Universidad Central

Escuela de Informática

Implementación de un procedimiento de Continuidad de TI alineado con el Marco de Gestión de TI existente para el Departamento de Tecnologías de Información de COOPECAJA R.L.

Trabajo final de graduación para optar por el grado académico de licenciatura en Gerencia Informática

Axel Solano Navarro

San José, Costa Rica

Mayo, 2019

Resumen ejecutivo

El siguiente trabajo se realizó en conjunto con colaboradores de COOPECAJA y el autor de la presente tesis, con el fin de buscar la configuración para implementar un procedimiento para la continuidad de TI, que mejor se adapte a la organización.

Se identificó una serie de debilidades que tiene la cooperativa en temas de continuidad de TI, los cuales hacen necesaria la implementación de un procedimiento de continuidad que esté alineado al marco de gestión de tecnologías de información y cumpla con los requisitos de negocio.

Para esto fue necesario conocer de la organización, la cultura así como valores, objetivos, misión, visión y estructura organizacional, son datos relevantes para diseñar un procedimiento que sea aceptado por todos los niveles jerárquicos requeridos y, además, lo más fácilmente adoptado por todos los involucrados.

Es de gran importancia conocer los conceptos de los términos utilizados en toda la tesis, para ello se redactaron de forma sencilla para que el presente documento sea más comprensible por profesionales de otras áreas o bien, personas ajenas al conocimiento informático. Al final, cualquier persona será capaz de comprender los conceptos informáticos con los cuales se está desarrollando el sistema que tiene como fin este documento.

En el marco metodológico se indican las pautas a seguir para el desarrollo de la investigación, es ahí donde se establece la manera en cómo se debe recolectar y analizar toda la información requerida. Todo esto con el fin de encontrar la posible solución al problema encontrado, desde un punto de vista teórico práctico, para mostrar tanto la documentación que respalda la investigación como comprobarla en el trabajo de campo.

Una vez finalizada la investigación y aplicadas las herramientas descritas durante esta, se puede observar el estado anterior del procedimiento y, asimismo, compararlo con el propuesto y las distintas configuraciones para llegar a él. Parte de los resultados obtenidos es el análisis de brechas realizado contra un marco de

referencia aceptado como es COBIT 5, con el cual se puede no solo mejorar lo que existe actualmente, sino se puede entrar en un proceso de mejora continua para que el procedimiento se mantenga funcional en el tiempo.

Una vez concluido el trabajo, basado en el conocimiento de la empresa y con los resultados de la investigación, se puede recomendar a COOPECAJA la configuración que más le conviene para la implementación de un procedimiento de continuidad de TI alineado con el Marco de Gestión de TI existente para el Departamento de Tecnologías de Información.

Dedicatoria

A mis hijos Luis Antonio y Juan Manuel, quienes me han inspirado a ser ejemplo de superación, sin importar la edad se debe seguir estudiando, creo en ellos, sé que lograrán grandes cosas.

A Floribeth Fernández, más que una madre en todo el proceso de estudio, apoyo incondicional, consejera y amiga.

A Ingrid Nájera, por motivarme a seguir adelante y creer en mí, espero que de la misma manera que motiva a los demás, consiga todo lo que se propone.

Agradecimiento

A Dios, que me permitió llevar a cabo el trabajo, me dio salud, tiempo y recursos para hacerlo, además puso personas en mi camino que me ayudaron en el proceso.

A Ingrid Nájera, amiga, compañera, colega, persona a quien admiro y fue quien hizo que tomara la decisión de seguir adelante con esta etapa que debía concluir.

Contenido

Capítulo I

1. Introducción

Las cooperativas de crédito y ahorro son organizaciones que pertenecen al sector financiero costarricense y han tenido gran auge en los últimos años. Su volumen transaccional las hace parecer bancos a menor escala, lo cual les exige contar con una serie de regulaciones y estándares para operar de forma legítima, salvaguardando los intereses de sus asociados y el país.

Para garantizar la transparencia y la seguridad de los clientes, las cooperativas, al igual que los bancos y otras entidades financieras, las supervisa la Superintendencia General de Entidades Financieras (SUGEF). Al ser reguladas por esta superintendencia, deben cumplir con una serie de estipulaciones, caso contrario se exponen a importantes multas y hasta al cierre total de la operación.

La SUGEF dicta un reglamento específico para la gestión de las tecnologías de información de las entidades financieras, este indica la manera adecuada de operar la tecnología y cómo debe reportar a la superintendencia. Es de acatamiento obligatorio y revisado periódicamente.

1.1. El problema y su importancia

El departamento de TI de Coopecaja no cuenta con un procedimiento de continuidad de TI, el cual se encuentre alineado al marco de gestión TI, con el fin de garantizar la continuidad de negocio y cumplir con la normativa según lo establecido por SUGEF.

La implementación de un procedimiento de continuidad de TI que contemple lo indicado en el proceso DSS04 de Cobit 5 (gestionar la continuidad), garantizaría a Coopecaja contar con un adecuado plan de continuidad de TI, el cual permita gestionar de forma oportuna la operación de TI ante un evento que comprometa la estabilidad de la organización y el cumplimiento regulatorio que es fundamental para las empresas que pertenecen al sector financiero.

Por otro lado, cabe destacar que la Superintendencia General de Entidades Financieras (SUGEF) regula el sector financiero del país, este órgano vela por la estabilidad, solidez y eficiente funcionamiento del sistema financiero nacional, dicta

las normas generales y directrices que estime necesarias para cumplir con su propósito.

Dentro de las normativas de la SUGEF se encuentra la 14-17 “Reglamento general de gestión de la tecnología de información”, en este se establece los requerimientos mínimos para la gestión de la tecnología de información que deben acatar las entidades supervisadas y reguladas del sistema financiero costarricense, reglamento que Coopecaja debe cumplir.

El artículo 8 del reglamento indica que las entidades supervisadas son responsables de planificar, implementar, controlar y mantener un marco de gestión de TI, de acuerdo con los procesos descritos en los Lineamientos Generales y considerando los riesgos de TI establecidos en la gestión integral de riesgos aprobada por el Órgano de Dirección de cada una de las entidades; este marco está basado en COBIT 5.

Uno de los procesos con los cuales se debe cumplir, según lo indicado en la regulación, es el de continuidad de TI. La auditoría interna de Coopecaja realiza un estudio para determinar el estado actual de la organización en este tema y detecta una serie de debilidades que deben ser atendidas de forma inmediata y solventarse en su totalidad.

Los hallazgos de auditoría indican que hace falta un procedimiento de continuidad, los pasos a seguir para ello son: la actualización de planes de continuidad de TI y planes de recuperación de infraestructura tecnológica, parámetros para activar los planes, procedimiento para distribución de planes, entre otros.

El no contar con todo lo requerido para un adecuado esquema de continuidad tiene repercusiones a nivel regulatorio, compromete la estabilidad de la empresa, genera insatisfacción y desconfianza a los clientes, afecta de forma significativa la imagen de la institución, en casos extremos puede provocar el cierre total de la empresa.

1.2. Planteamiento del problema

Uno de los aspectos más importantes a considerar en la administración de riesgos en una empresa es el plan de continuidad de negocios, esto ayuda a las organizaciones modernas a sobrevivir en un ambiente que se encuentre lleno de amenazas de muchos tipos.

Muchas empresas han cerrado por no tener capacidad de continuidad y recuperación ante eventos de gran impacto, es por este motivo que se han desarrollado mejores prácticas y estándares para garantizar la continuidad del negocio.

Una empresa que depende de las tecnologías de información para su funcionamiento y no cuente con un procedimiento para continuidad de TI, no puede garantizarla ante un evento de gran impacto. No contar con el presupuesto y los mecanismos requeridos de recuperación, son factores que pueden provocar el cierre total de una organización ante una eventualidad, además son motivos para estar en incumplimiento con el regulador.

¿Qué puede ocurrir si un evento de gran impacto afecta a Coopecaja y no cuenta con los procesos para garantizar la continuidad y la recuperación de sus operaciones?

1.3. Antecedentes

En este apartado se presenta la relación existente entre el actual trabajo de investigación y otros anteriores que estudien un tema similar.

Según las revisiones se encuentra el trabajo del ingeniero Freddy Bustos Zúñiga (TINF1630) que tiene gran similitud; pues también lo realizó para Coopecaja, y, de igual manera que el presente, por un tema regulatorio de una de las normativas de SUGEF.

Título de Tesis			
Propuesta de definición de los Acuerdos de Nivel de Servicio (SLA's) para el Departamento de Tecnologías de Información de COOPECAJA R.L.			
	Aspecto comparado	Tesis (TINF1630)	Trabajo Actual
Semejanzas	**Empresa**	Coopecaja	Coopecaja
	Necesidad	Responde a una regulación de SUGEF	Responde a una regulación de SUGEF
Diferencias	**Normativa**	SUGEF 14-09	SUGEF 14-17
	Marco de referencia	Cobit 4.1	Cobit 5
	Proceso Cobit	DS1 Definir y administrar niveles de servicio.	DSS04 Gestionar la Continuidad
	Estándar o mejor práctica	ITIL V3	ISO 22301

Tabla 1. Comparativo con tesis TINF 1630

Fuente: elaboración propia

1.4. Objetivos

General

Implementar procedimiento para elaborar el plan de continuidad de TI, el cual permita garantizar la continuidad de negocio del área de plataforma de servicios para Coopecaja.

Específicos

1. Comparar mediante un flujograma el procedimiento actual de continuidad de TI con uno sugerido, basándose en riesgos y tomando como referencia COBIT 5 y COBIT 5 para riesgos.
2. Analizar mediante un estudio de factibilidad las distintas configuraciones para la implementación del procedimiento de continuidad.
3. Determinar la configuración ideal para un procedimiento de continuidad de TI para Coopecaja.

4. Elaborar diseño de procedimiento de continuidad para Coopecaja.
5. Implementar procedimiento de continuidad de TI para el área de plataforma de servicios.

1.5. Los alcances de la investigación

El alcance de esta investigación es mostrar distintas configuraciones para un procedimiento de continuidad de TI, así como presentar un estudio de factibilidad y con esto seleccionar la mejor opción para implementar el procedimiento de continuidad de TI que requiere la organización, el cual esté alineado con el marco de gestión de TI existente, para los servicios declarados como críticos de Coopecaja y la infraestructura tecnológica que soporte esos servicios (colocación y recaudación).

1.6. Las limitaciones de la investigación

La entidad resguarda la información sensible; por tanto, hay datos como salarios y costo por hora de utilidad de servicios que no pueden ser proporcionados.

Capítulo II

Marco teórico

En el presente capítulo se darán a conocer conceptos de otros autores redactados de forma sencilla, para que el documento sea más comprensible por profesionales de otras áreas, así como para personas ajenas al conocimiento tecnológico.

También se explican conceptos vinculados a la organización a la que se presenta la investigación (Coopecaja) y de las áreas involucradas en el procedimiento.

Al final del capítulo, se espera que cualquier persona sea capaz de comprender los conceptos tecnológicos utilizados para el desarrollo de un procedimiento para gestionar un proceso de un departamento de tecnologías de información.

2.1. De la institución

2.1.1. Reseña histórica

COOPECAJA nació como un pequeño proyecto cooperativista para los empleados de la CCSS, hoy es una de las entidades financieras más sólidas del sistema financiero nacional y en la actualidad cuenta con más de 21 500 asociados, quienes han visto mejorar su calidad de vida por medio de esa organización.

Al inicio de la década de los setenta, un grupo de personas pertenecientes a la Unión de Empleados de la Caja (UNDECA), tuvieron la inquietud de encontrar una solución ante las pocas opciones de apoyo económico para los empleados de la Caja Costarricense de Seguro Social (CCSS). Ellos tenían el eslabón principal para iniciar una gran cadena guiada bajo la filosofía cooperativista, considerada como uno de los medios más eficientes para el desarrollo económico, social, cultural y democrático de un país.

Desde el planteamiento del sistema cooperativo hasta su aprobación definitiva, transcurrió poco más de medio año cuando se dio luz verde para el comienzo de la Cooperativa de Afiliados al Sindicato Nacional de Empleados de la Caja

Costarricense de Seguro Social (COOPEUNDECA), eso sí, como una sección aparte del sindicato.

El día 28 de mayo de 1971, a las 18:00 horas, aquel grupo visionario de la CCSS realizó la primera sesión oficial. En el acta número uno se definió en tinta y papel: *"[…] una cooperativa de ahorro y crédito y servicios múltiples, para llenar las necesidades sentidas por todos y con el ánimo de mejorar las condiciones económicas y sociales […]".*

En ese sentido, quienes deseaban pertenecer a COOPEUNDECA lo efectuaban por medio de una cuota fija de dos colones, correspondiente al monto de admisión y con esta obtenían derecho a créditos en artículos de consumo.

En su primer año, COOPEUNDECA realizó la venta de juguetes para la época navideña en el sótano del Hospital México. El proyecto fue todo un éxito y muchos trabajadores de la CCSS llevaron la alegría y la esperanza a sus hogares esa Noche Buena.

En 1978, la cooperativa cambió de nombre para convertirse en COOPECAJA R.L., dado que algunos aún no comprendían la dinámica del nuevo modelo integrado por el sindicalismo y el cooperativismo. Mientras tanto, en el país concluía el traspaso del sistema hospitalario de la Junta de Protección Social (JPS) a la Caja Costarricense de Seguro Social. De este modo, COOPECAJA era la primera cooperativa para los empleados de la CCSS. Con el paso del tiempo, la cooperativa reforzó su ideología y redefinió su rumbo.

Para 1980, dejó a un lado la actividad de consumo. Una decisión tomada a conciencia; pues la inexperiencia en la parte comercial evitó el cumplimiento de las expectativas planteadas desde un principio. Una vez aplicados los cambios, la cooperativa demostró su fortaleza y constancia al recuperar su estabilidad, manteniéndose en el mercado, con lo cual los asociados reafirmaron su confianza en la entidad.

En 1986 las oficinas se trasladan hacia un punto estratégico en la capital, ubicándolas en las cercanías del edificio de la CCSS, donde se encuentran en la actualidad.

La prioridad para COOPECAJA ha sido ofrecer los servicios de ahorro y crédito considerando el bolsillo de los asociados para contribuir con su desarrollo socioeconómico. Los servicios financieros de la cooperativa representan una solución oportuna para las necesidades de sus miembros, mediante la implementación de líneas de crédito acordes a las necesidades de los asociados; así como campañas educativas para promover los beneficios del ahorro.

En su camino, la cooperativa ha esquivado los obstáculos transformando las posibles amenazas en fortalezas, para llegar a ser de las mejores. La constancia y la lealtad, aunadas al trabajo en equipo de sus asociados y personal, la han convertido en una entidad cada día más fuerte.

Para 1986 se presentó una crisis significativa dentro del sistema cooperativo de ahorro y crédito costarricense. Las organizaciones consideradas en ese momento como las más representativas, se vieron en un gran riesgo financiero, un golpe muy fuerte para algunas que nunca se recuperaron y desaparecieron. Sin embargo, para finales de los ochenta, la cooperativa incrementó sus recursos de manera paulatina, pero segura y en menos de diez años duplicó sus activos.

A principios de los 90, la cooperativa decide retomar su asociación a la entonces renovada Fedecrédito, de quien se había separado años atrás; pues contaba con indicadores de confianza para generar el vínculo. Sin embargo, la federación amplió sus servicios, los cuales al cabo de los años no pudieron controlar, obligándola a su cierre definitivo en 1999. Este evento requirió soluciones inmediatas para no poner en riesgo la rentabilidad y la estabilidad obtenida por la cooperativa, así como la confianza depositada por los asociados.

