

Efectos: Pérdidas económicas por interrupciones largas de la operación y atrasos en la reanudación de su operación después de un evento o siniestro.

La no disponibilidad de los servicios genera pérdida económica a La Asociación de ¢ 106,019 por cada hora, más, cada asociado que se retire de La Asociación por pérdida de confianza y credibilidad ¢ 5,900,000 La salida normal de asociados es de 10 al mes, ante un evento que supere las 48 horas, se puede duplicar la salida de asociados, y generaría una pérdida de ¢ 118,000,000.

Otros efectos: Pérdida de datos e información sensible.
Falta de garantías legales por incumplimientos de los terceros.

Recomendaciones

Para: La Gerencia General de La Asociación

Establecer acuerdos de servicio con los terceros que brindan el servicio de respaldo y custodia de datos e información, para tener una protección legal ante eventualidades y tener bien claro los roles y responsabilidades del tercero.

Hallazgo N° 7: Sin realizar pruebas de restauración y de los respaldos de datos

Condición: La Asociación no ha realizado pruebas de restauración y de respaldos de los datos respaldados.

Causas:

Falta de concientización de la importancia de los respaldos y restauración de datos por parte de la Gerencia General.
Falta de una estructura definida para atender los temas de Continuidad del Negocio.
Inexistencia de la infraestructura requerida para poder realizar las pruebas de los datos e información respaldada por el tercero.
Carencia de procedimientos de restauración de datos e información.

Criterio: COBIT 4.1.: DS11.5 Respaldo y Restauración

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

Efectos:

Pérdidas económicas por interrupciones largas de la operación y atrasos en la reanudación de su operación después de un evento o siniestro.
La no disponibilidad de los servicios genera pérdida económica a La Asociación de ¢ 106,019 por cada hora, más, cada asociado que se retire de La Asociación por pérdida de confianza y credibilidad ¢ 5,900,000 La salida normal de asociados es de 10 al mes, ante un evento que supere las 48 horas, se puede duplicar la salida de asociados, y generaría una pérdida de ¢ 118,000,000.

Otros efectos:
Pérdida de datos e información sensible.

Recomendaciones

Para: La Gerencia General de La Asociación

Implementar los recursos necesarios para poder realizar pruebas de restauración y respaldo de los datos que respalda el tercero.
Definir un cronograma de pruebas de restauración y de los datos e información de respaldo.
Definir procedimientos de restauración de datos e información.

Conclusiones

La práctica realizada tiene como objetivo evaluar la gestión de la continuidad del negocio de La Asociación, respondiendo a las necesidades y requerimientos que

tiene la empresa actualmente e identificar las áreas de mejora con el fin de mitigar el riesgo de disponibilidad ante eventualidades o factores que pueden materializar el riesgo, con el fin de asegurar poder cumplir con los servicios que brinda a sus asociados de forma oportuna y sin inconvenientes.

Mediante el cuestionario aplicado y las revisiones efectuadas en la práctica, el resultado final ha determinado áreas de mejora que La Asociación debe de atender para mitigar los factores de riesgo relacionados a la continuidad del negocio que puedan impactar la organización, porque durante la revisión se evidencia el incumplimiento de las mejores prácticas que establece el marco de control COBIT 4.1., relacionadas a la continuidad del negocio.

La Asociación presenta áreas de mejora en la implementación de un ambiente de control que permita el desarrollo y ejecución de las actividades de continuidad de negocio, y debe de dedicarle recursos a los siguientes puntos: Implementación de un Comité de Continuidad del Negocio, Elaboración de Políticas, Normas y Procesos de Continuidad del Negocio, Elaboración de un Plan de Continuidad, Valoración de Riesgos y Factores de Continuidad del Negocio, Determinación de Impactos de Negocio, los RTO y RPO de la organización y Elaboración de Acuerdos de Servicios con los Terceros.

Para asegurar de una mejor forma los servicios que brinda la organización debe de adaptar los recursos necesarios según sus requerimientos para poder mejorar el ambiente de control relacionado a la continuidad el negocio, y no tener problemas para cumplir con los objetivos institucionales.

	Nombres	Firmas
Realizado por:	Alexander Jiménez Coto	
Recibido por:	Gerente General de la Asociación	
Observaciones:	N/A	
Fecha de Presentación final	21/05/2015	

Bibliografía

ISACA (2011) *Auditoría de Gestión de Continuidad de Negocio / Programa de Aseguramiento.* Recuperado de www.isaca.org

IT Gobernance Institute (2007). *Cobit 4.1*. Recuperado de http://www.isaca.org/Knowledge-Center/cobit/Documents/cobiT4.1spanish.pdf

ISACA (2014). *Auditoría de la Continuidad del Negocio*. Recuperado de http://www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IT-Audit-Basics/Pages/Auditing-Business-Continuity.aspx

ISACA (2014). *Glosario.* Recuperado de http://www.isaca.org/KnowledgeCenter/Documents/Glossary/cism_glossary.pdf

Deloitte, I. (2010). *Guía práctica para PYMES: cómo implantar un Plan de Continuidad de Negocio.* España.

ECOE Ediciones Ltda. (2005). *Informe COSO* (Cuarta ed.). (M. B. Alberto, Trad.) Colombia.

Instituto Nacional de Tecnologías de la Comunicación (INTECO), Deloitte. (Edición 2010). *Guía práctica para PYMES: cómo implantar un Plan de Continuidad de Negocio.* España.

ISACA. (s.f.). *Cobit 5 framework.*

ISACA. (s.f.). *Normas Generales para la Auditoría de los Sistemas de Información.*

Norma ISO. (s.f.). *ISO 22301 Gestión de la Continuidad del Negocio.*

V. Anexos

Anexo N° 1: Cédula de Hallazgos

AUDITOR EXTERNO	**CÉDULA DE HALLAZGOS**	Código: PH-1
		Página 53 de 95
		Versión: 1.0

Hallazgo N° 1: Inexistencia del Comité de Continuidad del Negocio

Condición: La Asociación no cuenta con un comité formal para gestionar los temas relacionados con la continuidad del negocio.

Causa: Falta de una estructura definida para atender los temas de Continuidad del Negocio

Criterio: COBIT 4.1.: DS4.1 Marco de Trabajo de Continuidad de TI
Desarrollar un marco de trabajo de continuidad de TI para soportar la continuidad del negocio con un proceso consistente a lo largo de toda la organización. El objetivo del marco de trabajo es ayudar en la determinación de la resistencia requerida de la infraestructura y de guiar el desarrollo de los planes de recuperación de desastres y de contingencias. El marco de trabajo debe tomar en cuenta la estructura organizacional para administrar la continuidad, la cobertura de roles, las tareas y las responsabilidades de los proveedores de servicios internos y externos, su administración y sus clientes; así como las reglas y estructuras para documentar, probar y ejecutar la recuperación de desastres y los planes de contingencia de TI. El plan debe también considerar puntos tales como la identificación de recursos críticos, el monitoreo y reporte de la disponibilidad de recursos críticos, el procesamiento alternativo y los principios de respaldo y recuperación.