La actitud del personal administrativo permitió que se saliera de forma positiva de esa difícil situación. En general, los dirigentes reconocen que los momentos críticos les han hecho madurar; por eso, toman decisiones de tipo conservador y

apoyan aspectos como el profesionalismo del personal para ofrecer una mejor atención al asociado. A finales de la década de los 90, se les abrieron las puertas para integrarse a esta gran familia cooperativista a los empleados del Ministerio de Salud, Acueductos y Alcantarillados y el Instituto sobre Alcoholismo Farmacodependencia.

La respuesta obtenida en los años anteriores puso sobre la mesa el tema de la apertura al sector público. Un proyecto analizado minuciosamente, pues ha sido una premisa para COOPECAJA el crecimiento controlado, para no poner en riesgo los intereses de la colectividad.

En mayo de 2005, la asamblea acuerda la apertura al sector público y pasó a ser la cooperativa de los trabajadores del sector público costarricense.

En el 2009 la cooperativa se afilia a FECOOPSE, con el fin de integrarse a una federación que vela por los intereses de sus afiliados, así como aprovechar las oportunidades de negocio existentes entre las cooperativas y su entorno.

En los últimos años, la cooperativa ha destinado presupuesto a grandes proyectos como la apertura de sucursales en Heredia, Desamparados, Puntarenas y Liberia, el proyecto de unidad móvil, la próxima construcción del nuevo edificio de oficinas centrales, la modernización de los equipos de cómputo, una central telefónica de vanguardia y un sistema de gestión de filas que facilita una mejor atención de los asociados en las oficinas. Además, muy pronto verá la luz el nuevo Core bancario NEO, un nuevo sistema de información para un manejo más seguro y eficiente de las gestiones, así como la integración al sistema SINPE del Banco Central y muchas otras iniciativas que ya se encuentran en desarrollo.

La atención personalizada, el calor humano, la constancia y la innovación aplicadas en equipo conllevan al éxito en una entidad. Por eso, quienes forman parte de COOPECAJA no temen al futuro, lo esperan con positivismo; pues la cooperativa hoy ocupa un lugar preponderante en el sistema financiero nacional.

2.1.2. Nombre de la institución

Coopecaja

2.1.3. Ubicación geográfica

San José, avenida 8, calles 5 y 7.

2.1.4. Antecedente y hechos relevantes

2.1.5. Misión

"Brindamos servicios cooperativos con soluciones financieras, sociales y solidarias que satisfacen las necesidades de las personas asociadas y clientes".

2.1.6. Visión

"Ser la mejor cooperativa, reconocida por su solidaridad, calidez, prestigio, solidez financiera y compromiso con el desarrollo integral de las personas asociadas, sus familias y clientes".

2.1.7. Valores

- Calidez: centrar la calidad del servicio en la amabilidad, respeto, empatía y cercanía, considerando el bienestar de las personas asociadas y la Cooperativa en general.
- Honestidad: probidad, buena fe en la toma de decisiones y transparencia en nuestras actuaciones.
- Trabajo en equipo: visión de trabajo integral; fortaleciendo el desempeño basado en el cumplimiento de objetivos, aplicando esfuerzos grupales.
- Compromiso: la convicción que tendremos todos por cumplir nuestra Visión y Misión.

2.1.8. Objetivo

COOPECAJA busca posicionarse como una cooperativa líder en el sector financiero nacional, emprendiendo ambiciosos proyectos con la finalidad de estar siempre a la vanguardia en tecnología, infraestructura y servicio, para ofrecer a sus asociados verdaderas soluciones financiares, de una forma ágil, segura y oportuna. (Bustos, 2016)

2.2. SUGEF

2.2.1. Antecedentes

La Superintendencia General de Entidades Financieras (SUGEF) por muchos años funcionó como un departamento del Banco Central de Costa Rica, denominado "Auditoría General de Bancos" (AGB). El Artículo 44 de la Ley 1552, publicada el 23 de abril de 1952, establecía como función de la AGB ejercer *"[...] la vigilancia y fiscalización permanente de todos los departamentos y dependencias del Banco, de las demás instituciones bancarias del país, incluyendo sucursales y otras dependencias, y cualesquiera otras entidades que las leyes sometan a su control [...]".*

Posteriormente, el 4 de noviembre de 1988 y con la promulgación de la Ley de Modernización del Sistema Financiero de la República, número 7107, la cual modificó la Ley 1552, la AGB se transformó en la Auditoría General de Entidades Financieras (AGEF), *"[…] como un órgano de desconcentración máxima adscrito al Banco Central [...]"* (Artículo 124 de la Ley 1552).

La figura jurídica de desconcentración máxima se define en el Artículo 83 de la Ley General de Administración Pública, número 6227 del 20 de diciembre de 1978, el cual establece que *"[…] Todo órgano distinto del jerarca estará plenamente subordinado a éste y al superior jerárquico inmediato, salvo desconcentración operada por ley [...]".* Se entiende la desconcentración como la imposibilidad del superior de avocar competencias del inferior y revisar su conducta. En lo que al grado de desconcentración se refiere, dispone el mismo artículo que será máxima *"[…] cuando el inferior esté sustraído además a órdenes, instrucciones o circulares del superior […]".*

De acuerdo con esta reforma, correspondía a la AGEF fiscalizar el funcionamiento de todos los bancos, incluidos el Banco Central de Costa Rica, las sociedades financieras de carácter no bancario y las demás entidades públicas o privadas, independientemente de su naturaleza

jurídica, que operasen en actividades de intermediación entre la oferta y la demanda de recursos financieros, directa o indirectamente, o en la prestación de otros servicios bancarios.

La nueva Ley Orgánica del Banco Central de Costa Rica (No. 7558), vigente desde el 27 de noviembre de 1995, declara de interés público la fiscalización de las entidades financieras y crea la Superintendencia General de Entidades Financieras (SUGEF), bajo la misma figura jurídica de la desconcentración máxima, pero esta vez dotada de mayores poderes y mayor autonomía administrativa, mediante la institución de su propio Consejo Directivo.

Esta reforma modifica, además, el esquema de regulación represiva *ex post* que venía utilizando la SUGEF, impulsa un novedoso enfoque de supervisión prudencial *ex ante*, el cual pretende garantizar la transparencia, promover el fortalecimiento y fomentar el desarrollo del sistema financiero de la República, y amplía su ámbito de fiscalización, sometiendo bajo su control a todas las entidades que realicen actividades de intermediación financiera dentro del territorio nacional, o hayan sido autorizadas por el Banco Central a participar en el mercado cambiario.

La promulgación de la Ley 7732 Ley Reguladora del Mercado de Valores, vigente a partir del 27 de marzo de 1998, trae cambios al sistema financiero bursátil y con ellos cambios a la Ley 7558.

Las funciones que ejercía el Consejo Directivo de la SUGEF serán realizadas por el Consejo Nacional de Supervisión del Sistema Financiero, el cual es común para las cuatro superintendencias encargadas de la supervisión y fiscalización de intermediarios financieros, mercado de valores, mercado de seguros y fondos de pensión, representadas estas por la Superintendencia General de Entidades Financieras, Superintendencia General de Valores, Superintendencia General de Seguros y Superintendencia General de Pensiones, respectivamente.

2.2.2. Marco estratégico

Misión

"Contribuir con la estabilidad y fortaleza del sistema financiero para preservar la confianza de la sociedad, aplicando las potestades de supervisión y fiscalización asignadas por el ordenamiento jurídico".

Visión

"Ser un supervisor reconocido por su trabajo con excelencia, ética y transparencia, para responder a las necesidades de la sociedad en su ámbito de competencia".

Propuesta de Valor

"Promover la confianza del público en el sistema financiero".

Política de calidad

La SUGEF supervisa y fiscaliza, mediante un enfoque basado en riesgos, a los intermediarios financieros de Costa Rica y a otras personas físicas y jurídicas encomendadas por ley, en lo cual demuestra cumplimiento de los requisitos de su Sistema de Gestión de la Calidad y mejora continua de sus procesos, en línea con su estrategia.

Valores corporativos

Excelencia
Integridad
Compromiso
Transparencia

2.2.3. Objetivos y funciones

Objetivos

Ser un supervisor reconocido por su trabajo con excelencia, ética y transparencia, para responder a las necesidades de la sociedad en su ámbito de competencia.

Contribuir con la estabilidad y fortaleza del sistema financiero para preservar la confianza de la sociedad, aplicando las potestades de supervisión y fiscalización asignadas por el ordenamiento jurídico.

Funciones

-Velar por la estabilidad, la solidez y el funcionamiento eficiente del sistema financiero nacional.
-Fiscalizar las operaciones y actividades de las entidades bajo su control.
-Dictar las normas generales que sean necesarias para el establecimiento de prácticas bancarias sanas.
-Establecer categorías de intermediarios financieros en función del tipo, tamaño y grado de riesgo.
-Fiscalizar las operaciones de los entes autorizados por el Banco Central de Costa Rica a participar en el mercado cambiario.
-Dictar las normas generales y directrices que estime necesarias para promover la estabilidad, solvencia y transparencia de las operaciones de las entidades fiscalizadas.
-Presentar informes de sus actividades de supervisión y fiscalización al Consejo Nacional de Supervisión del Sistema Financiero.

-Cumplir con cualesquiera otras funciones y atributos que le correspondan, de acuerdo con las leyes, reglamentos y demás disposiciones atinentes.

2.3. ACUERDO SUGEF 14-17

2.3.1. Gestión de TI:

La tecnología de la información (TI) resulta indispensable para gobernar, gestionar y tomar decisiones dentro de las organizaciones, asimismo, su adecuada administración permite mantener la competitividad y coadyuva en la consecución de las metas y los objetivos.

A principios de la década anterior, y en virtud de múltiples casos de quiebras y fraudes asociados a temas operativos y de mala gestión, varios organismos internacionales han emitido disposiciones en las cuales resaltan la necesidad de mejorar los sistemas de Gobierno Corporativo y, en consecuencia, la forma de gobernar TI.

Estos requerimientos plantean el reto de diseñar y mantener controles eficientes que faciliten la gestión de TI desde dos puntos de vista: el primero, tomando a TI como un proceso más del negocio, y, segundo, al considerar a TI como encargado de proveer y mantener la plataforma y los sistemas que apoyan la ejecución del resto de los procesos del negocio.

Esta dualidad implica para las entidades el diseño o la adopción de un marco que les permita gobernar, gestionar y controlar la función de TI, desde ambos puntos de vista en forma consistente.

Dado que la gobernanza orienta, dirige y supervisa la gestión de TI y que las tecnologías de información se consideran factores de riesgo operativo, al que están expuestas las entidades, resulta necesario que este reglamento incluya la evaluación de los procesos de gobierno y gestión de TI por parte de las Superintendencias.

2.3.2. Necesidad de control de TI:

Una inadecuada gestión del riesgo operacional en el área de la tecnología de información en las entidades supervisadas puede repercutir

negativamente en la continuidad de sus operaciones y, por consiguiente, impactar sus patrimonios y concomitantemente, afectando a los clientes de las entidades.

Por lo anterior, resulta indispensable que las entidades supervisadas determinen su marco de gestión, para el control de la tecnología de información, lo cual garantice la integridad, seguridad, auditabilidad y disponibilidad de la información y los servicios ofrecidos.

2.3.3. Sobre la implementación del marco de gestión de TI dispuesto en este reglamento:

El diseño e implementación del marco de gestión de TI requiere de esfuerzo planificado y progresivo por parte de las entidades supervisadas. Con el objeto de facilitar este proceso, su inversión y la definición concomitante de políticas, procesos y estructuras, el modelo de supervisión basada en riesgos le coadyuva, por medio de este reglamento, a que la entidad supervisada establezca su marco de gestión de TI en virtud de sus necesidades según su naturaleza, complejidad, modelo de negocio, volumen de operaciones, criticidad de sus procesos, riesgos y su dependencia tecnológica.

Los lineamientos generales que acompañan el reglamento establecen un periodo de implementación a partir de la entrada en vigor (gradualidad) que abarca hasta cinco años para entidades supervisadas por la SUGEVAL, SUPEN y SUGESE; asimismo, de tres años para las entidades supervisadas por la SUGEF, este último plazo en consideración del avance logrado a partir de los requerimientos del Acuerdo SUGEF 14-09 “Reglamento sobre la Gestión de la Tecnología de Información”. Estos plazos se estiman razonables para que las entidades puedan efectuar las adecuaciones necesarias para la implementación efectiva de su marco de gestión de TI.

Por otra parte, de acuerdo con la experiencia de la aplicación del “Reglamento sobre la Gestión de la Tecnología de Información” en SUGEF, se estima prudente mantener el lapso de nueve meses, contados

a partir de la notificación del requerimiento de auditoría externa de TI, para la remisión de los entregables de la auditoría externa de TI del marco de gestión de TI, así como sobre cualquier otro criterio que se considere necesario en virtud del perfil de riesgo de la entidad.

Dicha holgura permite a las entidades desarrollar los aspectos procedimentales necesarios a efecto de la contratación, ejecución y entrega de los resultados de la auditoría externa.

Finalmente, el Consejo ha considerado razonable el plazo de veinte días hábiles para la remisión del plan de acción, cuando haya sido requerido por alguna superintendencia. Dicha conclusión se desprende del hecho de que una entidad va recibiendo retroalimentación conforme evoluciona la auditoría externa, de manera que una vez finalizada ya cuenta con suficientes elementos y datos que le permiten perfilar un conjunto de acciones.

2.3.4. Supervisión basada en riesgos:

La supervisión basada en riesgos se caracteriza por la migración de un modelo basado en reglas hacia un enfoque donde la entidad supervisada es responsable de una gestión integral de los riesgos del negocio. En este enfoque corresponde a la entidad supervisada determinar, dentro de esa gestión de riesgos, el marco de gestión de TI que se adapte a su negocio, de manera que le permita identificar y establecer las medidas de mitigación para los riesgos que surgen de TI; por ello, la regulación se enfoca a un marco de gestión de TI con aquellas características prudenciales suficientes para el supervisor, sin que necesariamente se definan, de manera puntual, determinados estándares o herramientas de control.

En esa misma lógica, el reglamento que se emite encuentra sentido como parte de una estructura normativa transversal al sistema financiero, la cual no sustituye los procesos de supervisión sobre riesgo operacional que ya se desarrollan, sino más bien viene a complementarlos, aportando

información que nutre el criterio del supervisor a partir del aporte de especialistas externos.

2.3.5. Estándares disponibles como marco de referencia: la industria y los profesionales en TI, han venido desde hace varias décadas desarrollando estándares y marcos que permitan gestionar y controlar las tecnologías. Ante la incertidumbre y costo que significa el desarrollo interno de un marco de gestión de TI, las organizaciones han propendido por adoptar alguno de los marcos o estándares disponibles.

Marcos de referencia como Cobit e ITIL y estándares como ISO gozan en la actualidad de aceptación general, desde la visión del supervisor; Cobit es un marco apropiado que se ajusta al negocio y facilita que las organizaciones desarrollen un ambiente de control que responda a las necesidades del negocio; además de estandarizar procesos de TI, limitar desviaciones de los objetivos de negocio y, particularmente, lograr un balance entre los riesgos que introduce la tecnología de información y su aporte de valor al desempeño y rentabilidad. De igual forma, estos marcos permiten el desarrollo del enfoque de supervisión basada en riesgos, por las siguientes razones:

Desde la óptica del negocio:

a. Enfoque en Gobierno de TI: el marco se desarrolla dentro del nuevo enfoque de gobernabilidad de TI como parte del buen gobierno corporativo, procurando mayor involucramiento con los procesos clave, además define una estructura de relaciones y procesos diseñados y ejecutados por la entidad para dirigir y controlar la tecnología, sus riesgos y vinculación con las estrategias y objetivos de negocio.

b. Satisface los requerimientos de negocio: integración más clara entre los objetivos del negocio y la TI, mediante objetivos en el modelo de cascada y métricas que los soportan.

c. Logra la armonización: integración optimizada de otros estándares internacionales.

d. Definiciones y flujos de procesos: optimización en las descripciones de los procesos, actividades, entradas y salidas.

e. Lenguaje y presentación: utiliza un lenguaje accesible para todo tipo de usuario, mismo que permite a ejecutivos no versados en conocimientos tecnológicos identificar y comprender los principales aspectos de TI.