Efectos: Carencia de políticas, normas y procedimientos de continuidad del negocio.
Carencia de un plan de continuidad.
Atrasos en la reanudación de los servicios ante eventualidades.
Falta de planes para atender siniestros o eventos.

AUDITOR EXTERNO	**CÉDULA DE HALLAZGOS**	Código: PH-1
		Página 2 de 9
		Versión: 1.0

Recomendación

Para: La Gerencia General de La Asociación

Conformar un comité de continuidad del negocio y asignarle las responsabilidades y roles requeridos para que funcione adecuadamente, según las necesidades de la organización.

Hallazgo N° 2: Inexistencia de Políticas, Normas y Procedimientos de Continuidad del Negocio.

Condición: En La Asociación no existen políticas, normas y procedimientos que regulen temas relacionados a la continuidad del negocio.

Causa: Falta de una estructura definida para atender los temas de Continuidad del Negocio

Criterio: **COBIT 4.1.: PO6.3 Administración de Políticas para TI.**
Elaborar y dar mantenimiento a un conjunto de políticas que apoyen la estrategia de TI. Estas políticas deben incluir su intención, roles y responsabilidades, procesos de excepción, enfoque de cumplimiento y referencias a procedimientos, estándares y directrices. Su relevancia se debe confirmar y aprobar en forma regular.

Efecto: Materialización del riesgo de disponibilidad de los servicios de La Asociación por no poder gestionar adecuadamente la continuidad del negocio.

AUDITOR EXTERNO	**CÉDULA DE HALLAZGOS**	Código: PH-1
		Página 3 de 9
		Versión: 1.0

Recomendación

Para: La Gerencia General de La Asociación

Elaborar políticas, normas y procedimientos que regulen la continuidad del negocio de La Asociación, adaptados a la naturaleza de la organización y a los requerimientos diarios de operación.

Hallazgo N° 3: Carencia de un plan de continuidad de negocio.

Condición: La Asociación carece de un plan de continuidad del negocio documentado.

Causa: Falta de una estructura definida para atender los temas de Continuidad del Negocio

Criterio: COBIT 4.1.:DS4.2 Planes de Continuidad de TI de

Desarrollar planes de continuidad de TI con base en el marco de trabajo, diseñado para reducir el impacto de una interrupción mayor de las funciones y los procesos clave del negocio. Los planes deben considerar requerimientos de resistencia, procesamiento alternativo, y capacidad de recuperación de todos los servicios críticos de TI. También deben cubrir los lineamientos de uso, los roles y responsabilidades, los procedimientos, los procesos de comunicación y el enfoque de pruebas.

AUDITOR EXTERNO	**CÉDULA DE HALLAZGOS**	Código: PH-1
		Página 4 de 9
		Versión: 1.0

Efectos: Materialización del riesgo de disponibilidad de los servicios de La Asociación por no poder gestionar adecuadamente la continuidad del negocio.
Problemas para volver a su operación diaria después de un siniestro o evento.
Pérdida de confianza y reputación de La Asociación ante sus asociados.
Pérdida de datos e información relevante.
Pérdidas económicas por no ejercer su operación diaria.

Recomendaciones

Para: La Gerencia General de La Asociación

Elaborar un plan de continuidad de negocios acorde a los requerimientos de la organización, que contemple lo necesario para poder enfrentar incidentes que aumenten la probabilidad de ocurrencia del riesgo de disponibilidad de los servicios de La Asociación.

Hallazgo N° 4: Sin evaluar los riesgos relacionados a la continuidad del negocio

Condición: La Asociación no evalúa los riesgos asociados a la continuidad del negocio.

Causa: Falta de una estructura definida para atender los temas de Continuidad del Negocio.

AUDITOR EXTERNO	**CÉDULA DE HALLAZGOS**	Código: PH-1
		Página 5 de 9
		Versión: 1.0

Criterio: COBIT 4.1.: PO9.4 Evaluación de Riesgos de TI

Evaluar de forma recurrente la probabilidad e impacto de todos los riesgos identificados, usando métodos cualitativos y cuantitativos. La probabilidad e impacto asociados a los riesgos inherentes y residuales se debe determinar de forma individual, por categoría y con base en el portafolio.

Efectos: Inexistencia de actividades de control para mitigar los riesgos.
Falta de identificación de los factores que pueden disparar los riesgos.
Falta de concientización de los colaboradores de los riesgos a que se expone La Asociación.

Recomendación

Para: La Gerencia General de La Asociación

Implementar una evaluación de riesgos que permita identificar los factores que pueden llevar a materializar el riesgo o riesgos identificados en los procesos relacionados a la continuidad el negocio.

Hallazgo N° 5: Sin establecer el impacto del negocio, los RTO y RPO de la organización

Condición: En la organización no se definen los RTO ni los RPO de la organización.

AUDITOR EXTERNO	**CÉDULA DE HALLAZGOS**	Código: PH-1
		Página 6 de 9
		Versión: 1.0

Causas: Falta de una estructura definida para atender los temas de Continuidad del Negocio.
Falta de capacitación para definir los RTO y RPO de la organización.

Criterio: COBIT 4.1.: DS4.1 Marco de Trabajo de Continuidad de TI
Desarrollar un marco de trabajo de continuidad de TI para soportar la continuidad del negocio con un proceso consistente a lo largo de toda la organización. El objetivo del marco de trabajo es ayudar en la determinación de la resistencia requerida de la infraestructura y de guiar el desarrollo de los planes de recuperación de desastres y de contingencias. El marco de trabajo debe tomar en cuenta la estructura organizacional para administrar la continuidad, la cobertura de roles, las tareas y las responsabilidades de los proveedores de servicios internos y externos, su administración y sus clientes; así como las reglas y estructuras para documentar, probar y ejecutar la recuperación de desastres y los planes de contingencia de TI. El plan debe también considerar puntos tales como la identificación de recursos críticos, el monitoreo y reporte de la disponibilidad de recursos críticos, el procesamiento alternativo y los principios de respaldo y recuperación.

Efectos: Desconocimiento de los tiempos que La Asociación puede estar sin operar de sus servicios.
Desconocimiento de la cantidad de datos o información que puede perder La Asociación ante un evento o siniestro.
Pérdidas económicas por interrupciones largas de la operación.

AUDITOR EXTERNO	**CÉDULA DE HALLAZGOS**	Código: PH-1
		Página 7 de 9
		Versión: 1.0

Recomendaciones

Para: La Gerencia General de La Asociación

La Asociación debe de capacitarse para poder calcular el impacto de negocio, incluyendo los RTO y RPO de la organización. Debe de comunicarlos a sus colaboradores para fomentar la concientización de la importancia de la continuidad de negocio en la organización.

Hallazgo N° 6: Carencia de acuerdos de servicio (SLA) con terceros que brindan el servicio de respaldo

Condición: Carencia de acuerdos de servicio o SLA formales con los terceros que brindan el servicio de respaldo de los datos, y con el tercero que custodia los respaldos.