Desde la óptica del supervisor:

f. Permite evaluar la integración de los procesos de TI con los procesos y líneas de negocio y el logro de los objetivos de la entidad.

g. Permite identificar el grado de dependencia de las entidades de la tecnología de información en sus operaciones.

h. Permite identificar los perfiles de riesgo en TI de los supervisados, con el propósito de concentrar esfuerzos en entidades con mayor exposición o con mayores debilidades de control.

i. Es un marco integrador (alineado con otros estándares y buenas prácticas que puede usarse en conjunto con ellas), enfocado al negocio, y diseñado para ser utilizado por una amplia gama de usuarios, pero principalmente, como guía integral para la alta administración para los líderes o responsables de los procesos y líneas de negocio.

2.3.6. Sobre la estrategia del supervisor

La experiencia con los intermediarios financieros en relación con el proceso de implementación del marco de gestión de TI del Acuerdo SUGEF 14-09 “Reglamento sobre la Gestión de la Tecnología de Información”, develó que varios grupos y conglomerados financieros gestionan la tecnología de información de forma corporativa en las empresas que los integran. Conscientes de esta realidad, el CONASSIF ha concebido la necesidad de integrar en un solo cuerpo normativo los requerimientos de control para la gestión de TI para un grupo o conglomerado. Dicha estrategia tiene como objetivo permitir, entre otros aspectos, la estandarización de procesos, la generación de economías de escala y la creación de una cultura proclive a la mejora de la gobernabilidad de la TI.

El reglamento que se emite también reconoce que entre los supervisados se presentan diferencias en el grado de dependencia de las tecnologías de información y, como consecuencia, la materialización de los riesgos a esas tecnologías les impacta de manera diferente.

Esa condición descrita en el párrafo anterior se refleja al implementar el principio de “proporcionalidad” que rige los esquemas de supervisión basada en riesgo. Dicho principio promueve que las prácticas y las demandas de supervisión se definan y apliquen en consonancia con el perfil de riesgo y la importancia sistémica de los supervisados, el enfoque asumido permite que los supervisados agreguen otros estándares o bien, exista una exigencia particular en función de su rol dentro del mercado en que opera. Finalmente, sobre una base de costo beneficio, naturaleza de la entidad y perfil tecnológico; se permite la definición de marcos de gestión de TI diferentes en reconocimiento de estas diferencias.

La pretensión última de esta estrategia es generar, bajo un esquema de supervisión integrada y coordinada, mejoras en el nivel de la gestión de la tecnología de información y sus riesgos asociados, como herramienta para contribuir al proceso de gestión de riesgos y preparación ante los retos que impone un ambiente financiero competitivo e innovador.

2.3.7. Auditoría externa

La auditoría de los sistemas de tecnología de información es una actividad altamente especializada para la cual existen certificaciones con reconocimiento mundial; se considera conveniente, que la revisión del marco de gestión de TI y cualquier otro criterio que las Superintendencias consideren necesario, en virtud del perfil de riesgo de las entidades supervisadas, sea ejecutada por auditores externos, con el fin de contribuir con la eficiencia en el proceso de supervisión. Los resultados de esta auditoría pueden enriquecer la supervisión en torno a los riesgos operacionales y de tecnología de la información que realizan las Superintendencias y se constituye en un elemento adicional dentro de la supervisión basada en riesgos.

2.3.8. Registro de Auditores Elegibles

Actualmente se cuenta con un registro de auditores con requisitos en torno a su capacidad e independencia, dicho registro se concentra en auditores financieros; sin embargo, con el propósito de ir avanzando en la integración en un solo cuerpo reglamentario, el cual regule los requerimientos de los distintos profesionales que convergen en procesos de revisión y auditoría, se amplía el alcance de este registro para que incluya a los auditores externos de tecnologías de la información.

2.3.9. Comité de TI

Dentro de las funciones del Órgano de Dirección, el Reglamento de Gobierno Corporativo señala establecer los comités técnicos que considere pertinentes para la buena gestión de la entidad; por lo tanto, la creación del comité de TI estará en función de las necesidades de las entidades supervisadas según su naturaleza, complejidad, modelo de negocio, volumen de operaciones, criticidad de sus procesos y su dependencia tecnológica.

2.3.10. Coordinación entre superintendencias

Para evitar costos innecesarios a las entidades supervisadas resulta imprescindible coordinar los procesos de supervisión de las diferentes superintendencias, cuando una misma unidad de TI presta servicios a entidades supervisadas por distintos órganos supervisores.

2.3.10.1. El inciso i) del artículo 171 de la Ley Reguladora del Mercado de Valores establece, como una de las funciones del Consejo Nacional de Supervisión del Sistema Financiero, reglamentar el intercambio de información que podrán realizar entre sí las diferentes Superintendencias, para el estricto cumplimiento de sus funciones de supervisión prudencial. La Superintendencia que reciba información en virtud de este inciso, deberá mantener las obligaciones de confidencialidad a que está sujeto el receptor inicial de dicha información.

2.3.11. Definiciones y abreviaturas.

a) Auditor externo de TI: profesional independiente o socio de una firma o despacho responsable de la auditoría externa de TI.

b) Auditoría externa de TI: servicio de auditoría directa que implica un compromiso de reporte directo según el estándar definido por ISACA.

c) Cliente: persona relacionada a las entidades supervisadas denominadas: ahorrantes, inversionistas, afiliados a fondos de inversión o fondos de pensiones, tomadores de seguros, asegurados, beneficiarios de pólizas de seguros, según sea el caso.

e) Gestión de TI: estructura de relaciones y procesos diseñados y ejecutados para dirigir y controlar la tecnología de información, sus riesgos asociados y su vinculación con las estrategias y objetivos del negocio.

f) Guías de aseguramiento: guía con los pasos de prueba sugeridos para auditar el cumplimiento de los objetivos de control.

g) Gobierno de TI: componente del marco de gobierno corporativo por medio del cual, el Órgano de Dirección y la Gerencia de la entidad o vehículo de administración de recursos de terceros, evalúa, controla y dirige el uso actual y futuro de la tecnología de información, para contribuir con el soporte de las metas estratégicas y el monitoreo en el cumplimiento de los planes.

h) Hallazgo: debilidad, deficiencia o brecha apreciable respecto a un criterio o estándar previamente definido.

i) ISACA: acrónimo en inglés de la Asociación de Auditoría y Control de los Sistemas de Información (*Information Systems Audit and Control Association*).

j) Marco de Gestión de TI: conjunto de procesos, destinados a gestionar las tecnologías de información, que la entidad supervisada debe adoptar como referencia para la gestión integral de sus riesgos tecnológicos, considerando su naturaleza, complejidad, modelo de negocio, volumen de operaciones, criticidad de sus procesos y la dependencia tecnológica que estas tienen en procesos de TI.

k) Objetivo de control: declaración del resultado o fin que se desea lograr, al implantar procedimientos de control en una actividad de TI en particular.
l) Órgano de Dirección: máximo órgano colegiado de la entidad, responsable de la organización.
m) Perfil tecnológico: descripción de la estructura organizacional, los procesos y la infraestructura de TI de la entidad supervisada, así como, del nivel de automatización de sus procesos de negocio y gestión del riesgo.
n) Plan de acción: documento que describe las acciones, plazos y responsables que establezca una entidad supervisada, para atender los hallazgos y riesgos detectados y comunicados en el reporte del supervisor.
o) Prácticas de control: indicaciones detalladas para dar cumplimiento a los objetivos de control.
p) Proceso de negocio: cadena de actividades que agregan valor y permiten la generación de un producto o servicio bajo determinadas condiciones y plazo.
q) Proveedor de TI: persona física o jurídica que provee o presta un servicio relacionado con TI a la unidad de TI, o a una entidad supervisada, sea independiente o pertenezca al mismo grupo o conglomerado financiero, esto incluye las casas matrices, indistintamente de su domicilio.
r) Riesgo de TI: posibilidad de pérdidas financieras o afectaciones derivadas de un evento relacionado con el acceso o uso de la tecnología, que afecta el desarrollo de los procesos de negocio y la gestión de riesgos de la entidad, al atentar contra la confidencialidad, integridad, disponibilidad, eficiencia, confiabilidad y oportunidad de la información.
s) TI: acrónimo de Tecnologías de Información, definidas como el conjunto de técnicas para la captura, almacenamiento, transformación, transmisión y presentación de la información generada o recibida a partir de procesos de negocios, de manera que pueda ser organizada y utilizada

en forma consistente y comprensible por los usuarios que estén relacionados con ella. Incluye elementos de hardware, software, telecomunicaciones y conectividad, entre otros.

t) Tipo de gestión de TI: conjunto de características o aspectos que determinan si la gestión que realizan las entidades es individual o corporativa.

u) Unidad de TI: unidad que provee los procesos y servicios de TI para las entidades supervisadas. (Superintendencia General de Entidades Financieras, 2017)

2.4. ISACA

Con 95.000 asociados en 160 países, ISACA es un líder global proveedor de conocimiento, certificaciones, comunidad, promoción y educación sobre aseguramiento y seguridad de sistemas de información (SSII), gobierno empresarial y gestión de TI y riesgo relacionado con TI y cumplimiento. Fundada en 1969, ISACA independiente y sin ánimo de lucro, celebra conferencias internaciones, publica el ISACA® *Journal* y desarrolla estándares internaciones de control y auditoría de SSII, que ayudan a sus miembros a asegurar la confianza y aportar valor desde, los sistemas de información.

También avanza y avala habilidades y conocimientos en TI mediante los globalmente reconocidos certificados (CISA®) *Certified Information Systems Auditor*®, (CISM®) *Certified Information Security Manager*®, (CGEIT®) *Certified in the Governance of Enterprise IT*® y (CRISCTM) *Certified in Risk and Information Systems Control TM*. ISACA actualiza continuamente el COBIT®, el cual ayuda a los profesionales de TI y líderes de las organizaciones a llevar a cabo sus responsabilidades en la gestión y gobierno de TI, particularmente en las áreas de aseguramiento, seguridad, riesgo y control y proporciona valor al negocio.

ISACA se inició en 1967, cuando un pequeño grupo de personas con trabajos similares (controles de auditoría en los sistemas informáticos que se estaban

volviendo cada vez más críticos para las operaciones de sus organizaciones) se sentó para discutir la necesidad de una fuente centralizada de información y orientación en el campo. En 1969, el grupo se formalizó y se incorporó como la Asociación de Auditores de EDP.

En 1976, la asociación formó una fundación educativa para emprender esfuerzos investigativos a gran escala, para ampliar el conocimiento y el valor del campo de control y gobernanza de TI. Anteriormente, conocida como la Asociación de Auditoría y Control de Sistemas de la Información®, ISACA ahora se usa solo por sus siglas, para reflejar la amplia gama de profesionales de gobierno de TI a los que sirve.

En la actualidad, la circunscripción de ISACA, con más de 140 000 miembros en todo el mundo, se caracteriza por su diversidad. Los constituyentes viven y trabajan en más de 180 países y cubren una variedad de puestos profesionales relacionados con TI: para nombrar solo a algunos, auditor de IS, consultor, educador, profesional de seguridad de IS, regulador, director de información y auditor interno. Algunos son nuevos en el campo, otros son de nivel medio de gestión y otros están en los rangos más altos. Trabajan en casi todas las categorías de la industria, esto incluye finanzas y banca, contabilidad pública, gobierno y el sector público, servicios públicos y manufactura. Esta diversidad permite a los miembros aprender unos de otros e intercambiar puntos de vista ampliamente divergentes sobre una variedad de temas profesionales. Durante mucho tiempo ha sido considerado uno de los puntos fuertes de ISACA.

Otro de los puntos fuertes de ISACA es su red de capítulos. En ese sentido, contiene más de 200 capítulos establecidos en más de 80 países en todo el mundo, y esos capítulos brindan educación a los miembros, intercambio de recursos, defensa, redes profesionales y una gran cantidad de otros beneficios a nivel local.

Desde su creación, ISACA se ha convertido en una organización global que establece el ritmo para los profesionales de la gobernanza, el control, la seguridad y la auditoría de la información. Sus auditorías de SI (Sistemas de

Información) y sus normas de control de SI son seguidas por profesionales de todo el mundo. Su investigación señala problemas profesionales que desafían a sus electores.

Su certificación de *Certified Information Systems Auditor* (CISA) se reconoce a nivel mundial y más de 118 000 profesionales lo han obtenido desde su inicio. La certificación *Certified Information Security Manager* (CISM) se dirige exclusivamente a la audiencia de administración de seguridad de la información y ha sido obtenida por más de 28 000 profesionales.

Por otro lado, la designación *Certified in the Governance of Enterprise IT* (CGEIT) promueve el avance de los profesionales que desean ser reconocidos por su experiencia y conocimiento vinculados con el gobierno de TI y ha sido ganado por más de 6 000 profesionales. La designación de Certificado en Control de Sistemas de Riesgo e Información (CRISC) para quienes identifican y administran riesgos por medio del desarrollo, implementación y mantenimiento de controles de sistemas de información lo han obtenido más de 18 000 profesionales.

ISACA publica una revista técnica líder en el campo de control de información, la revista ISACA. Alberga una serie de conferencias internacionales que se centran en temas técnicos y de gestión pertinentes a las profesiones de aseguramiento, control, seguridad y gobierno de TI de SI. Juntos, ISACA y su Instituto de Gobernanza de TI afiliados, lideran la comunidad de control de tecnología de la información y prestan servicios a sus profesionales al proporcionar los elementos que necesitan los profesionales de TI en un entorno mundial en constante cambio.

2.5. COBIT 5

COBIT 5 es el marco de gestión y de negocio global para el gobierno y la gestión de las TI de la empresa. Este documento contiene los cinco principios de COBIT 5 y define los siete catalizadores que componen el marco; asimismo, permite

comprender el gobierno y la gestión de las tecnologías de información (TI) de una organización, así como evaluar el estado en que se encuentran las TI en la empresa.

En la siguiente imagen se muestran la familia de productos de COBIT 5:

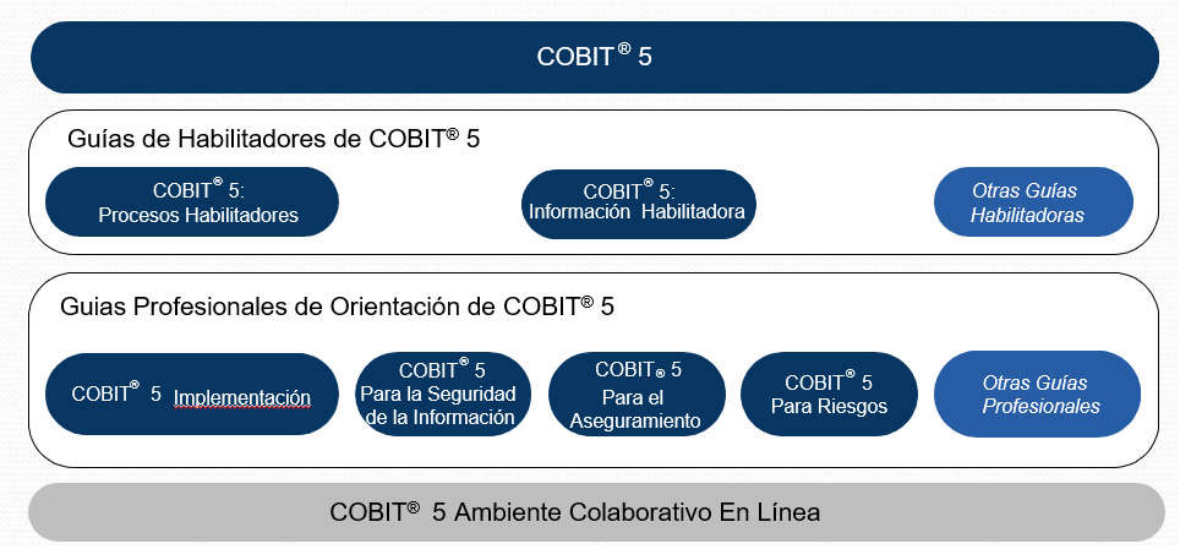

Ilustración 1. Familia de productos COBIT 5

Fuente: Procesos Catalizadores COBIT 5 (ISACA 2012).

Principios

Este marco de trabajo cuenta con cinco principios que una organización debe seguir para adoptar la gestión de TI:

a) Satisfacción de las necesidades de los accionistas: se alinean las necesidades de los accionistas con los objetivos empresariales específicos, objetivos de TI y objetivos habilitadores. Se optimiza el uso de recursos cuando se obtienen beneficios con un nivel aceptable de riesgo.

b) Considerar la empresa de punta a punta: el gobierno de TI y la gestión de TI se asumen desde una perspectiva global, de tal modo que se cubren todas las necesidades corporativas de TI. Esto se aplica desde una perspectiva "de punta a punta" basada en los siete habilitadores de COBIT.

c) Aplicar un único modelo de referencia integrado: COBIT 5 integra los mejores marcos de *Information Systems Audit and Control Association* (ISACA) como Val IT, el cual relaciona los procesos de COBIT con los de la gerencia requeridos para conseguir un buen valor de las inversiones en TI. También se vincula con Risk IT, lanzado por ISACA para ayudar a organizaciones a equilibrar los riesgos con los beneficios. Se considera el uso de *Business Model for Information Security* (BMIS) e IT *Assurance Framework* (ITAF). Además, permite alinearse con los principales estándares o marcos como *Information Technology Infrastructure Library* (ITIL), *The Open Group Architecture Forum* (TOGAF), *Project Management Body of Knowledge* (PMBOK), *PRojects IN Controlled Environments 2* (PRINCE2), *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) y estándares ISO.

d) Posibilitar un enfoque holístico: los habilitadores de COBIT 5 están identificados en siete categorías que abarcan la empresa de punta a punta. Individual y colectivamente, estos factores influyen para que el gobierno y la gestión de TI operen en función de las necesidades del negocio.

e) Separar el gobierno de la gestión: COBIT 5 distingue con claridad los ámbitos del gobierno y la gestión de TI. Se entiende por gobierno de TI las funciones relacionadas con la evaluación, la dirección y el monitoreo de las TI. El gobierno busca asegurar el logro de los objetivos empresariales y también evalúa las necesidades de los accionistas, así como las condiciones y las opciones existentes. La dirección se concreta mediante la priorización y la toma efectiva de decisiones. Y el monitoreo abarca el desempeño, el cumplimiento y el progreso de acuerdo con los objetivos acordados. La gestión está más relacionada con la planificación, la construcción, la ejecución y el monitoreo de las actividades alineadas con la dirección establecida por el organismo de gobierno para el logro de los objetivos empresariales.

Habilitadores

COBIT 5 describe siete habilitadores, los cuales se constituyen en factores que, individual y colectivamente, influyen sobre si algo funcionará, en el caso de COBIT, Gobierno y Administración sobre la TI corporativa. Impulsados por las metas en cascada, o sea: las metas de alto nivel relacionadas con la TI definen qué deberían lograr los diferentes habilitadores.

a) Procesos: describen una serie organizada de prácticas y actividades para lograr determinados objetivos y producir una serie de resultados como apoyo al logro de las metas globales relacionadas con la TI.
b) Estructuras Organizacionales: constituyen las entidades claves para la toma de decisiones en una organización.
c) Cultura, Ética y Comportamiento: de los individuos, así como de la organización; se subestima frecuentemente como factor de éxito en las actividades de gobierno y administración.
d) Principios, Políticas y Marcos: son los vehículos para traducir el comportamiento deseado en una orientación práctica para la administración diaria.
e) Información: se encuentra presente en todo el ambiente de cualquier organización; o sea se trata de toda la información producida y usada por la Organización. La información se requiere para mantener la organización en marcha y bien gobernada, pero a nivel operativo, la información frecuentemente es el producto clave de la entidad en sí.
f) Servicios, Infraestructura y Aplicaciones: incluyen la infraestructura, la tecnología y las aplicaciones que proporcionan servicios y procesamiento de tecnología de la información a la entidad.
g) Personas, Habilidades y Competencias: están vinculadas con las personas y son requeridas para completar exitosamente todas las actividades y tomar las decisiones correctas, así como para llevar a cabo las acciones correctivas.

Procesos de COBIT 5

En el Capítulo 2 se recapitula las metas en cascada de COBIT 5 y se complementa con una serie de métricas, ejemplo para las metas corporativas y las metas relacionadas con la TI.

En el Capítulo 3 se explica el Modelo de Procesos de COBIT 5 y se definen sus componentes.

En el Capítulo 4 se muestra el diagrama de dicho Modelo de Referencias de Procesos.

El Capítulo 5 contiene la información detallada de procesos para todos los 37 procesos de COBIT 5 en el Modelo de Referencias de Procesos.

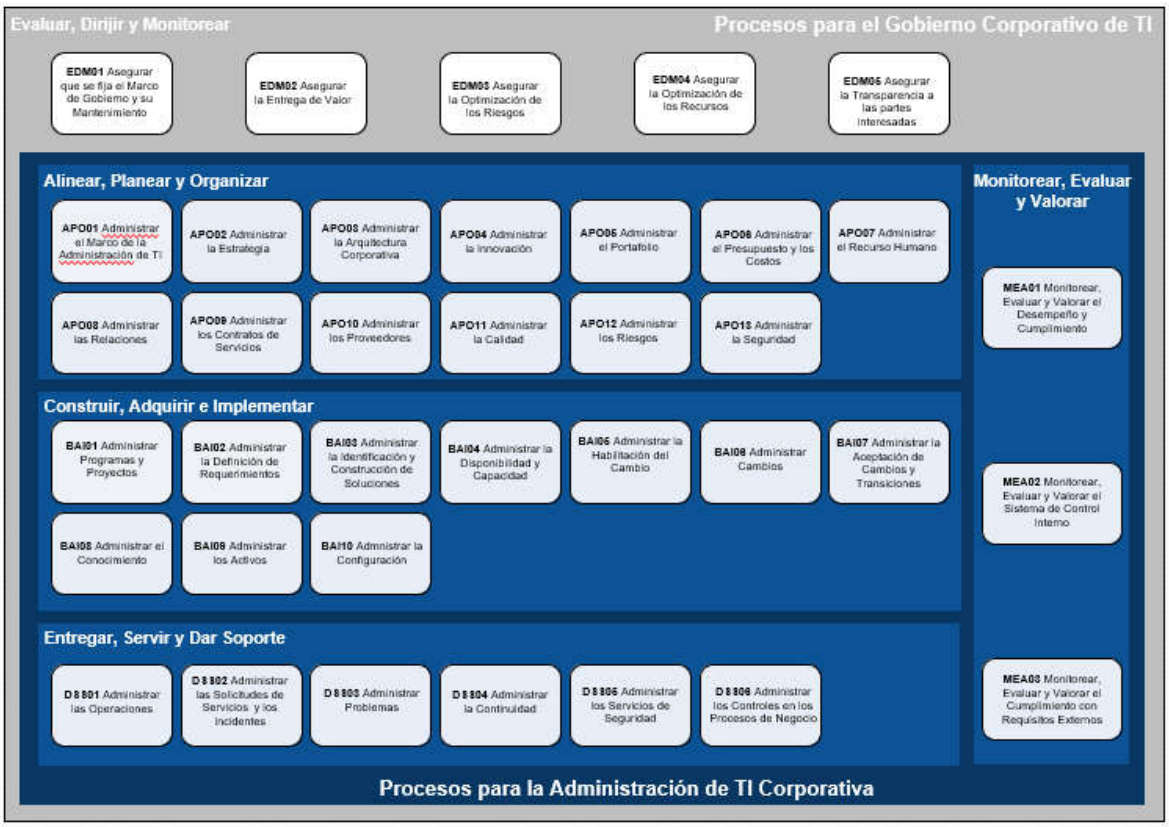

Ilustración 2. Procesos Catalizadores

Fuente: Procesos Catalizadores COBIT 5 (ISACA 2012).

2.6. Otras definiciones

ISACA (2013) Plan de continuidad de negocio: es un plan de emergencia con el objetivo de mantener la funcionalidad de la organización a un nivel mínimo aceptable durante una contingencia, como es el caso de la emergencia.

ISACA (2013) Recuperación: se trata de un proceso de recuperación que cubre los datos, el hardware y el software crítico, para que un negocio pueda comenzar de nuevo sus operaciones en caso de un desastre natural o causado por humanos.

ISACA (2013) Evento: es algo que ocurre en un lugar o tiempo específico que puede afectar la ejecución apropiada de las funciones de negocio. Pueden ser divididos en amenazas, vulnerabilidades y pérdidas.

ISACA (2013) Tecnologías de información: es la aplicación de ordenadores y equipos de telecomunicación para almacenar, recuperar, transmitir y manipular datos, con frecuencia utilizado en el contexto de los negocios u otras empresas.

ISACA (2013) COBIT: Objetivos de Control para Información y Tecnologías Relacionadas, es un marco aceptado internacionalmente como una buena práctica para el control de la información, TI y los riesgos que conllevan. COBIT se utiliza para implementar el gobierno de IT y mejorar los controles de IT.

ISACA (2013) ITIL: Biblioteca de Infraestructura de Tecnologías de la Información es un conjunto de conceptos y buenas prácticas usadas para la gestión de servicios de tecnologías de la información, el desarrollo de tecnologías de la información y las operaciones relacionadas con esta en general

ISACA (2013) Gobernabilidad: capacidad de una organización para controlar y regular su propio funcionamiento, con el fin de evitar los conflictos de intereses vinculados con la división entre los beneficiarios y los actores. Gobernabilidad de TI se refiere a la administración y la regulación de los sistemas de información que establece una compañía para el logro de sus objetivos. Por lo tanto, la gobernabilidad de TI forma parte integral del control corporativo.

ISACA (2012) ISACA: Asociación de Auditoría y Control de Sistemas de Información es líder global proveedor de conocimiento, certificaciones, comunidad, promoción y educación sobre aseguramiento y seguridad de sistemas de información (SSII), gobierno empresarial y gestión de TI y riesgo relacionado con TI y cumplimiento.

ISACA (2012) Enfoque holístico: el holismo supone que todas las propiedades de un sistema no pueden ser determinadas o explicadas como la suma de sus componentes. En otras palabras, el holismo considera que el sistema completo se comporta de un modo distinto que la suma de sus partes.

ISACA (2013) Centro de Datos: sitio físico donde el equipo informático se agrupa en armarios de almacenamiento para formar un sistema de información.

James A. Seen (2001) Flujograma: también denominado diagrama de flujo. Es una muestra visual de una línea de pasos de acciones que implican un proceso determinado. En otras palabras, el flujograma consiste en representar gráficamente, situaciones, hechos, movimientos y relaciones de todo tipo a partir de símbolos.

ISACA (2013) Mitigación: Conjunto de medidas para minimizar el impacto destructivo y perturbador de la materialización de un riesgo.

Capítulo III

3. Marco metodológico

Según Barrantes (2002), uno de los aspectos más importantes en cualquier investigación es el planteamiento del marco metodológico. Este es el que sirve para indicar cómo se planteará la investigación.

Cabe señalar que esta parte de la investigación debe describirse detalladamente, pues es la que otorga validez al estudio, la que demuestra la profundidad con la cual se realizó la investigación e indica el tipo de enfoque, el tipo de estudio y las técnicas utilizadas.

3.1. Enfoque de investigación

Hernández, Fernández y Baptista (2014) indican que los enfoques de investigación cualitativos y cuantitativos emplean procesos cuidadosos, metódicos y empíricos en su esfuerzo para generar conocimiento; por lo tanto, la definición previa de investigación se aplica a los dos por igual. En términos generales, estos métodos utilizan cinco estrategias similares y relacionadas entre sí (Grinnell, 1997):

1. Llevan a cabo la observación y evaluación de fenómenos.
2. Establecen suposiciones o ideas como consecuencia de la observación y evaluación realizadas.
3. Demuestran el grado en que las suposiciones o ideas tienen fundamento.
4. Revisan tales suposiciones o ideas sobre la base de las pruebas o del análisis.
5. Proponen nuevas observaciones y evaluaciones para esclarecer, modificar y fundamentar las suposiciones e ideas o incluso para generar otras.

3.1.1. Cualitativo

Enfoque cualitativo Utiliza la recolección y análisis de los datos para afinar las preguntas de investigación o revelar nuevas interrogantes en el proceso de interpretación.

Además de lo anterior, el enfoque o aproximación cualitativa posee las siguientes características:

1. El investigador o investigadora plantea un problema, pero no sigue un proceso definido claramente. Sus planteamientos iniciales no son tan específicos como en el enfoque cuantitativo y las preguntas de investigación no siempre se han conceptualizado ni definido por completo.
2. En la búsqueda cualitativa, en lugar de iniciar con una teoría y luego "voltear" al mundo empírico para confirmar si esta es apoyada por los datos y resultados, el investigador comienza examinando los hechos en sí y en el proceso desarrolla una teoría coherente para representar lo que observa (Esterberg, 2002). Dicho de otra forma, las investigaciones cualitativas se basan más en una lógica y proceso inductivo (explorar y describir, y luego generar perspectivas teóricas). Van de lo particular a lo general. Por ejemplo, en un estudio cualitativo típico, el investigador entrevista a una persona, analiza los datos que obtuvo y saca conclusiones; posteriormente, entrevista a otra persona, analiza esta nueva información y revisa sus resultados y conclusiones; del mismo modo, efectúa y analiza más entrevistas para comprender el fenómeno que estudia. Es decir, procede caso por caso, dato por dato, hasta llegar a una perspectiva más general.
3. En la mayoría de los estudios cualitativos no se prueban hipótesis, sino que se generan durante el proceso y se perfeccionan conforme se recaban más datos; son un resultado del estudio.
4. El enfoque se basa en métodos de recolección de datos no estandarizados ni predeterminados completamente. Tal recolección consiste en obtener las perspectivas y los puntos de vista de los participantes (sus emociones, prioridades, experiencias, significados y otros aspectos más bien subjetivos). También resultan de interés las interacciones entre individuos, grupos y colectividades. El investigador hace preguntas más abiertas, recaba datos expresados por medio del lenguaje escrito, verbal y no verbal, así como visual, los cuales describe, analiza y convierte en temas que vincula, así como reconoce sus

tendencias personales. Debido a ello, la preocupación directa del investigador se concentra en las vivencias de los participantes tal como fueron (o son) sentidas y experimentadas (Sherman y Webb, 1988). Patton (2011) define los datos cualitativos como descripciones detalladas de situaciones, eventos, personas, interacciones, conductas observadas y sus manifestaciones.