Causa: Falta de una estructura definida para atender los temas de Continuidad del Negocio.

Criterio: COBIT 4.1.: DS1.3 Acuerdos de Niveles de Servicio

Definir y acordar convenios de niveles de servicio para todos los procesos críticos de TI con base en los requerimientos del cliente y las capacidades en TI. Esto incluye los compromisos del cliente, los requerimientos de soporte para el servicio, métricas cualitativas y cuantitativas para la medición del servicio firmado por los interesados, en caso de aplicar, los arreglos comerciales y de financiamiento;

AUDITOR EXTERNO	**CÉDULA DE HALLAZGOS**	Código: PH-1
		Página 9 de 9
		Versión: 1.0

y los roles y responsabilidades, incluyendo la revisión del SLA. Los puntos a considerar son disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, niveles de soporte, planeación de continuidad, seguridad y restricciones de demanda.

Efectos: Pérdida de datos e información sensible.
Atrasos en la reanudación de sus operaciones después de un evento o siniestro.
Pérdidas económicas por interrupciones largas de la operación.
Falta de garantías legales por incumplimientos de los terceros.

Recomendaciones

Para: La Gerencia General de La Asociación

Establecer acuerdos de servicio con los terceros que brindan el servicio de respaldo y custodia de datos e información, para tener una protección legal ante eventualidades y tener bien claro los roles y responsabilidades del tercero.

Hallazgo N° 7: Sin realizar pruebas de restauración y de los respaldos de datos

Condición: La Asociación no ha realizado pruebas de restauración y de respaldos de los datos respaldados.

Causas: Falta de una estructura definida para atender los temas de Continuidad del Negocio.
Inexistencia de la infraestructura requerida para poder realizar las pruebas de los datos e información respaldada por el tercero.
Carencia de procedimientos de restauración de datos e información.

AUDITOR EXTERNO	**CÉDULA DE HALLAZGOS**	Código: PH-1
		Página 9 de 9
		Versión: 1.0

Criterio: COBIT 4.1.: DS11.5 Respaldo y Restauración

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

Efectos: Pérdida de datos e información sensible.
Atrasos en la reanudación de sus operaciones después de un evento o siniestro.
Pérdidas económicas por interrupciones largas de la operación.

Recomendaciones

Para: La Gerencia General de La Asociación

Implementar los recursos necesarios para poder realizar pruebas de restauración y respaldo de los datos que respalda el tercero.
Definir un cronograma de pruebas de restauración y de los datos e información de respaldo.
Definir procedimientos de restauración de datos e información.

Revisado por	Alexander Jiménez Coto	Fecha: 10/05/2015

Anexo N° 2: Impactos económicos de los hallazgos

AUDITOR EXTERNO	**TABLA DE IMPACTOS ECONÓMICOS**	Código: PH-2
		Página 1 de 2
		Versión: 1.0

Tabla 11 Detalle de ingresos

Se presenta el detalle de los ingresos netos anuales, la cantidad de asociados, el ingreso por hora, por día y el ingreso generado por asociado anualmente, para cuantificar los impactos de las observaciones en el informe de resultados.

Detalle	Importe / Cantidad
Ingresos netos anual	¢ 700,000,000
Cantidad de Asociados	1,400
Ingreso neto por día	¢ 1,944,444
Ingreso neto por hora	¢ 81,019
Ingreso generado por asociado anual	¢ 500,000

Tabla 12 Detalle de patrimonio

Se presenta el detalle por el aporte promedio que realiza cada asociado a la Asociación.

Detalle	Importe / Cantidad
Patrimonio	¢ 7,560,000,000
Cantidad de asociados	1,400
Patrimonio promedio por asociado	¢ 5,400,000

Tabla 13 Detalle por cantidad de asociados (ingresos más aporte patrimonio)

Se presenta el detalle por el aporte en ingresos más patrimonio promedio que realiza cada asociado a La Asociación.

Cantidad de asociados	Importe ingreso	Importe patrimonio	Total
1	¢ 500,000	¢ 5,400,000	¢ 5,900,000
2	¢ 1,000,000	¢ 10,800,000	¢ 11,800,000
4	¢ 2,000,000	¢ 21,600,000	¢ 23,600,000
8	¢ 4,000,000	¢ 43,200,000	¢ 47,200,000
10	¢ 5,000,000	¢ 54,000,000	¢ 59,000,000

Tabla 14 Detalle por cantidad de horas interrumpidas (ingresos más costos)

Se presenta el detalle de la pérdida económica por horas por interrupción de eventos que tiene La Asociación. A esta pérdida, se le debe de sumar la pérdida por la cantidad de Asociados que estará perdiendo La Asociación por la des confianza y la imagen negativa que genera eventos largos sin brindar los servicios, que se puede catalogar superiores a 24 horas.

Cantidad de horas de interrupción	Importe ingreso	Costos	Total
1	¢ 81,019	¢ 25,000	¢106,019
2	¢ 162,037	¢ 50,000	¢212,037
4	¢ 324,074	¢ 100,000	¢ 424,074
8	¢ 648,148	¢ 200,000	¢ 848,148
16	¢ 1,296,296	¢ 400,000	¢ 1,696,296
24	¢ 1,944,444	¢ 800,000	¢ 2,744,444
48	¢ 3,888,889	¢1,600,000	¢ 5,488,889

Anexo N° 3: Entrevista General

AUDITOR EXTERNO	**CÉDULA DE ENTREVISTA**	Código: PE-1
		Página 64 de 8
		Versión: 1.0

Preguntas generales

1. ¿Se han realizado auditorías de continuidad de negocio?

No

2. ¿La Asociación tiene organigrama, me puede brindar una copia?

Sí.

3. ¿Existirá limitaciones y / o restricciones que afectan a la capacidad de auditar la continuidad del negocio?

No.

4. ¿Tienes identificado que riesgo se expone La Asociación con respecto a la continuidad del negocio?

Sí, sería la disponibilidad, porque es una empresa de servicio a sus asociados, y de forma diaria tenemos que tener las operaciones disponibles para los colaboradores que forman parte de la organización.

5. ¿Tiene conocimiento del concepto continuidad del negocio?

(X) SÍ ( ) NO

AUDITOR EXTERNO	**CÉDULA DE ENTREVISTA**	Código: PE-1
		Página 2 de 8
		Versión: 1.0

6. En caso de un eventual incidente ¿cuenta dentro de la organización con alguien encargado de coordinar, que gestione un plan de continuidad? De ser afirmativo, ¿a quién le corresponde dicho rol?

( ) SÍ (X) NO

7. ¿La organización cuenta con algún tipo de documento que establezca la actuación, responsabilidades u otros en caso de incidentes? En caso de ser afirmativo que información o estructura contiene básicamente.

( ) SÍ (X) NO

8. ¿Cuáles son sus productos y servicios clave?

Líneas crediticias de diferente tipo

Líneas de ahorro o inversión

Convenios con instituciones de enseñanza, recreativas y comerciales

Opción de integrarse a diferentes fondos de inversión

Venta de artículos y diferentes productos

Página de Intranet que brinda al asociado información sobre su estado de cuenta, cambio de información, tramitar solicitudes de ahorro y préstamo, estatus de solicitudes

AUDITOR EXTERNO	**CÉDULA DE ENTREVISTA**	Código: PE-1
		Página 3 de 8
		Versión: 1.0

9. ¿Qué impacto tendría en la organización la interrupción de alguno de estos productos o servicios claves? ¿El impacto lo tiene cuantificado económicamente?

No lo tengo cuantificado económicamente, sin embargo, no es conveniente por la imagen de la empresa y la confianza que tienen los asociados sobre el funcionamiento de la organización.

10. Actualmente, ¿se realiza alguna metodología de valoración de riesgos? ¿Cuál? ¿Con qué frecuencia se realiza?

No.

11. ¿La empresa tiene alguna alternativa o plan de recuperación ante un incidente, desastre?

(X) SÍ ( ) NO

Sí su respuesta es SI indicar cuáles son:

La Asociación en relación con los eventos de pérdida de datos tiene un tercero que le brinda el servicio de respaldo de los datos del servidor de la organización, sin embargo, no da el servicio de restauración.

Además, las cintas de respaldo se custodian en un tercero que brinda el servicio.

Sí su respuesta es SÍ, indicar si tiene una estrategia de recuperación por escrito para realizar los planes de recuperación:

No existe por escrito la estrategia de recuperación.

AUDITOR EXTERNO	**CÉDULA DE ENTREVISTA**	Código: PE-1
		Página 4 de 8
		Versión: 1.0

12. ¿Conoce el concepto de: *El Tiempo Máximo Permitido de Interrupción (MTD) de la actividad crítica*?

( ) SÍ (X) NO

Sí su respuesta es SÍ, indicar si la empresa lo tiene y como lo cálculo:

13. ¿Conoce el concepto de: *El Tiempo de Recuperación Objetivo (RTO)*?

( ) SÍ

(X) NO

Sí su respuesta es SÍ, indicar si la empresa lo tiene y como lo cálculo:

14. ¿Conoce el concepto de: *La pérdida máxima de información que una empresa se puede permitir (RPO*) ?

( ) SÍ (X) NO

Sí su respuesta es SÍ, indicar si la empresa lo tiene y como lo cálculo:

15. Marque las opciones que se encuentran en la empresa (no necesariamente es una persona por cada opción):

( ) Responsable de analizar y acotar el impacto de un incidente en la empresa.

( ) Encargado de activar el plan de continuidad del negocio en caso de una contingencia.

( ) Responsable de reunir los medios necesarios para la reactivación de la actividad

( ) Responsable de la recuperación de la infraestructura dañada.

AUDITOR EXTERNO	**CÉDULA DE ENTREVISTA**	Código: PE-1
		Página 5 de 8
		Versión: 1.0

16. ¿Existen planes en la empresa documento(s) de manera que les permita a los empleados tener el conocimiento necesario para poder darle continuidad al negocio, los cuales están escritos de manera que sean fáciles de leer y entender por todos los miembros del staff? ¿Este documento incluye las actividades y recursos críticos que deben ser recuperados; los tiempos de recuperación de dichas actividades y recursos; cuando deben ser utilizados y la información útil para la gestión de la contingencia (teléfonos, inventarios de proveedores, servicios) ?

No existe documentación física.

RESPUESTA A INCIDENTES

¿Existe un plan de respuesta a cualquier incidente que le permita confirmar el tipo de incidente y su criticidad? A tomar el control de la situación y acotar o limitar el impacto que dicho incidente puede provocar?

No existe ningún plan.

AUDITOR EXTERNO	**CÉDULA DE ENTREVISTA**	Código: PE-1
		Página 6 de 8
		Versión: 1.0

PROCEDIMIENTOS DE RECUPERACIÓN

17. Se tiene definido, cuando se aplica el plan de respuesta a incidentes, los siguientes puntos:

( ) Quién, cómo y bajo qué circunstancias debe ser activado

( ) Persona/s que deben ser informadas de la activación del plan de continuidad en primer lugar

( ) Localización física de las personas que intervienen en el plan

( ) Qué servicios están disponibles, cuándo y dónde

( ) En qué momento y de qué forma la información que se genera en la ejecución del plan de continuidad es transmitida a responsables, empleados, unidades de dirección, etc.

No existe un plan de recuperación.

PLAN DE VUELTA A LA NORMALIDAD

18. ¿Existe un plan con los mecanismos necesarios para recuperar la normalidad de funcionamiento y el “día a día” de las actividades?

No existe un plan para recuperar y volver a la normalidad de las operaciones ante un evento.

AUDITOR EXTERNO	**CÉDULA DE ENTREVISTA**	Código: PE-1
		Página 7 de 8
		Versión: 1.0

DISPONER DE LOS MEDIOS Y RECURSOS NECESARIOS PARA EJECUTAR EL PLAN DE CONTINUIDAD DE NEGOCIO

19. Se tiene definido, en caso de un incidente, los medios y recursos necesarios para aplicar el plan de continuidad del negocio que incluya:

• Servicios generales, medios materiales, transporte, medios de almacenamiento, etc.

• Tecnología (servidores, dispositivos móviles) y comunicaciones.

• Recursos humanos y puestos de trabajo alternativos.

• Información crítica redundante y necesaria para el desarrollo de las actividades de negocio.

No existe un plan de continuidad de negocio.

AUDITOR EXTERNO	**CÉDULA DE ENTREVISTA**	Código: PE-1
		Página 8 de 8
		Versión: 1.0

EJECUCIÓN DE PRUEBAS

20. ¿Se realizan simulacros, test o ejercicios para confirmar/mejorar los planes existentes antes que suceda un incidente?

No existen planes.

Lo que existe es el proveedor que brinda el servicio de respaldo de los datos, sin embargo, no se han realizado pruebas para validar si funcionan correctamente las cintas en donde se almacena la información respaldada.

Además, no se cuenta con los recursos necesarios para hacer las pruebas, sin embargo, se puede implementar para planear la realización d pruebas.

Anexo N° 4: Objetivos de Control DS4 Garantizar la Continuidad del Negocio COBIT 4.1

DS4.1 Marco de Trabajo de Continuidad de TI

Desarrollar un marco de trabajo de continuidad de TI para soportar la continuidad del negocio con un proceso consistente a lo largo de toda la organización. El objetivo del marco de trabajo es ayudar en la determinación de la resistencia requerida de la infraestructura y guiar el desarrollo de los planes de recuperación de desastres y contingencias. El marco de trabajo debe tomar en cuenta la estructura organizacional para administrar la continuidad, la cobertura de roles, las tareas y las responsabilidades de los proveedores de servicios internos y externos, su administración y sus clientes; así como las reglas y estructuras para documentar, probar y ejecutar la recuperación de desastres y los planes de contingencia de TI. El plan debe también considerar puntos tales como
la identificación de recursos críticos, el monitoreo y reporte de la disponibilidad de recursos críticos, el procesamiento alternativo y los principios de respaldo y recuperación.