5. Así, el investigador cualitativo utiliza técnicas para recolectar datos, como: la observación no estructurada, entrevistas abiertas, revisión de documentos, discusión en grupo, evaluación de experiencias personales, registro de historias de vida, e interacción e introspección con grupos o comunidades.
6. El proceso de indagación es más flexible y se mueve entre las respuestas y el desarrollo de la teoría. Su propósito consiste en "reconstruir" la realidad, tal como la observan los actores de un sistema social definido previamente. Es holístico, porque se precia de considerar el "todo" sin reducirlo al estudio de sus partes.
7. La aproximación cualitativa evalúa el desarrollo natural de los sucesos; es decir, no hay manipulación ni estimulación de la realidad (Corbetta, 2003).
8. Este tipo de investigación se fundamenta en una perspectiva interpretativa centrada en el entendimiento del significado de las acciones de seres vivos, sobre todo de los humanos y sus instituciones (busca interpretar lo que va captando activamente).
9. Postula que la "realidad" se define por medio de las interpretaciones de los participantes en la investigación respecto de sus propias realidades. De este modo, convergen varias "realidades", por lo menos la de los participantes, la del investigador y la producida en la interacción de todos los actores. Además, son realidades que van modificándose conforme transcurre el estudio y son las fuentes de datos.
10. Por lo anterior, el investigador se introduce en las experiencias de los participantes y construye el conocimiento, siempre consciente de que es

parte del fenómeno estudiado. Así, en el centro de la investigación está situada la diversidad de ideologías y cualidades únicas de los individuos.

11. Las indagaciones cualitativas no pretenden generalizar de manera probabilística los resultados a poblaciones más amplias ni obtener necesariamente muestras representativas; incluso, por lo general no pretenden que sus estudios lleguen a repetirse.
12. El enfoque cualitativo puede concebirse como un conjunto de prácticas interpretativas que hacen al mundo “visible”, lo transforman y convierten en una serie de representaciones en forma de observaciones, anotaciones, grabaciones y documentos. Es naturalista -porque estudia los fenómenos y seres vivos en sus contextos o ambientes naturales y en su cotidianidad- e interpretativo; pues intenta encontrar sentido a los fenómenos en función de los significados que las personas les otorguen.

    En la aproximación cualitativa hay una variedad de concepciones o marcos de interpretación, los cuales guardan un común denominador: todo individuo, grupo o sistema social tiene una manera única de ver el mundo y entender situaciones y eventos, la cual se construye por el inconsciente, lo transmitido por otros y la experiencia, y mediante la investigación, se debe tratar de comprenderla en su contexto.

    Creswell (2013b) y Neuman (1994) sintetizan las actividades principales del investigador o investigadora cualitativa con los siguientes comentarios:

    - Adquiere un punto de vista “interno” (dentro del fenómeno), aunque mantiene una perspectiva analítica o cierta distancia como observador externo.
    - Utiliza diversas técnicas de investigación y habilidades sociales de una manera flexible, de acuerdo con los requerimientos de la situación.
    - No define las variables con el propósito de manipularlas experimentalmente.

- Produce datos en forma de notas extensas, diagramas, mapas o “cuadros humanos” para generar descripciones bastante detalladas.
- Extrae significado de los datos y no necesita reducirlos a números ni debe analizarlos estadísticamente (aunque el conteo puede utilizarse en el análisis).
- Entiende a los participantes que son estudiados y desarrolla una empatía hacia ellos; no solo registra hechos “objetivos”.
- Mantiene una doble perspectiva: analiza los aspectos explícitos, conscientes y manifiestos, así como aquellos implícitos, inconscientes y subyacentes. En este sentido, la realidad subjetiva en sí misma es objeto de estudio.
- Observa los procesos sin irrumpir, alterar ni imponer un punto de vista externo, sino tal como los perciben los actores del sistema social.
- Es capaz de manejar paradojas, incertidumbres, dilemas éticos y ambigüedades.

3.1.2. Cuantitativo

El enfoque cuantitativo utiliza la recolección de datos para probar hipótesis con base en la medición numérica y el análisis estadístico, con el fin de establecer pautas de comportamiento y probar teorías.

El enfoque cuantitativo tiene las siguientes características:

1. Refleja la necesidad de medir y estimar magnitudes de los fenómenos o problemas de investigación: ¿cada cuánto ocurren y con qué magnitud?
2. El investigador o investigadora plantea un problema de estudio delimitado y concreto sobre el fenómeno, aunque en evolución. Sus preguntas de investigación versan sobre cuestiones específicas.

3. Una vez planteado el problema de estudio, el investigador o investigadora considera lo que se ha indagado sobre el tema anteriormente (la revisión de la literatura) y construye un marco teórico (la teoría que habrá de guiar su estudio), del cual deriva una o varias hipótesis (aspectos que examinará si son ciertas o no) y las somete a prueba mediante el empleo de los diseños de investigación apropiados. Si los resultados corroboran las hipótesis o son congruentes con estas, se aporta evidencia en su favor. Si se refutan, se descartan en busca de mejores explicaciones y nuevas hipótesis. Al apoyar las hipótesis se genera confianza en la teoría que las sustenta. Si no es así, se rechazan las hipótesis y, eventualmente, la teoría.
4. Así, las hipótesis (por ahora se denominarán “creencias”) se generan antes de recolectar y analizar los datos.
5. La recolección de los datos se fundamenta en la medición (se miden las variables o conceptos contenidos en las hipótesis). Esta recolección se lleva a cabo al utilizar procedimientos estandarizados y aceptados por una comunidad científica. Para que una investigación sea creíble y aceptada por otros investigadores, debe demostrarse que se siguieron los procedimientos adecuados. Como en este enfoque se pretende medir, los fenómenos estudiados, deben poder observarse o referirse al “mundo real”.
6. Debido a que los datos son producto de mediciones, se representan mediante números (cantidades) y se deben analizar con métodos estadísticos.
7. En el proceso se trata de tener el mayor control para lograr que otras posibles explicaciones, distintas o “rivales” a la propuesta del estudio (hipótesis), se desechen y se excluya la incertidumbre y minimice el error. Por ello, se confía en la experimentación o las pruebas de causalidad.
8. Los análisis cuantitativos se interpretan a la luz de las predicciones iniciales (hipótesis) y estudios previos (teoría). La interpretación

constituye una explicación de cómo los resultados encajan en el conocimiento existente (Creswell, 2013a).

9. La investigación cuantitativa debe ser lo más “objetiva” posible. Los fenómenos que se observan o miden el investigador no deben afectarlos; por el contrario, debe evitar en lo posible que sus temores, creencias, deseos y tendencias influyan en los resultados del estudio o interfieran en los procesos y tampoco sean alterados por las tendencias de otros (Unrau, Grinnell y Williams, 2005).
10. Los estudios cuantitativos siguen un patrón predecible y estructurado (el proceso) y se debe tener presente que las decisiones críticas sobre el método se toman antes de recolectar los datos.
11. En una investigación cuantitativa se intenta generalizar los resultados encontrados en un grupo o segmento (muestra) a una colectividad mayor (universo o población). También se busca que los estudios efectuados puedan replicarse.
12. Al final, con los estudios cuantitativos se pretende confirmar y predecir los fenómenos investigados, buscando regularidades y relaciones causales entre elementos. Esto significa que la meta principal es la formulación y demostración de teorías.
13. Para este enfoque, si se sigue rigurosamente el proceso y, de acuerdo con ciertas reglas lógicas, los datos generados poseen los estándares de validez y confiabilidad, las conclusiones derivadas contribuirán a la generación de conocimiento.
14. Esta aproximación se vale de la lógica o razonamiento deductivo, el cual comienza con la teoría, y de esta se derivan expresiones lógicas denominadas “hipótesis” que el investigador somete a prueba.
15. La investigación cuantitativa pretende identificar leyes “universales” y causales (Bergman, 2008).
16. La búsqueda cuantitativa ocurre en la “realidad externa” al individuo. Conviene ahora explicar cómo se concibe la realidad con esta aproximación a la investigación.

Para este fin, se utilizará la siguiente argumentación basada en Grinnell (1997) y Creswell (2013a):

1. Hay dos realidades: la primera es interna y consiste en las creencias, presuposiciones y experiencias subjetivas de las personas, que van desde las muy vagas o generales (intuiciones) hasta las convicciones bien organizadas y desarrolladas lógicamente por medio de teorías formales. La segunda realidad es objetiva, externa e independiente de las creencias que se tengan sobre ella: la autoestima, una ley, los mensajes televisivos, una edificación, el sida, entre otros; es decir, cada una constituye una realidad a pesar de lo que se piense de ella.
2. Esta realidad objetiva es susceptible de conocerse. Bajo esta premisa, resulta posible investigar una realidad externa y autónoma del investigador.
3. Se necesita comprender o tener la mayor cantidad de información sobre la realidad objetiva. Se conoce la realidad del fenómeno y los eventos que la rodean por medio de sus manifestaciones. Para entender cada realidad (el porqué de las cosas), resulta necesario registrar y analizar dichos eventos. Desde luego, en el enfoque cuantitativo lo subjetivo existe y posee un valor para los investigadores; pero este enfoque se aboca a demostrar cuán bien se adecua el conocimiento a la realidad objetiva. Documentar esta coincidencia constituye un propósito central de muchos estudios cuantitativos; por ejemplo, los efectos que se consideren que provoca una enfermedad sean “verdaderos”, se capte la relación “real” entre las motivaciones de una persona y su conducta, un material que se supone posea determinada resistencia auténticamente la tenga, entre otros.
4. Cuando las investigaciones creíbles establezcan que la realidad objetiva es diferente de las propias creencias, estas deben modificarse para adaptarse a tal realidad.

3.1.3. Mixta

Roberto Hernández-Sampieri (2014) indican que la meta de la investigación mixta no es reemplazar a la investigación cuantitativa ni a la cualitativa, sino utilizar las fortalezas de ambos tipos de indagación, combinándolas y tratando de minimizar sus debilidades potenciales.

Los métodos mixtos representan un conjunto de procesos sistemáticos, empíricos y críticos de investigación e implican la recolección y el análisis de datos cuantitativos y cualitativos, así como su integración y discusión conjunta, para realizar inferencias producto de toda la información recabada (metainferencias) y lograr un mayor entendimiento del fenómeno bajo estudio (Hernández-Sampieri y Mendoza, 2008).

Por otro lado, Chen (2006) los define como la integración sistemática de los métodos cuantitativo y cualitativo en un solo estudio, con el fin de obtener una "fotografía" más completa del fenómeno y señala que estos pueden ser conjuntados, de tal manera que las aproximaciones cuantitativa y cualitativa conserven sus estructuras y procedimientos originales ("forma pura de los métodos mixtos"); o bien, que dichos métodos pueden ser adaptados, alterados o sintetizados para efectuar la investigación y lidiar con los costos del estudio ("forma modificada de los métodos mixtos").

En resumen, los métodos mixtos utilizan evidencia de datos numéricos, verbales, textuales, visuales, simbólicos y de otras clases para entender problemas en las ciencias (Creswell, 2013a y Lieber y Weisner, 2010).

Johnson et al. (2006) en un "sentido amplio" visualizan la investigación mixta como un continuo, en donde se mezclan los enfoques cuantitativo y cualitativo, y se centra más en uno de ellos o les ofrece el mismo "peso", donde cabe señalar que cuando se comente del método cuantitativo se abreviará como CUAN y cuando se trate del método cualitativo como CUAL. Asimismo, las mayúsculas-minúsculas indican prioridad o énfasis.

La decisión de emplear los métodos mixtos solo resulta apropiada cuando se agrega valor al estudio en comparación con utilizar un único enfoque, porque regularmente implica la necesidad de mayores recursos económicos, de involucramiento de más personas, conocimientos y tiempo (Lieber y Weisner, 2010).

De acuerdo con Creswell (2013a), Niglas (2010) y Unrau, Grinnell y Williams (2005), los factores que se consideran para elegir un enfoque cuantitativo, cualitativo o uno mixto son:

1. El enfoque que el investigador piense que armoniza o se adapta más a su planteamiento del problema. En este sentido, cabe recordar que los problemas los cuales necesitan establecer tendencias se ajustan mejor a un diseño cuantitativo; y, los que requieren ser explorados para obtener un entendimiento profundo, empatan más con un diseño cualitativo. Asimismo, cuando el problema o fenómeno es complejo, los métodos mixtos pueden ser la respuesta.

2. La aproximación en la cual el investigador posea más conocimientos y entrenamiento. Aunque desde luego, hoy es importante prepararse en los tres enfoques.

Ante la indecisión, Creswell (2013) sugiere buscar en la literatura cómo ha sido abordado el planteamiento y cuán exitosos han resultado los estudios que utilizaron distintos enfoques.

Anteriormente se mencionó que los métodos mixtos, utilizan evidencia de datos numéricos, verbales, textuales, visuales, simbólicos y de otras clases para comprender problemas, la presente investigación debe utilizar este enfoque; pues para brindar opciones para seleccionar la configuración que mejor se adapte para la elaboración de un procedimiento, se debe contar con: documentación, indicadores, recursos humanos, tiempo, presupuesto, entre otros elementos.

No todos los recursos con que se debe contar para un procedimiento son fácilmente medibles de forma cuantitativa, lo relacionado con recursos humanos y sus habilidades requiere en algunos casos abordarse de manera cualitativa, y, de

ahí, tomar decisiones para determinar cómo encajan dentro de un flujo que debe ser estructurado con claridad y sin posibilidad de dejar a interpretación del usuario.

3.2. Tipos de investigación

Según (Sampieri, Fernández y Lucio 2014) la investigación científica cumple dos propósitos fundamentales: a) producir conocimiento y teorías (investigación básica) y b) resolver problemas (investigación aplicada). Gracias a estos dos tipos de investigación la humanidad ha evolucionado. La investigación es la herramienta para conocer lo que nos rodea y su carácter es universal. Como señaló uno de los pensadores más connotados de finales del siglo XX, Carl Sagan, al hablar del posible contacto con seres “inteligentes” de otros mundos.

La investigación incluye la recopilación de hechos, datos e información para el avance del conocimiento. Esta actividad académica se entiende que debe seguir un proceso estructural específico. La investigación puede ser clasificada por el método o propósito. Cuando se clasifica según su propósito, hay dos categorías más importantes, esto incluye la investigación aplicada y básica.

• Investigación básica: (Sampieri, Fernández y Lucio 2014) también se conoce como investigación básica o pura. Este tipo de investigación se lleva a cabo para aumentar el conocimiento. Por lo tanto, está recogiendo conocimiento por causa del conocimiento. Se efectúa para persuadir a la curiosidad ante la pregunta de por qué los cambios de la sociedad o lo que produce que los eventos sucedan, entre otros aspectos. Sin embargo, la investigación básica casi nunca ayuda a nadie directamente. Este tipo de investigación solo alienta a formas innovadoras de pensar. De esta manera, la idea principal detrás de la investigación básica es la de ampliar los conocimientos, es la fuente más importante de la mayoría de las nuevas ideas, teorías y principios.

No obstante, en el largo plazo, la investigación básica constituye la base de desarrollo de productos comerciales o investigación aplicada. Resulta esencial comprender que la importancia de la investigación básica no se puede negar.

Cuando el trabajo de base se realiza primero y luego solo es posible seguir adelante para la investigación aplicada. No resulta factible predecir el futuro lo suficientemente bien como para pronosticar lo que construirá desde la investigación básica. Con todo, esta es investigación teórica pura, destinada a aumentar el conocimiento sobre determinadas conductas o fenómenos.

• Investigación aplicada: (Sampieri, Fernández y Lucio 2014) este tipo de investigación hace uso de los métodos del pasado, los conocimientos o las teorías o la investigación básica para resolver un problema existente. Se propone transformar el conocimiento 'puro' en conocimiento útil. Tiene por finalidad la búsqueda y consolidación del saber y la aplicación de los conocimientos para el enriquecimiento del acervo cultural y científico, así como la producción de tecnología al servicio del desarrollo integral de las naciones.