DS4.2 Planes de Continuidad de TI

Desarrollar planes de continuidad de TI con base en el marco de trabajo, diseñado para reducir el impacto de una interrupción mayor de las funciones y los procesos clave del negocio. Los planes deben considerar requerimientos de resistencia, procesamiento alternativo, y capacidad de recuperación de todos los servicios críticos de TI. También deben cubrir los lineamientos de uso, los roles y responsabilidades, los procedimientos, los procesos de comunicación y el enfoque de pruebas.

DS4.3 Recursos Críticos de TI

Centrar la atención en los puntos determinados como los más críticos en el plan de continuidad de TI, para construir resistencia y establecer prioridades en situaciones de recuperación. Evitar la distracción de recuperar los puntos menos críticos y asegurarse de que la respuesta y la recuperación están alineadas con las necesidades prioritarias del negocio, asegurándose también que los costos se mantienen a un nivel aceptable y se cumple con los requerimientos regulatorios y contractuales. Considerar los requerimientos de resistencia, respuesta y recuperación para diferentes niveles de prioridad, por ejemplo, de una a cuatro horas, de cuatro a 24 horas, más de 24 horas y para periodos críticos de operación del negocio.

DS4.4 Mantenimiento del Plan de Continuidad de TI

Exhortar a la gerencia de TI a definir y ejecutar procedimientos de control de cambios, para asegurar que el plan de continuidad de TI se mantenga actualizado y que refleje de manera continua los requerimientos actuales del negocio. Es esencial que los cambios en los procedimientos y las responsabilidades sean comunicados de forma clara y oportuna.

DS4.5 Pruebas del Plan de Continuidad de TI

Probar el plan de continuidad de TI de forma regular para asegurar que los sistemas de TI pueden ser recuperados de forma efectiva, que las deficiencias son atendidas y que el plan permanece aplicable. Esto requiere una preparación cuidadosa, documentación, reporte de los resultados de las pruebas y, de acuerdo con los resultados, la implementación de un plan de acción. Considerar el alcance de las pruebas de recuperación en aplicaciones individuales, en escenarios de pruebas integrados, en pruebas de punta a punta y en pruebas integradas con el proveedor.

DS4.6 Entrenamiento del Plan de Continuidad de TI

Asegurarse que todas las partes involucradas reciban sesiones de entrenamiento de forma regular respecto a los procesos y sus roles y responsabilidades en caso de incidente o desastre. Verificar e incrementar el entrenamiento de acuerdo con los resultados de las pruebas de contingencia.

DS4.7 Distribución del Plan de Continuidad de TI

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

DS4.8 Recuperación y Reanudación de los Servicios de TI

Planear las acciones a tomar durante el período en que TI está recuperando y reanudando los servicios. Esto puede representar la activación de sitios de respaldo, el inicio de procesamiento alternativo, la comunicación a clientes y a los interesados, realizar procedimientos de reanudación, etc. Asegurarse de que los responsables del negocio entienden los tiempos de recuperación de TI y las inversiones necesarias en tecnología para soportar las necesidades de recuperación y reanudación del negocio.

DS4.9 Almacenamiento de Respaldos Fuera de las Instalaciones

Almacenar fuera de las instalaciones todos los medios de respaldo, documentación y otros recursos de TI críticos, necesarios para la recuperación de TI y para los planes de continuidad del negocio. El contenido de los respaldos a almacenar debe determinarse en conjunto entre los responsables de los procesos de negocio y el

personal de TI. La administración del sitio de almacenamiento externo a las instalaciones, debe apegarse a la política de clasificación de datos y a las prácticas de almacenamiento de datos de la empresa. La gerencia de TI debe asegurar que los acuerdos con sitios externos sean evaluados periódicamente, al menos una vez por año, respecto al contenido, a la protección ambiental y a la seguridad. Asegurarse de la compatibilidad del hardware y del software para poder recuperar los datos archivados y periódicamente probar y renovar los datos archivados.

DS4.10 Revisión Post Reanudación

Una vez lograda una exitosa reanudación de las funciones de TI después de un desastre, determinar si la gerencia de TI ha establecido procedimientos para valorar lo adecuado del plan y actualizar el plan en consecuencia.

Anexo N°5: Guía de Auditoría de Continuidad del Negocio emitida por ISACA

Auditoría / Programa	Norma COBIT 4.1
1. Planificación y alcance la auditoría de continuidad de negocio	
1.1 Definir los objetivos de auditoría Los objetivos de auditoría son de alto nivel y designa los objetivos generales de la auditoría.	
1.1.1 Revisión de los objetivos de auditoría en la introducción a esta gestión de continuidad de negocio (BCM)	
1.2 Definir los límites de la revisión La revisión debe tener un alcance definido. El revisor debe entender el entorno operativo y preparar una propuesta de alcance, sujeto a una evaluación de riesgos	
1.2.1 Obtener la documentación de la política BCM	
1.2.2 Obtener y revisar los planes de BCM de la empresa.	
1.2.3 Determinar si la auditoría BCM incluirá la empresa o limitarse a las unidades de negocio específicas	
1.2.4 Identificar las limitaciones y/o restricciones que afectan a la capacidad de auditar los departamentos específicos, ubicaciones o entidades.	
1.3 Identificar y documentar la Auditoría de Riesgos La evaluación de riesgos es necesaria evaluarla para determinar en qué se debe centrar la auditoría y como se utilizarán los recursos. El enfoque basado en el riesgo asegura la utilización más eficaz de los recursos de la auditoría.	
1.3.1 Determinar si la calificación de la evaluación del riesgo asignado por el departamento de auditoría son razonables.	
1.3.2 Evaluar el perfil de riesgo general para la realización de la revisión.	
1.3.3 Determinar si las auditorías de BCM se han realizado previamente. En caso afirmativo, entonces determinar lo siguiente.	
1.3.3.1 Determinar el estado de los problemas previamente identificados.	
1.3.3.2 Determinar si el estado de los problemas previamente identificados requiere un ajuste a la calificación de riesgo de auditoría y la prioridad de la auditoría.	
1.3.4 Sobre la base de la evaluación del riesgo de auditoría, identificar cambios en el alcance.	
1.3.5 Analizar los riesgos con una gestión adecuada, y ajustar la evaluación de riesgos de auditoría, según sea necesario.	
1.4 Definir la Auditoría y proceso de cambio o ajustes	

El enfoque de la auditoría inicial se basa en el entendimiento del revisor del entorno operativo y los riesgos asociados. A medida que se realizan más investigaciones y análisis, tendrán como resultado cambios o ajustes en el alcance y enfoque.	
1.4.1 Identificar el recurso de aseguramiento superior responsable de la revisión.	
1.4.2 Establecer el proceso para sugerir e implementar cambios en el programa de auditoría / garantía de BCM y las autorizaciones necesarias.	
1.5 Definir el éxito. La asignación de los factores de éxito deben ser identificados.	
1.5.1 Identificar los controladores para una revisión exitosa. (Esto debería existir en las normas y procedimientos de la función de garantía.)	
1.5.2 Comunicar éxito atribuye al propietario del proceso o de los interesados, y obtener un acuerdo.	
1.6 Definir los recursos requeridos para la auditoría Los recursos necesarios se definen en la introducción de este programa de auditoría / garantía de BCM.	
1.6.1 Determinar las habilidades de auditoría necesarios para la revisión.	
1.6.2 Considerar cómo el proceso / garantía de auditoría integrará recursos de auditoría interna basada en experiencia en el tema.	
1.6.3 Estimación de los recursos totales de auditoría (horas) y el calendario (fechas de inicio y final) que se requieren para la revisión.	
1.7 Definir Entregables La entrega no se limita al informe final. BCM también no se limita a una sola de las partes interesadas. La comunicación entre el equipo de control de auditoría y las diversas partes interesadas es esencial para el éxito de asignación.	
1.7.1Determinar las prestaciones provisionales, incluidas las conclusiones iniciales, informes de estado, los proyectos de informe, fechas de vencimiento de las respuestas o reuniones y el reporte final.	
1.7.2 Determinar quiénes son los representantes principales de cada organización afectada y determinar su participación en el estado y el proceso de elaboración del informe final.	
1.8 Comunicaciones El proceso / garantía de auditoría se debe comunicar claramente a la organización.	
1.8.1 Identificar los destinatarios de los informes de estado y otras comunicaciones.	
1.8.2 Reuniones de estado, calendario y procedimientos de información de estado.	
2. PLAN DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO	
2.1 Organización de Gestión de la Continuidad del Negocio	

Objetivo Auditoría: El equipo del plan de gestión de la continuidad del negocio debe estar organizado para representar a todas las funciones empresariales	
2.1.1 Organización de Gestión de la Continuidad del Negocio Control: El equipo de BCM tiene un líder designado, reportando a un alto ejecutivo de la organización. Composición del equipo de BCM incluye los principales segmentos de las unidades de negocio de la empresa, así como las funciones de apoyo críticas, tales como, recursos legales humanos, relaciones públicas, gestión de la cadena de suministro y logística, fabricación, seguridad de la información, las operaciones de TI, colaboradores internos y auditores	PO4.6 DS4.1
2.1.1.1 Obtener un organigrama que describe las descripciones de puestos BCM, relaciones jerárquicas, nivel de autoridad, personal asignado a cada posición y determinar si todo el personal está activo en la empresa.	
2.1.1.2 Obtener los documentos relacionados con los procesos y procedimientos a seguir por el grupo BCM en caso de una contingencia, la composición del grupo, la frecuencia de las reuniones, y los requisitos de comunicaciones.	
2.1.1.3 Determinar si las siguientes funciones se representan en el equipo de BCM : • Gestión de equipos • Finanzas • Recursos Humanos • Instalaciones • Legal • Relaciones Públicas • Tecnología • Operaciones • Gestión de la cadena de suministro y logística • Comunicaciones •Terceros críticos, por ejemplo, contratistas, proveedores de tecnología • Auditoría interna y externa	
2.1.1.4 Determinar si los representantes participan regularmente o son consultados sobre cuestiones estratégicas y operacionales que afectan a la continuidad del negocio.	
2.1.1.4.1 Obtener actas de las reuniones, organigramas y otra documentación como prueba de la participación.	
2.1.1.4.2 Determinar si los informes del equipo llegan a un nivel superior adecuado de la organización.	
2.1.1.4.3 Identificar la forma y el procedimiento para la relación de subordinación.	
3. POLÍTICAS, NORMAS Y PROCEDIMIENTOS (BCM)	
3.1 Política y Estándares	

Objetivo Auditoría: Las políticas que afectan la continuidad del negocio se implementan para garantizar la integridad y cobertura adecuada de los riesgos de negocio.	
3.1.1 Definición de la política Control: Determinar si la función BCM participa activamente en el establecimiento de la política de continuidad de negocio.	PO6.3 DS4.1 DS4.2
3.1.1.1 Obtener las políticas y normas de la empresa.	
3.1.1.1.1 Determinar si BCM se basa en los estándares o marcos reconocidos, por ejemplo, BS 25999 Guía para la preparación y gestión de incidentes de Continuidad Operacional o la Guía de Planificación de Contingencia SP800-34 NIST para Sistemas de Información.	
3.1.1.1.2 Obtener actas de las reuniones de BCM para verificar la participación, y la familiaridad con las políticas y normas de la empresa.	
3.1.1.1.3 Determinar si la documentación BCM refleja los informes correspondientes, cuadros de mando, etc., para asegurar la gobernabilidad BCM por políticas corporativas.	
3.1.1.1.4 Determinar si el equipo de BCM está involucrado en el desarrollo de políticas y normas.	
3.1.1.1.5 Procedimientos de revisión y aprobación de la política para la inclusión de BCM en el proceso.	
3.2 Procedimientos de Auditoría BCM / Aseguramiento Objetivo: Los procedimientos de BCM se definen, aplican y controlan.	
3.2.1 Procedimientos Control: Los procedimientos de BCM incluye una carta o alcance y objetivos.	
3.2.1.1 Obtener la carta BCM o el alcance y objetivos.	
3.2.2 Políticas de Personal Control: Las políticas de personal se establecen e incluyen la evaluación de habilidades y programas de capacitación para la función de BCM	PO7 DS4.3 DS7
3.2.2.1 Determinar si los recursos asignados a la función BCM tienen competencias adecuadas para desempeñar sus tareas.	
3.2.2.2 Determinar si los recursos asignados a la función BCM tienen requisitos, horarios de entrenamiento y monitoreo de la capacitación.	
3.2.2.2.1 Obtener registros de la capacitación para los recursos de BCM.	
3.2.2.2.2 Evaluar los registros de capacitación; determinar si abordan la evaluación de las competencias identificadas deficientes.	
3.2.3 Respuesta a Incidentes Control: Las responsabilidades y ejercicios de respuesta a incidentes están claramente definidos se ejecutan de forma rutinaria.	DS4.1 DS8.3 DS8.4 DS10
3.2.3.1 Obtención de las políticas y procedimientos de respuesta a incidentes.	
3.2.3.2 Determinar si las responsabilidades de incidentes están claramente identificados.	
3.2.3.3 Determinar si los simulacros de incidentes son programados regularmente.	