Este trabajo no está destinado a la adquisición de nuevos conocimientos en materia de continuidad de negocio; por el contrario, se basa en marcos de referencia. Por tanto, pretende solucionar un problema específico y como producto se requiere una solución tangible, lo cual indica que el tipo de investigación a seguir es aplicada, para ello se estudiará el estado actual de la cooperativa en lo relacionado a continuidad de TI, se comparará lo observado con marcos de referencia aceptados en el tema y luego se brindará opciones, para la implementación del procedimiento.

3.3. Sujetos y fuentes de la investigación

Hernández, Fernández y Baptista (2006), citando a Dahnke, distinguen tres tipos básicos de fuentes de información, e indican que estas se componen de fuentes primarias o directas, secundarias y terciarias.

Las fuentes primarias o directas son las que proporcionan información de primera mano, se pueden considerar los libros, las revistas, los periódicos, los artículos, las monografías y las tesis. Las fuentes secundarias son compilaciones, resúmenes y listados de referencias de fuentes primarias publicadas en un área de

conocimiento, en donde se mencionan y discuten artículos, libros, tesis, entre otros. Por último, las fuentes terciarias son documentos que compendian nombres y títulos de revistas, boletines, conferencias, simposios, entre otros más.

Para los insumos de este proyecto se trabaja con fuentes primarias de información, con el fin de determinar la situación actual de la cooperativa en temas de continuidad. Se investiga en los procedimientos establecidos, políticas, manuales, informes de auditoría, toda esta documentación la proporciona el jefe de TI.

Los sujetos clave para esta investigación es personal que está directamente vinculado con continuidad de negocio y TI, para esto se requiere contar con la Jefatura de TI, Oficial de Control Interno de TI y personal del área administrativa encargado del proceso de continuidad de negocio.

3.4. Población

(Sampieri, Fernández y Lucio 2014) se refiere a los participantes, objetos, sucesos o colectividades de estudio población. Es el conjunto total sobre el cual están interesados en obtener los datos y del cual desea hacer referencia; por lo general, resulta demasiado grande para abarcarlo. En este caso en particular, para esta investigación se cuenta con una población de 180 colaboradores de Coopecaja.

3.5. La muestra

Una muestra es un subgrupo de la población del cual se recolectan los datos y debe ser representativo de dicha población. La muestra es importante; pues *"pocas veces es posible medir a toda la población, por lo que obtenemos o seleccionamos una muestra y, desde luego, se pretende que este subconjunto sea un reflejo fiel del conjunto de la población"* (Hernández, Fernández y Baptista, 2006:240).

Dado el grado de dificultad que implica medir a toda la población, se selecciona una parte de esta para realizar la investigación, para hacer esto existen dos formas de seleccionarla: muestras probabilísticas y no probabilísticas o dirigidas.

Según Hernández y otros (2006), la muestra probabilística es un *"subgrupo de la población en el que todos los elementos de ésta tienen la misma probabilidad de ser elegidos"*. Para lograrlo se debe aplicar una serie de fórmulas matemáticas y estadísticas para su escogencia, y el tamaño de la muestra depende de lo homogénea o no que sea la población total.

En el caso de la muestra no probabilística o dirigida es aquella donde se *"suponen procedimientos de selección informal y hasta arbitrarios"* (Barrantes, 2005:135). Se seleccionan usualmente por la disposición del subgrupo o criterio de expertos. Son comunes donde se conocen bien las características generales de la población y existen conocimientos suficientes para asegurar la generalización de la investigación a toda la población.

Para el presente proyecto la muestra serán tres funcionarios, ellos tienen acceso a la información requerida y tienen el conocimiento de la organización y los procesos vinculados al estudio que se realiza.

3.6. Variables de la investigación

Hernández, Fernández y Baptista (2014) indican que una variable es una propiedad que puede fluctuar y cuya variación es susceptible de medirse u observarse. Ejemplos de variables son el género, la presión arterial, el atractivo físico, el aprendizaje de conceptos, la religión, la resistencia de un material, la masa, la personalidad autoritaria, la cultura fiscal y la exposición a una campaña de propaganda política. El concepto de variable se aplica a personas u otros seres vivos, objetos, hechos y fenómenos, los cuales adquieren diversos valores respecto de la variable referida. Por ejemplo, la inteligencia, ya que es posible clasificar a las personas de acuerdo con su inteligencia; no todas las personas la poseen en el mismo nivel; es decir, varían en inteligencia.

Otros ejemplos de variables son: el rendimiento de cierta especie de semilla, la eficacia de un procedimiento de construcción, el tiempo que tarda en manifestarse una enfermedad u otros. En todos los casos se producen variaciones.

Las variables adquieren valor para la investigación científica cuando llegan a relacionarse con otras variables; es decir, si forman parte de una hipótesis o una teoría. En este caso, se les suele denominar constructos o construcciones hipotéticas.

Para el enfoque cualitativo, al igual que para el cuantitativo, la recolección de datos resulta fundamental, solamente que su propósito no es medir variables para llevar a cabo inferencias y análisis estadístico. De acuerdo con lo anterior, en un estudio cualitativo se busca obtener datos (se convertirán en información) de personas, seres vivos, comunidades, situaciones o procesos en profundidad; en las propias “formas de expresión” de cada uno.

En el caso que ocupa esta investigación, al tratarse de seres humanos, los datos que interesan son conceptos, percepciones, imágenes mentales, creencias, emociones, interacciones, pensamientos, experiencias y vivencias manifestadas en el lenguaje de los participantes, ya sea de manera individual, grupal o colectiva. Se recolectan con la finalidad de analizarlos y comprenderlos, y así responder a las preguntas de la investigación y generar conocimiento.

Para esta investigación se requiere no se requiere estimar en forma numérica las variables; por tanto, se utilizarán variables cualitativas que brinden información de los procesos, políticas y manuales de la cooperativa, así como regulación vigentes y marcos de referencia, para analizar y así determinar configuraciones de un procedimiento de continuidad útil para la organización.

3.7. Técnicas e instrumentos

3.7.1. Observación

Barrantes (2002) indica que la cuidadosa observación permite “ver” más cosas de las que se observan a simple vista. Para realizar una observación científica hay una serie de consideraciones, las cuales se deben cumplir. No toda observación es científica, por ejemplo, si un extraño a la educación entra en un aula de clases, su observación podría darse en aspectos como: estructura física, cantidad de personas, forma de vestir, entre otros aspectos; pero sería difícil que observara aspectos vinculados con la metodología que está aplicando el maestro, sobre

asuntos de conducta, de utilización del espacio físico, etc. El solo hecho de que un observador extraño esté en un determinado lugar, puede traer distorsión en un fenómeno, por eso hay que decidir con mucho cuidado qué, cómo y cuándo puede observarse.

Una de las características por la que se diferencia la observación científica de otros tipos es el modo en cómo se lleva a cabo. Esta debe ser sistemática, sea que dé lugar a datos susceptibles, o bien, a los obtenidos y replicados por cualquier investigador.

Para la investigación realizada, la observación debe hacerse a la documentación que tiene Coopecaja vinculadas con políticas, procedimientos y manuales para efectuar el proceso de continuidad de negocio, estos documentos deben ser comparados con lo establecido en el proceso DSS04 Gestionar la Continuidad de COBIT 5, con el fin de encontrar brechas entre lo que se cuenta actualmente y lo que indica el marco de referencia, para luego elaborar un procedimiento para la cooperativa, el cual cumpla con lo indicado por la regulación.

3.7.2. Entrevista

Según Hernández, Fernández y Baptista (2014) una entrevista es una conversación, generalmente oral, entre dos personas, de quienes uno es el entrevistador y el otro el entrevistado. El papel de ambos puede variar según sea el tipo de entrevista.

Esencialmente, hay dos tipos de entrevistas: a) la guiada, controlada, estructurada, dirigida y b) la no dirigida o no estructurada. La diferencia fundamental entre ambas es que la entrevista no dirigida deja la iniciativa al entrevistado, esto le permite que vaya narrando sus experiencias, sus puntos de vista. El entrevistador puede hacer alguna pregunta inicial con miras a que el entrevistado exprese sus puntos de vista.

La entrevista dirigida, en cambio, sigue un procedimiento fijo, de antemano, por un cuestionario o guía, o sea, una serie de preguntas que el entrevistador prepara previamente.

Para la investigación realizada se requiere una entrevista dirigida, donde se realiza una serie de preguntas con el fin de identificar los aspectos en los cuales la documentación actual de la cooperativa cumple con lo indicado por el marco de referencia, para esto se consulta punto a punto según lo indicado en el proceso DSS04 Gestionar la Continuidad de COBIT 5 y se solicita la documentación que respalde la respuesta dada.

3.7.3. Lista de chequeo

Las “listas de control”, “listas de chequeo”, “check-lists” u “hojas de verificación”, son formatos creados para efectuar actividades repetitivas, controlar el cumplimiento de una lista de requisitos o recolectar datos ordenadamente y de forma sistemática. Se usan para hacer comprobaciones sistemáticas de actividades o productos asegurándose de que el trabajador o inspector no se olvida de nada importante.

Los usos principales de las listas de chequeo son los siguientes:

1. Realización de actividades en las que es importante que no se olvide ningún paso o deben hacerse las tareas con un orden establecido.
2. Realización de inspecciones donde se debe dejar constancia de cuáles han sido los puntos inspeccionados.
3. Verificar o examinar artículos.
4. Examinar o analizar la localización de defectos. Verificar las causas de los defectos.
5. Verificación y análisis de operaciones.
6. Recopilar datos para su futuro análisis.

Para esta investigación es necesario efectuar una lista de chequeo con los requisitos descritos en el proceso de COBIT 5 DSS04 Gestionar la Continuidad, para compararlos con lo establecido por Coopecaja y así identificar brechas que serán insumo en la recomendación del procedimiento a implementar para la continuidad de TI.

Capítulo IV

4. Análisis de resultados

Al utilizar las herramientas descritas anteriormente, en este capítulo se puede verificar el estado actual de Coopecaja en el procedimiento de continuidad de TI y hacia dónde se requiere llevar para cumplir con la regulación actual, alineado al marco de gestión de TI y también utilizar como referencia el marco de referencia COBIT 5.

Se mostrarán las principales brechas entre el procedimiento actual y el proceso DSS04 Gestionar la continuidad del marco de referencia.

4.1. Estudio de factibilidad

En ese sentido, Sampieri, Fernández y Lucio (2014) indican que resulta necesario considerar un aspecto importante del planteamiento del problema: la viabilidad o factibilidad del estudio; para ello, se debe tomar en cuenta la disponibilidad de tiempo, recursos financieros, humanos y materiales que determinarán, en última instancia, los alcances de la investigación (Mertens, 2010 y Rojas, 2001).

Asimismo, resulta indispensable que se tenga acceso al lugar o contexto donde se realizará el estudio. Es decir, cabe preguntarse, de manera realista, si es posible llevar a cabo esta investigación y cuánto tiempo tomará efectuarla. Estas preguntas son particularmente importantes cuando se sabe de antemano que se dispondrá de pocos recursos.

Las investigaciones que se demoran más allá de lo previsto pueden no ser útiles cuando se concluyen, sea porque sus resultados no se aplican, o han sido superados por otros estudios o bien, porque el contexto cambió. La oportunidad y el cumplimiento de las especificaciones son esenciales (Hernández-Sampieri, 2014).

Asimismo, La viabilidad es un elemento que se valora y se pondera según el tiempo, los recursos y las capacidades. ¿Es posible llevar a cabo el estudio? ¿Se cuenta con los recursos para hacerlo?

En relación con las deficiencias del conocimiento del problema, cabe indicar qué contribuciones hará la investigación al conocimiento actual.

Para la implementación de un procedimiento de continuidad de TI para Coopecaja, se realiza un estudio de factibilidad mostrando tres escenarios distintos:

1) Escenario 1: implementar un procedimiento TI basado en el procedimiento de continuidad de negocio ya existente en Coopecaja.
2) Escenario 2: implementar un procedimiento de continuidad de TI desde cero, sin considerar lo existente por negocio.
3) Escenario 3: realizar una reingeniería a procedimiento de negocio, esto incluye el procedimiento de continuidad de TI.

Coopecaja cuenta con los recursos humanos, tecnológicos y económicos para efectuar la implementación siguiendo cualquiera de los tres escenarios. A continuación, se indican los principales recursos necesarios:

- Recurso humano: Coopecaja posee el personal para continuidad de negocio, riesgo operativo, en TI se cuenta con un recurso para temas regulatorios y mejora de procedimientos, además del apoyo de la gerencia general.
- Tecnológico: la cooperativa tiene un centro de datos ubicado en la sede central, además posee un sitio alterno con un esquema de alta disponibilidad, el cual utiliza ya hace varios años atrás.

Dado lo anterior se presenta a continuación los resultados del estudio de factibilidad, donde se observa que el factor que puede pesar para cualquiera de los escenarios es el tiempo de implementación y la diferencia en costo por hora de personal requerido.

Seguidamente, se muestra en forma resumida un comparativo de las distintas factibilidades para los tres escenarios propuestos, los cuadros de color representan en forma proporcional la diferencia que hay para cada uno de los escenarios en términos de costos, horas y cantidad de personal, tecnología requerida y estructura organizativa.

Factibilidad	Implementar un procedimiento TI basado en el procedimiento ya existente de negocio	Implementar un procedimiento desde cero específico para TI	Reingeniería a procedimiento de negocio incluyendo procedimiento de TI
Económica			
Operativa			
Técnica			
Institucional (Tamaño del cambio)			

Tabla 2. Comparativo estudio factibilidad

Fuente: elaboración propia.

4.1.1. Factibilidad económica

James A. Seen (2001) se refiere a que se dispone del capital en efectivo o de los créditos de financiamiento necesarios para invertir en el desarrollo del proyecto, mismo que deberá haber probado que sus beneficios a obtener son superiores a sus costos en los cuales incurrirá al desarrollar e implementar el proyecto o sistema.

Como se mencionó anteriormente, Coopecaja cuenta con recursos humanos y tecnológicos para la implementación de un procedimiento de continuidad de TI, en este caso el factor económico está relacionado al costo por hora de recurso humano requerido para la implementación y la cantidad de horas necesarias de cada uno de los involucrados, a continuación, se muestra el costo para cada uno de los escenarios.

Criterio	Implementar un procedimiento TI basado en el procedimiento ya existente de negocio		Implementar un procedimiento desde cero específico para TI		Reingeniería a procedimiento de negocio incluyendo procedimiento de TI	
Horas personal	Jefe TI	(20h x $31 = $625)	Jefe TI	(80h x $31 = $2500)	Jefe TI	(80h x $31 = $2500)
	Oficial C.I.	(60h x $13 = $750)	Oficial C.I.	(120h x $13 = $1500)	Oficial C.I.	(120h x $13 = $1500)
	Encargado C.N.	(12h x $13 = $150)	Encargado C.N.	(8h x $13 = $100)	Encargado C.N.	(80h x $13 = $100)
	Oficial R.O.	(8h x $31 = $250)	Oficial R.O.	(8h x $31 = $250)	Oficial R.O.	(8h x $31 = $250)
	Gerente general	(2h x $63 = $125)	Gerente general	(2h x $63 = $125)	Gerente general	(8h x $63 = $500)
	Estudiante	(20h x $0 = $0)	Estudiante	(80h x $0 = $0)	Estudiante	(0h x $0 = $0)
	Consultor	(0h x $70 = $0)	Consultor	(0h x $70 = $0)	Consultor	(120h x $70 = $8400)
Total $		**$ 1.900**		**$ 4.475**		**$14.150**

Tabla 3. Factibilidad económica

Fuente: elaboración propia.

Los tiempos indicados para cada uno de los recursos se estiman de acuerdo con la implementación de otros procedimientos que ha realizado Coopecaja, utilizando cada unos de los tres escenarios.