3.2.3.4 Determinar si las políticas y los procedimientos están al día y se revisan con regularidad	
3.2.4 Procedimiento Monitoreo BCM. Control: Procesos de BCM son monitoreados rutinariamente, y los resultados son comunicados y evaluados por una gestión responsable.	ME1 ME2 ME4
3.2.4.1 Determinar si se supervisan las políticas y procedimientos de BCM.	
3.2.4.2 Determinar si el proceso de presentación de informes de monitoreo incluye el uso de cuadros de mando y autoevaluaciones.	
3.2.4.2.1 Obtener y tarjetas de puntuación de revisión. Determinar si los procedimientos de expedición de vigilancia están en vigor para asegurar la resolución de las cuestiones identificadas.	
3.2.4.3 Determinar con qué frecuencia se generan informes y la idoneidad de la persona (s) que recibe los informes.	
3.3 Mantenimiento BCM. Objetivo Auditoría: Las políticas y procedimientos de BCM están sujetos a revisión de rutina para asegurarse de que abordan cuestiones de continuidad de negocio actuales.	
3.3.1 Mantenimiento BCM. Control: Las revisiones periódicas de las políticas y procedimientos de BCM son programadas regularmente, realizadas y los resultados evaluados.	PO8 AI4 DS4.4
3.3.1.1 Obtener una lista de toda la documentación BCM.	
3.3.1.2 Determinar si la documentación BCM se ha actualizado con regularidad y los cambios o fechas efectivas en cada página de la documentación.	
3.3.1.3 Determinar si los colaboradores documentan la finalización del proceso de examen con su firma.	
3.3.1.4 Determinar si el personal de revisión de los documentos están calificados.	
3.3.1.5 Determinar si un alto ejecutivo ha aprobado formalmente todos los cambios materiales recientes a los procedimientos, políticas y la documentación del BCM.	
3.3.1.6 Determinar si están disponibles en forma adecuada independiente de la infraestructura interna, por ejemplo, en papel o de forma electrónica y mantenidos fuera de las instalaciones o en una versión basada en la nube en línea las políticas, procedimientos y documentación del BCM.	
3.3.1.7 Determinar si la continuidad empresarial clave, línea de negocio y personal de apoyo tengan el acceso de la documentación.	
4.EVALUACIÓN DE IMPACTODE NEGOCIO(BIA)	
4.1 Definir necesidades de continuidad de negocios BIA Auditoría / Aseguradora. Objetivo: Un análisis exhaustivo del impacto empresarial es la base para las decisiones de continuidad del negocio.	
4.1.1 Metodología definida del BIA. Control: Una metodología del BIA se define y ejecuta.	DS4.1 DS4.2

4.1.1.1 Obtener la metodología BIA	
4.1.1.2 Revisar los procesos para implementar modificaciones para reflejar los cambios en el ambiente de negocios y de procesamiento e incidente de historia.	
4.1.1.3 Determinar que la organización ha determinado el RTO (tiempo de recuperación objetivo y RPO (punto de recuperación objetivo) para cada aplicación crítica.	
4.1.1.4 Evaluar que el RTO y RPO son prácticos y razonables para cada aplicación y línea de negocio o función	
4.1.2 Soportes del BIA. Control: Justificar BIA.	DS4.1 DS4.2
4.1.2.1 Obtener informes de gestión, actas de reuniones, correos electrónicos, etc., que documentan formalmente comunicaciones BIA e informes de estado.	
4.1.3 Evaluar continuamente las necesidades de continuidad de negocios Control: El BIA se actualiza, por lo menos anualmente, por las unidades de negocio y de apoyo.	DS4.4
4.1.3.1 Obtener informes de gestión, actas de reuniones, etc., que los documentos, actualizaciones periódicas a la BIA.	
4.1.3.1.1 Revisar los informes de gestión para asegurar que todas las unidades de negocio y soporte realizan la evaluación anual.	
4.1.3.1.2 Seleccionar informes anuales específicos de las unidades funcionales de alto riesgo; determinan que se llevaron a cabo las actualizaciones anuales de las unidades seleccionadas según sea necesario e incluyen una nueva evaluación de las necesidades de continuidad del negocio.	
4.1.3.2 Determinar que los directores de las unidades de negocio documentan la realización de una revisión anual (o más frecuente) del BIA.	
4.1.3.3 Determinar si el sesgo se lleva a cabo, en respuesta al cambio de procesos de negocio significativo y cuando las unidades de negocio son adquiridos o vendidos.	
4.1.4 Puntos únicos de fallo control: El BIA incluye un análisis detallado de todos los puntos únicos de fallo en las funciones de negocio y de apoyo.	DS4.3 DS4.4
4.1.4.1 Obtener análisis de puntos únicos de falla dentro de las unidades de negocio y soporte, por ejemplo, la cadena de suministro, la cadena logística, información financiera, tecnología (todos los niveles de la tecnología de apoyo a una función de negocio de hardware a través de las redes a las capas de aplicaciones, bases de datos, web interfaces, etc.)	
4.1.4.2 Determinar que todos los puntos únicos de falla han sido o plenamente remediados o la empresa ha aceptado formalmente los riesgos o los riesgos han sido despedidos (por lo general mediante la compra de cobertura de seguro adecuada.)	

5. Evaluación del riesgo	
5.1 Integración con la empresa. Gestión de Riesgos (ERM) Objetivo Auditoría: El BCM es un componente integral del programa de ERM.	
5.1.1 Gestión Riesgo. Control: La gerencia debe participar en un programa de gestión activa del riesgo.	PO9
5.1.1.1 Determinar que el equipo de BCM (u otro equipo apropiado) realiza evaluaciones del riesgo anual o más frecuente, con base en las condiciones de negocio actuales.	
5.1.1.2 Determinar si las evaluaciones de riesgo incluyen la cadena de suministro y logística, problemas de la cadena, así como las relaciones de terceros de misión crítica.	
5.1.1.3 Determinar si están siendo monitoreados los peligros identificados.	
5.1.1.4 Determinar que el equipo de BCM prepara un perfil de riesgo residual, identificar riesgos significativos, y revisar los documentos para determinar la gestión de seguimiento.	
5.1.1.5 Obtener actas de las reuniones de gestión y demás documentación para determinarla participación de la función de BCM.	
5.1.1.6 Determinar que la función BCM participa en la función de gestión de riesgos.	
5.1.2 Gestión de Riesgos Corporativos (ERM). Control: la gestión de continuidad del negocio es un proceso dentro del ERM	PO9
5.1.2.1 Si las evaluaciones de riesgos utilizan el proceso de gestión del riesgo empresarial, lleve a cabo lo siguiente:	
5.1.2.1.1 Obtener e inspeccionar los documentos de evaluación de riesgos.	
5.1.2.1.2 Determinar que la evaluación de riesgos asigna probabilidades razonables a los incidentes que afectan la continuidad del negocio.	
5.1.2.1.3 Revisar la evaluación de riesgos para determinar si la evaluación del riesgo se lleva a cabo de manera imparcial y con el apoyo de hecho o justificación gestión razonable.	
5.1.2.1.4 Determinar que el proceso de gestión de riesgos asigna calificaciones de riesgo residual	
5.1.2.1.5 Determinar cómo las calificaciones de riesgo residual de los procesos están incluidos en los planes de continuidad de negocio.	
5.1.2.1.6 Determinar si las calificaciones del ERM riesgo residual están en alineación con la evaluación anual del riesgo de Auditoría Interna, se determinarán las diferencias materiales y obtener explicaciones	
5.1.2.1.7 Determinar si las unidades de negocio clave y las unidades de apoyo están incluidas en el ERM.	
5.1.2.2 Si un sistema MTC no ha sido establecido, realice lo siguiente.	
5.1.2.2.1 Determinar si las unidades de negocio críticos y unidades de apoyo necesarias para su inclusión en una evaluación del riesgo (es decir, las unidades dependientes de riesgo) se han considerado.	