Por temas de confidencialidad no se brindó información de salarios, lo que se proporcionó es la relación entre los salarios de los disitintos puestos y un aproximado basado en salarios de otras empresas similares a la cooperativa.

Puesto	Salario Mes	Horas laboradas x mes	Salario x Hora
Jefe TI	$5 000	160	$31
Oficial C.I.	$2 000	160	$13
Encargado C.N.	$2 000	160	$13
Oficial R.O.	$5 000	160	$31
Gerente General	$10 000	160	$63
Consultor			$70

Tabla 4. Salarios

Fuente: elaboración propia.

El costo de cualquiera de los escenarios está dentro de los rangos de un proyecto “pequeño” para la cooperativa; por tanto, resulta viable económicamente y la necesidad de cumplir con una regulación es de suficiente peso para que cualquiera de los casos esté justificado en términos de costo – beneficio.

4.1.2. Factibilidad operativa

Por otro lado, James A. Seen (2001) menciona todos aquellos recursos donde interviene algún tipo de actividad (Procesos), depende de los recursos humanos que participen durante la operación del proyecto.

Para la implementación del procedimiento de continuidad de TI se consideró el personal requerido y la cantidad de horas por recurso humano.

La ejecución del procedimiento se lleva a cabo por los mismos actores en cualquiera de los tres escenarios, por tanto, no se incluye en el comparativo que se muestra a continuación.

Criterio	Implementar un procedimiento TI basado en el procedimiento ya existente de negocio	Implementar un procedimiento desde cero específico para TI	Reingeniería a procedimiento de negocio incluyendo procedimiento de TI
Horas personal	Jefe TI 20h	Jefe TI 80h	Jefe TI 80h
	Oficial C.I. 60h	Oficial C.I. 120h	Oficial C.I. 120h
	Encargado C.N. 12h	Encargado C.N. 8h	Encargado C.N. 80h
	Oficial R.O. 8h	Oficial R.O. 8h	Oficial R.O. 8h
	Gerente general 2h	Gerente general 2h	Gerente general 8h
	Estudiante 20h	Estudiante 80h	Estudiante 0h
	Consultor 0h	Consultor 0h	Consultor 120h

Tabla 5. Factibilidad operativa

Fuente: elaboración propia.

4.1.3. Factibilidad técnica

Asimismo, James A. Seen (2001) indica si se dispone del equipo y las herramientas para ejecutarlo, de no ser así, si existe la posibilidad de generarlos o crearlos en el tiempo requerido por el proyecto.

Anteriormente se mencionó que Coopecaja cuenta con un moderno centro de datos ubicado en la sede central, además está soportado por un sitio alterno con todas las condiciones requeridas para trabajar en contingencia ante una eventualidad. En el siguiente cuadro se detalla la infraestructura requerida para la contingencia tecnológica, para cualquiera de los escenarios se utiliza la misma infraestructura, no es requerido incurrir en gastos extra.

Requerimiento	Costo por mes
Centro de datos en sitio	$3000
Centro de datos alterno	$8000
Enlace de datos principal	$500
Enlace de datos contingencia	$500
Total $	**$12000**

Tabla 6. Factibilidad Técnica

Fuente: elaboración propia.

4.1.4. Factibilidad institucional

La factibilidad institucional se refiere a la voluntad política de las autoridades de Coopecaja para implantar un lineamiento, norma o procedimiento en la institución. Esta es la condición primera y excluyente, si no existe voluntad política, no se puede implantar con éxito desde el gobierno, e incluso sería casi una pérdida

de tiempo y recursos, para presentar cambios ante la alta gerencia. Cabe indicar el tamaño del cambio a realizar para que, basado en esto, se tome la decisión.

Criterio	Implementar un procedimiento TI basado en el procedimiento ya existente de negocio	Implementar un procedimiento desde cero específico para TI	Reingeniería a procedimiento de negocio incluyendo procedimiento de TI
Tamaño de cambio	Mediano	Pequeño	Grande

Tabla 7. Factibilidad institucional

Fuente: elaboración propia.

4.2. Resultados de lista de chequeo

Para la implementación del procedimiento de continuidad de TI para Coopecaja se utiliza de referencia el marco COBIT 5, no es requisito tener una implementación que cumpla al 100% con cada una de las actividades descritas en este marco; sin embargo, si se toma como base el libro Procesos Catalizadores de COBIT 5, se elabora una lista de chequeo y se utilizan las actividades descritas en cada una de las prácticas de gestión del proceso.

Lo que se pretende con esta lista de chequeo, es ofrecer una comparación entre lo implementado actualmente en la cooperativa y lo descrito por el marco de referencia COBIT 5, las brechas que se detecten pueden formar parte del proceso a implementar por Coopecaja.

En COBIT 5 se cuenta con otras herramientas para evaluar los procedimientos de una organización, pero para este caso, por tratarse de una implementación, se utilizarán las actividades de las prácticas de gestión, cuando la cooperativa madure más en este procedimiento podrá utilizar otras herramientas para evaluar el procedimiento.

A continuación, se muestra un resumen del resultado de la lista de chequeo, más adelante se describen las brechas detectadas.

Práctica de gestión	Porcentaje de cumplimiento	Activades evaluadas	Cumplen	No Cumplen
DSS04.01 Definir la política de continuidad de negocio, objetivos y alcance.	63%	8	5	3
DSS04.02 Mantener una estrategia de continuidad.	44%	9	4	5
DSS04.03 Desarrollar e implementar una respuesta a la continuidad del negocio.	86%	14	12	2
DSS04.04 Ejercitar, probar y revisar el BCP.	73%	11	8	3
DSS04.05 Revisar, mantener y mejorar el plan de continuidad.	50%	10	5	5
DSS04.06 Proporcionar formación en el plan de continuidad.	100%	3	3	0
DSS04.07 Gestionar acuerdos de respaldo.	100%	5	5	0
DSS04.08 Ejectuar revisiones post-reanudación.	100%	4	4	0

Tabla 8. Resumen resultado lista de chequeo

Fuente: elaboración propia.

4.2.1. Brechas detectadas

Según la revisión efectuada, la cual se apoya en la lista de chequeo descrita anteriormente, se detectan las siguientes brechas entre el procedimiento actual de Coopecaja y el proceso DSS04 Gestionar la continuidad del marco de referencia COBIT 5.

Práctica de gestión	Brecha
DSS04.01 Definir la política de continuidad de negocio, objetivos y alcance.	A pesar de que en continuidad de negocio se observan aspectos como identificación de procesos internos de negocio, actividades subcontratadas y de servicio que son críticas para las operaciones de la empresa o necesarias para cumplir con las obligaciones legales o contractuales, continuidad de TI no los tiene contemplados.

Práctica de gestión	Brecha
DSS04.02 Mantener una estrategia de continuidad.	El plan de continuidad de TI se elabora y actualiza periódicamente, pero no contempla criterio importantes como: Establecer el tiempo mínimo necesario para recuperar un proceso de negocio y su soporte de TI. Analizar la probabilidad de amenazas que puedan causar pérdidas de continuidad de negocio e identificar medidas que puedan reducir la probabilidad y el impacto, para mejorar la prevención e incrementar la resiliencia. Analizar los requerimientos de continuidad para identificar las posibles estrategias de negocio y opciones técnicas. Determinar las condiciones de decisiones clave que puedan causar la invocación de los planes de continuidad. Identificar los requerimientos de recursos y costes para cada opción técnica estratégica y realizar recomendaciones estratégicas.
DSS04.03 Desarrollar e implementar una respuesta a la continuidad del negocio.	En la respuesta de continuidad de TI no se observa que se contemplen las habilidades necesarias para los individuos implicados en la ejecución de los planes y procedimientos ni planes de proveedores de servicio externalizados.
DSS04.04 Ejercitar, probar y revisar el BCP.	No se observa que las pruebas a los planes de continuidad contemplen la definición de objetivos para ejercitar y probar los sistemas del plan (logísticos, procedimentales y administrativos) para verificar la completitud del plan de continuidad de negocio (BCP) y enfrentarse a los riesgos de negocio.
DSS04.05 Revisar, mantener y mejorar el plan de continuidad.	En las revisiones de los planes de continuidad de TI no se observa que se considere el impacto de cambios nuevos o mayores en: organización de la empresa, procesos de negocio y acuerdos de externalización.

Tabla 9. Brechas lista de chequeo

Fuente: elaboración propia.

4.3. Resultados de las entrevistas

Se entrevistó al personal encargado de control interno de TI y al de continuidad de negocio, con el fin de comprender mejor lo descrito en los procedimientos de ambas áreas. En la entrevista al personal encargado de continuidad de negocio explica a fondo el plan con el que cuentan, en este se observa que muchas de las actividades que debe realizar TI ya son efectuadas por negocio. El encargado de control interno de TI responde que el departamento de TI puede adaptarse a lo utilizado por el negocio para mejorar su procedimiento de continuidad.

Por otro lado, el personal encargado de continuidad de negocio comenta que aspectos detectados como debilidades en la lista de chequeo, tales como: los criterios para la activación del plan de continuidad, los criterios para la actualización del plan de continuidad, la periodicidad con que debe ser actualizado, el canal oficial de comunicación, los procesos de negocio que deben ser considerados, ya están contemplados dentro del plan de continuidad de negocio, todos estos criterios pueden ser referenciados del plan de continuidad de TI y así utilizar un mismo procedimiento para ambas áreas; con ello se consigue mayor efectividad y se garantiza una actualización de ambos procedimientos en el momento requerido y según lo indicado en el marco de referencia utilizado.

Pregunta	Control Interno TI	Continuidad de negocio
¿Cada cuánto se actualiza el plan de continuidad?	Una vez al año	Existen distintos criterios que se encuentran documentados en el plan de continuidad de negocio.
¿Cuáles criterios se utilizan para la actualización del plan de continuidad?	Periodicidad, una vez al año	Cuando ocurren: Incidentes de TI Incidentes operativos Desastre natural Evento acción industrial Eventos geopolíticos Imagen de Cooperativa comprometida Incumplimiento regulatorio.

Pregunta	Control Interno TI	Continuidad de negocio
¿Cómo se determinan las necesidades de negocio en temas de continuidad?	Según lo establecido en el BIA	Según lo establecido en el BIA.
¿Cuál es el canal oficial para comunicar eventos que requieran activar protocolos de continuidad?	Área de comunicaciones	Área de comunicaciones.
¿Cuáles procesos de negocio deben ser considerados en el BIA?	No está claro	Los que soportan la operación de los servicios críticos y que están en el catálogo oficial de procesos de negocio.

4.4. Resultados de la observación

Para realizar esta técnica se solicita a Coopecaja documentación vinculada con continuidad de TI y de negocio, se proporcionan los siguientes documentos:

- Plan de continuidad de negocio
- Análisis de impacto de TI (TIA)
- Plan de continuidad de TI
- Mapa de procesos de Coopecaja
- Inventario de servicios de Coopecaja
- Lineamientos generales de continuidad de negocio
- Planes alternos de operación
- Planes de recuperación
- Capacitación de continuidad de negocio

Los documentos presentados se revisan y se comparan con lo indicado en la entrevista realizada; además, resultan un insumo para completar la lista de chequeo que se efectúa según el proceso DSS04 Gestionar la Continuidad de COBIT 5, la documentación sirve de evidencia para sustentar lo indicado en la ejecución de la lista de chequeo.

Como resultado de la observación de los documentos presentados, se identifica que varios de los aspectos requeridos por el proceso DSS04 Gestionar la Continuidad de COBIT 5, los lleva a cabo Coopecaja; sin embargo, no están debidamente documentados en un procedimiento, lo cual provoca que la institución se encuentre en incumplimiento ante un regulador.

4.4.1. Resultado de revisión de documentos

Seguidamente, se presentan las brechas identificadas por parte de la gestión de TI, pero que son ejecutadas y documentadas en la gestión realizada por parte del área de continuidad de negocio.

Brecha detectada en TI	¿Se ejecuta en Coopecaja?	Comentario
No se identifican procesos de negocio internos que sean críticos para las operaciones de la empresa o necesarias	Sí	Está en plan de continuidad de negocio, no en el de TI.
No se establece el tiempo mínimo necesario para recuperar un proceso de negocio y su soporte de TI, basándose en una duración aceptable de interrupción del negocio y la interrupción máxima tolerable.	Sí	Está en plan de continuidad de negocio, no en el de TI.
No se analiza la probabilidad de amenazas que puedan causar pérdidas de continuidad de negocio e identificar medidas que puedan reducir la probabilidad y el impacto, mejorando la prevención e incrementando la resiliencia.	Sí	Está en plan de continuidad de negocio, no en el de TI.
No se analizan los requerimientos de continuidad para identificar las posibles estrategias de negocio y opciones técnicas.	Sí	Está en plan de continuidad de negocio, no en el de TI.

Brecha detectada en TI	¿Se ejecuta en Coopecaja?	Comentario
No se determinan las condiciones de decisiones clave que puedan causar la invocación de los planes de continuidad.	Sí	Está en plan de continuidad de negocio, no en el de TI.
No se identifican los requerimientos de recursos y costes para cada opción técnica estratégica y realizar recomendaciones estratégicas.	Sí	Está en plan de continuidad de negocio, no en el de TI.
No se determinan las habilidades necesarias para los individuos implicados en la ejecución de los planes y procedimientos.	Sí	Está en plan de continuidad de negocio, no en el de TI.
No están definidos los objetivos para ejercitar y probar los sistemas del plan (logísticos) para verificar la completitud del plan de continuidad de negocio (BCP) para enfrentarse los riesgos de negocio.	Sí	Está en plan de continuidad de negocio, no en el de TI.
No se revisa el plan y la capacidad de continuidad de forma regular frente a las adquisiciones hechas y los objetivos de negocio actuales, tanto estratégicos como operativos.	Sí	Está en plan de continuidad de negocio, no en el de TI.
No se considera si es necesario una revisión del análisis de impacto en el negocio, dependiendo de la naturaleza de los cambios.	Sí	Está en plan de continuidad de negocio, no en el de TI.
No se revisa el plan de continuidad regularmente para considerar el impacto de cambios nuevos o mayores en: organización de la empresa.	Sí	Está en plan de continuidad de negocio, no en el de TI.

4.4.2. Criterio experto

El plan de continuidad de negocio de Coopecaja se halla bastante completo con respecto a lo requerido, según las prácticas de gestión del proceso de COBIT 5 DSS04 Gestionar la continuidad, toda la documentación está debidamente aprobada por los órganos correspondientes, se lleva de forma ordenada de acuerdo con los criterios de calidad establecidos por la organización.

Con el plan de continuidad de negocio definido, se puede hacer frente a eventos de gran impacto para la cooperativa, este plan contiene muchos de los requerimientos para el plan de continuidad de TI.

El personal encargado de la continuidad de negocio conoce bien todos los requerimientos para actualización y ejecución de los planes, se encuentra en capacidad de defender y ejecutar lo establecido en el proceso antes, durante y después de un evento.

Capítulo V

5. Propuesta

En este capítulo se hará referencia a una propuesta para la implementación de un procedimiento para Continuidad de TI, alineado con el Marco de Gestión de TI existente para el Departamento de Tecnologías de Información; además, se basa en el estudio de factibilidad y se compara con tres distintos de escenarios: implementación de un procedimiento para continuidad de TI desde cero; implementación de un procedimiento para continuidad de TI basado en el proceso de continuidad de negocio o la reingeniería del proceso de continuidad de negocio incluyendo continuidad de TI. Se observa como opción más factible implementar un procedimiento de continuidad de TI basado en el proceso de continuidad de negocio.

La siguiente es una propuesta según el escenario indicado anteriormente, queda a libertad de la empresa implementar el procedimiento a su mejor parecer, según los escenarios presentados.