5.1.2.2.2 Determinar si estas unidades de riesgo dependientes realizan sus propias evaluaciones de riesgo.	
5.1.2.2.3 Determinar los procesos utilizados para las evaluaciones de riesgos independientes	
5.1.2.2.4 Determinar si las calificaciones de riesgo residual de la unidad individual están en alineación con la evaluación anual del riesgo de auditoría interna, identificar las diferencias materiales y obtener explicaciones	
5.1.3 Riesgo de Monitoreo de Emisión de Gestión Control: los riesgos identificados se introducen en un sistema de monitoreo para su inclusión en un plan de continuidad del negocio.	PO9
5.1.3.1 Revisión del proceso para la inclusión de los riesgos en un sistema de monitoreo para su inclusión en el programa de gestión de la continuidad del negocio.	
5.1.3.2 Obtenga el más reciente informe de seguimiento al problema.	
5.1.3.2.1 Determinar si los problemas identificados se han abordado adecuadamente por BCM.	
5.1.3.2.2 Evaluar partidas abiertas y evaluar la calificación de Riesgo Asociado a cada elemento. Determinar si las Calificaciones son las adecuadas.	
5.1.3.2.3 Determinar la frecuencia del monitoreo, tema de seguimiento y evaluar su idoneidad.	
6.DOCUMENTACIÓN	
6.1 Documentación apropiada Objetivo Auditoría: El plan de continuidad del negocio está debidamente documentado para llevar a cabo actividades comerciales eficaces y procedimientos de recuperación provisional después de una interrupción de la actividad declarada.	
6.1.1 La documentación es adecuada para apoyarla Continuidad del Negocio Control: El plan de toda la continuidad del negocio está documentado y disponible durante una emergencia declarada.	PO8 AI4 DS4.4 DS4.7
6.1.1.1 Obtener documentación plan de continuidad del negocio.	
6.1.1.2 Determinar que el plan se ha mantenido vigente y refleja los cambios en los procesos de negocio, el medio ambiente, la tecnología, las relaciones con terceros, contratos y requisitos regulatorios y otros de cumplimiento.	
6.2 La documentación es adecuada para apoyar la recuperación	
6.2.1 Documentación del Plan de Recuperación Control: El plan de recuperación de toda empresa está documentado y disponible durante una emergencia declarada.	DS4.4 DS4.7
6.2.1.1 Determinar si el plan de recuperación está en su lugar.	
6.2.1.2 Obtener documentación del plan de recuperación.	
6.2.1.3 Determinar que el plan se ha mantenido vigente y refleja los cambios relevantes en los procesos de negocio, medio ambiente,	

relaciones con terceros, contratos y requisitos regulatorios y otros de cumplimiento.	
6.2.1.4 Determinar si la información de contacto se ha mantenido al día.	
6.2.1.5 Determinar si está disponible en forma adecuada independiente de la infraestructura interna.	
6.2.1.6 Determinar si el personal clave de recuperación tienen acceso a la documentación.	
7.PLAN PRUEBAS	
7.1 Pruebas del Plan Objetivo Auditoría: El plan debe ser probado con regularidad, y las pruebas debería incluir una verificación integral de los procesos de continuidad y ejercicios situacionales para poner a prueba los supuestos y procedimientos alternativos dentro del plan.	DS4.5 DS4.6
7.1.1 Políticas de pruebas de Control: Políticas de pruebas definen la frecuencia de prueba, tipos de pruebas, el uso de ejercicios situacionales y otros procesos reconocidos.	
7.1.1.1 Obtener documento políticas de pruebas.	
7.1.1.2 Determinar que las siguientes políticas se expresan y documentan: La frecuencia mínima de prueba Las condiciones que requieren pruebas más frecuentes Tipos de escenarios a ensayar	
7.1.2 Métodos de ensayo Control: Las pruebas incluyen dos tutoriales y ejercicios a gran escala de los planes de procesos y recuperación provisionales.	
7.1.2.1 Determinar que los ensayos de recorrido se realizan regularmente e incluyen todas las facetas del plan.	
7.1.2.2 Determinar que a gran escala las pruebas se realizan regularmente e incluyen mayores eventos y riesgos.	
7.1.2.3 Determinar si existe una lista de llamadas después de horas y es actual.	
7.1.2.4 Determinar si existe un programa de concientización de continuidad y se ejecuta con regularidad.	
7.1.3 Análisis de los Resultados de la Prueba Control: Los resultados de las pruebas del plan se analizan para determinar las cuestiones que requieren revisión del BCP, formación adicional o recursos adicionales.	DS4.10
7.1.3.1 Verificar que los cambios en los planes de recuperación se han logrado como resultado de las pruebas y las lecciones aprendidas.	
7.1.3.2 Determinar si los resultados han sido comunicados a la dirección.	
7.1.3.3 Determinar los interesados y las funciones de control para garantizar y recibir análisis post-test.	
7.1.4 Gestión de Pruebas de Control: Pruebas de BCM se documentan y proporcionan la estructura para identificar fallas.	DS4 DS5 DS9
7.1.4.1 Obtener la documentación del ejercicio realizado.	

7.1.4.2 Determinar si los ejercicios habían sido eficaces en la identificación de posibles deficiencias en el BCM.	
7.2 Prueba de Niveles de Servicio de Recuperación. Control: Las pruebas del Plan incluye la verificación de que las pruebas se completan dentro de los intervalos establecidos en la BIA y BCP.	DS4.5 DS4.8
7.2. Determinar si los resultados se comparan con los criterios de prueba (RTO, RPO, etc.).	
7.3 Frecuencia de prueba. Control: El plan de continuidad se prueba de forma rutinaria, de acuerdo con la política. Las pruebas abordan los requisitos dentro del BCP y se documentan.	DS4.6 DS4.8
7.3.1 Verificar que los planes de recuperación se prueban periódicamente.	
7.3.2 Revisar los criterios de prueba para determinar si va aprobar adecuadamente el plan con los requisitos señalados en el BIA.	
7.4 Pruebas de Estrés. Control: Las pruebas de continuidad de negocio utilizan ejercicios situacionales donde los recursos previstos no están disponibles para la prueba, o las circunstancias de la prueba son modificados sin previo aviso para verificarla capacidad del equipo de recuperación de adaptarse a situaciones imprevistas.	DS4.5
7.4.1 Verifique que las pruebas incluyen situaciones sin previo aviso para realizar pruebas de esfuerzo premisas del plan de recuperación y capacidad del personal para reaccionar ante acontecimientos imprevistos.	