5.1. Flujograma

Para una adecuada gestión de la continuidad de TI se propone un procedimiento integrado con continuidad de negocio y otras áreas de apoyo, requeridas para obtener los insumos necesarios para una óptima valoración de los riesgos y así construir o actualizar un plan de continuidad que contemple las distintas necesidades del negocio en términos de control y recuperación.

El flujograma para la actualización del plan de continuidad de negocio muestra cómo las distintas áreas proporcionan la información requerida para cada paso siguiente en que interviene otra área. En ese sentido, se inicia con el área de continuidad que se encarga de brindar el inventario de procesos de negocio con sus respectivos responsables, para luego elaborar el análisis de impacto de negocio apoyándose en la información brindada por TI de los activos del inventario de activos de información que soportan los procesos de negocio; una vez realizado el análisis de impacto de negocio, continuidad, con apoyo de la información obtenida del área de riesgos operativos, se determina la criticidad de los procesos de

negocio, para luego indicar la asociación con los activos de información y su dependencia.

Ya identificados los procesos críticos de negocio, la clasificación de la información y los activos de información que los soporta, se procede a identificar los activos de información que son críticos; para ello se utilizan las amenazas y las vulnerabilidades de TI más las metas críticas y procesos que los soportan, acompañado de las amenazas y las vulnerabilidades de seguridad de información, se identifican los escenarios de riesgos de TI, para estos escenarios también se utiliza el catálogo de riesgos genéricos asociado al procedimiento de continuidad de TI.

Luego de obtener los escenarios de riesgos, se continúa con los pasos de la gestión de riesgos, que consta de la evaluación, para la cual es requerida la historia como incidentes de TI y de seguridad, hallazgos de auditoría, entre otros, más la estimación de eventos que no han ocurrido.

Con lo anterior mencionado, se obtiene una valoración de riesgos que será utilizada para dos gestiones: 1) los riesgos que se determine afectan la continuidad de negocio, requieren ser incluidos en los planes de continuidad y recuperación, 2) tanto los riesgos que afectan la continuidad, como los que no y superen el apetito de riesgos establecido por la organización, deben tener planes de mitigación. Con esto se consigue buscar acciones de mitigación para los riesgos de TI que afectan el negocio teniendo como compensatorios planes de continuidad y recuperación.

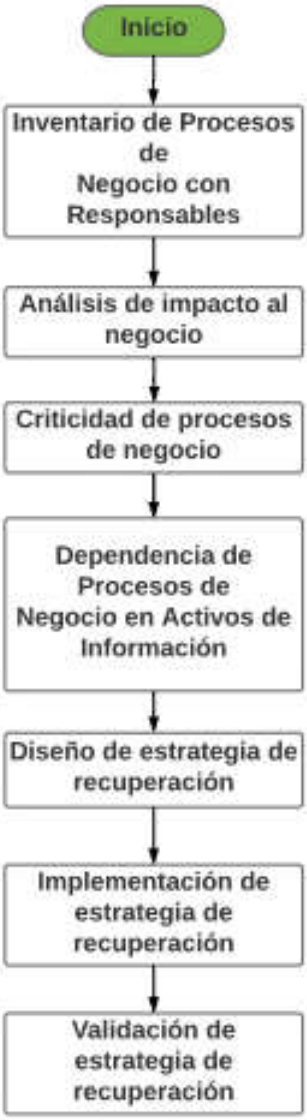

Ilustración 3. Flujograma actual

Fuente: elaboración propia.

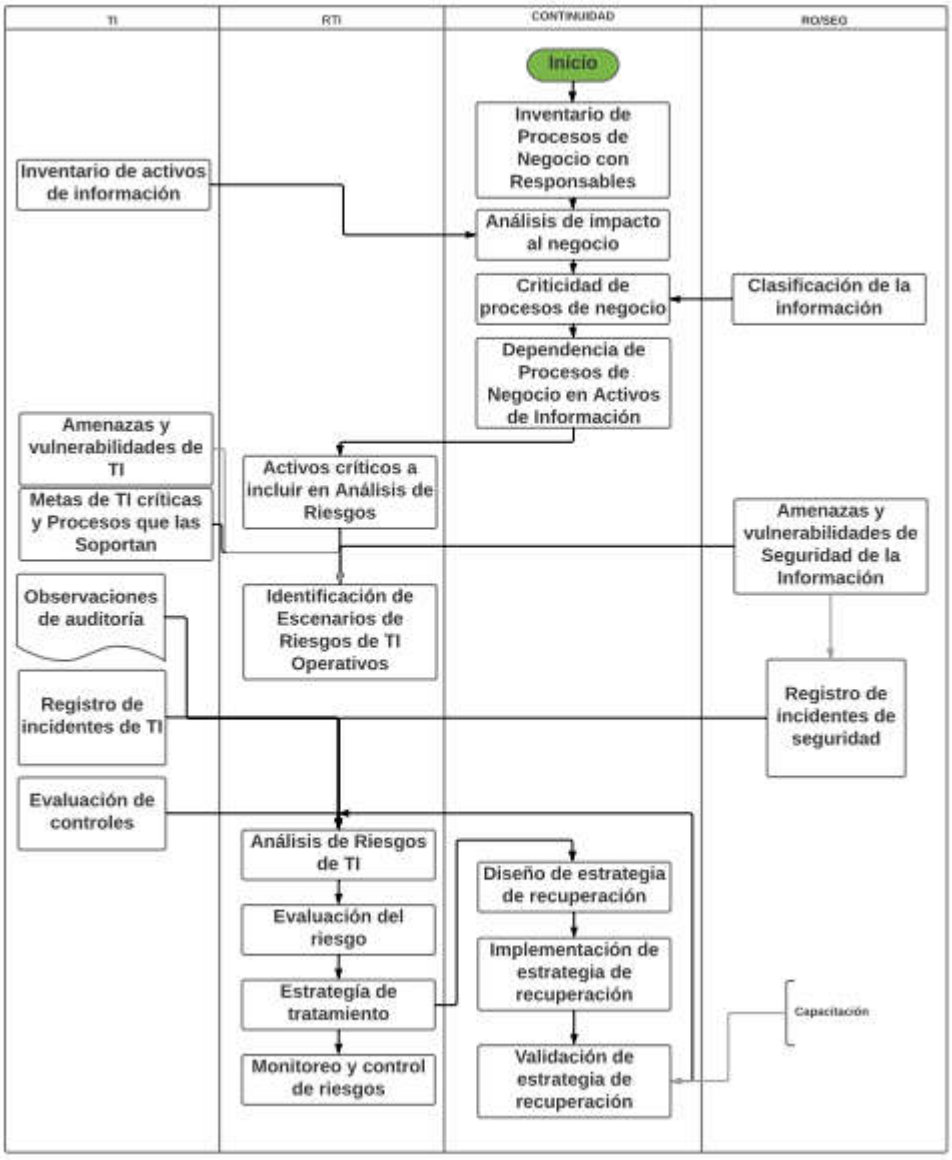

Ilustración 4. Flujograma propuesto

Fuente: elaboración propia.

5.2. Matriz de responsabilidades

A continuación, se presenta la matriz de responsabilidades propuesta para llevar a cabo la actualización del plan de continuidad de negocio y los demás pasos del procedimiento de continuidad.

Actividad/Recurso	Jefe de TI	Jefe operaciones	Encargado de RTI	Encargado de Continuidad	Riesgo Operativo / Seguridad de	Comité de Continuidad
Establecer procesos críticos mediante análisis de impacto al negocio		A		R	C	I
Identificar escenarios de riesgos de TI	R		R	A	C	I
Gestionar estrategias de recuperación de TI	A/R		C	C	C	I
Velar por la oportuna actualización del plan de continuidad de TI	R	A	C	R	C	I
Gestionar todo lo referente a la comunicación ante eventos de impacto al negocio	R	A	I	R	I	I
Aprobar plan de continuidad de TI	C			C	C	A
Definir la política de continuidad del negocio, objetivos y alcance.		A				
Mantener una estrategia de Continuidad.		A		R	C	
Desarrollar e implementar una respuesta a la continuidad del negocio.	R	R		A		
Ejercitar, probar y revisar el plan de continuidad.	R	R		A		
Revisar, mantener y mejorar el plan de continuidad.		A	C	R	C	
Revisar, mantener y mejorar el plan de continuidad.				A		R
Ejecutar revisiones postreanudación				A		R

Tabla 10. Matriz de responsabilidades

Fuente: elaboración propia.

5.3. Indicadores del procedimiento

<table>
<tr><td colspan="5">Actualización de planes</td></tr>
<tr><td>Responsable</td><td colspan="4">Encargado de continuidad.</td></tr>
<tr><td>Objetivo</td><td colspan="4">Conocer si el plan de continuidad de TI se actualiza en todas las ocasiones que es requerido.</td></tr>
<tr><td colspan="2">Descripción

Porcentaje de veces que se actualizó el plan de continuidad de TI.</td><td colspan="3">Fórmula Matemática

x = (Cantidad de veces que se actualizó el plan/cantidad de veces que debía actualizarse el plan) * 100</td></tr>
<tr><td colspan="2">Información</td><td>Fuente de datos</td><td colspan="2">Tolerancia</td></tr>
<tr><td>Unidad</td><td>N/A.</td><td rowspan="3">Reportes de Mesa de Servicio.</td><td>Verde</td><td>85%≤x</td></tr>
<tr><td>Frecuencia</td><td>Anual.</td><td>Amarillo</td><td>70%≤x<85%</td></tr>
<tr><td>Meta</td><td>85%.</td><td>Rojo</td><td>x<70%</td></tr>
</table>

Tabla 11. Indicador 1

Fuente: elaboración propia.

<table>
<tr><td colspan="5">Ejecución de pruebas de continuidad</td></tr>
<tr><td>Responsable</td><td colspan="4">Encargado de continuidad.</td></tr>
<tr><td>Objetivo</td><td colspan="4">Conocer si las pruebas de continuidad fueron ejecutadas.</td></tr>
<tr><td colspan="2">Descripción

Porcentaje de pruebas planificadas que se ejecutaron.</td><td colspan="3">Fórmula matemática

x = (Cantidad de pruebas ejecutadas/total de pruebas planificadas) * 100</td></tr>
<tr><td colspan="2">Información</td><td>Fuente de datos</td><td colspan="2">Tolerancia</td></tr>
<tr><td>Unidad</td><td>N/A.</td><td rowspan="3">Reportes de Mesa de Servicio.</td><td>Verde</td><td>85%≤x</td></tr>
<tr><td>Frecuencia</td><td>Mensual.</td><td>Amarillo</td><td>70%≤x<85%</td></tr>
<tr><td>Meta</td><td>85%.</td><td>Rojo</td><td>x<70%</td></tr>
</table>

Tabla 12. Indicador 2

Fuente: elaboración propia.

5.4. Procedimiento

a) Definir la política de continuidad de negocio, objetivos y alcance

El encargado de continuidad de negocio debe definir una directriz de continuidad, la cual incluya objetivos y alcances. El Comité de Continuidad de Negocios debe aprobar por y revisar esta política al menos una vez al año.

La directriz debe establecer las pautas para la activación y la actualización de los planes de continuidad, así como los responsables y los canales utilizados para la adecuada comunicación. Además, debe indicarse cuál es la estrategia de continuidad que la cooperativa ha implementado, y, basado en esta estrategia del negocio, se establece el procedimiento de continuidad de la entidad.

b) Mantener una estrategia de continuidad

El encargado de continuidad de negocio en conjunto con la jefatura de TI son los responsables de mantener la estrategia de continuidad definida en la *Business Continuity Plan* (BCP), ahí contemplan todo lo requerido a nivel de negocio y tecnologías de información. Para esto se necesita que se se efectúe un análisis de impacto de negocio (BIA y TIA), en el cual se establecen las necesidades de negocio y los tiempos de recuperación. En el flujograma (Anexo xxxx) se muestran los pasos a seguir para el mantenimiento de planes de continuidad.

El documento PLA-006 BCP_Coopecaja contempla aspectos requeridos para el mantenimiento de la estrategia de continuidad, tales como: necesidades de negocio y tiempos de recuperación, recursos, costos y tiempos. En la sección de ayuda se explica cada una de las secciones que contiene el formulario y cómo contribuyen con la estrategia de continuidad.

c) Desarrollar e implementar una respuesta a la continuidad del negocio

El encargado de continuidad de negocio, en conjunto con la jefatura de TI, son responsables de desarrollar un plan de continuidad de negocio basado en la

estrategia que documente los procedimientos y la información lista para el uso en un incidente, para facilitar que la empresa continúe con sus actividades críticas.

En el documento PLA-006 BCP_Coopecaja, se describe los parámetros para activar el plan de continuidad de TI, procedimiento para actualizar y distribuir los procedimientos de recuperación y plan de continuidad, procedimientos de recuperación y pruebas de Continuidad.

En el documento Análisis de impacto TI se encuentra información de recursos de TI, tales como: servidores, bases de datos, aplicaciones, telecomunicaciones, almacenamiento. Además, contiene información de personal de TI y proveedores que intervienen en los procesos de recuperación.

d) Ejercitar, probar y revisar el BCP

El encargado de continuidad de negocio, en conjunto con la jefatura de TI, son responsables de elaborar un plan de pruebas para ejercitar los planes de recuperación respecto a resultados predeterminados, para permitir el desarrollo de soluciones innovadoras y para ayudar a verificar que el plan funcione, como se espera.

Para formular y ejecutar las pruebas se requiere utilizar el formulario establecido por la organización, toda prueba debe quedar debidamente documentada y los resultados deben analizarse, en caso de encontrar algún escenario de impacto no contemplado, se necesita ejecutar el flujo Actualización de plan para hacer las mejoras requeridas.

Con el formulario de pruebas se evalúa la eficacia del plan de continuidad de TI y procedimientos de recuperación de la infraestructura crítica, se contempla: efectividad del Plan de continuidad, ejecución de los roles y responsabilidades, habilidades del personal para atender la interrupción, impacto de la interrupción, proveedores e infraestructura tecnológica.

e) Revisar, mantener y mejorar el plan de continuidad

El encargado de continuidad de negocio, en conjunto con la jefatura de TI, son responsables de revisar periódicamente el plan de continuidad, con el fin de asegurar su continua idoneidad, adecuación y efectividad. Asimismo, gestionar los cambios en el plan de acuerdo con el proceso de control de cambios, para asegurar que el plan de continuidad se mantenga actualizado y refleje los requerimientos actuales del negocio.

Para la actualización del plan de continuidad se deben llevar a cabo los siguientes pasos:

Paso	Descripción
1) Inventario de procesos de negocio	Se identifican y documentan los procesos de negocio.
2) Inventario de activos de información	Realizar un inventario de activos tecnológicos que soportan información.
3) Análisis de impacto al negocio	Determinar el impacto de negocio en términos de disponibilidad de servicios, regulaciones, financiero e imagen.
4) Clasificación de la información	Clasificar la información según su criticidad para identificar qué es sensible y crítico para negocio.
5) Criticidad de procesos de negocio	Una vez realizado el análisis de impacto de negocio y una debida clasificación de datos, se requiere identificar cuáles procesos son críticos.
6) Dependencia de procesos de negocio en activos de información	Se debe identificar los activos tecnológicos de información que soportan los procesos críticos de negocio.
7) Activos críticos a incluir en análisis de riesgos	Identificar cuáles activos formarán parte del análisis de riesgos.

Paso	Descripción
8) Amenazas y vulnerabilidades de TI	Identificar amenazas y vulnerabilidades de TI.
9) Metas críticas y procesos que las soportan	Brindar información de metas críticas de TI y procesos que las soportan, con el fin de entender cuáles procesos son prioritarios en TI.
10) Amenazas y vulnerabilidades de seguridad de la información	Identificar las amenazas y vulnerabilidades de seguridad de información.
11) identificación de escenarios de riesgos de TI	Con las amenazas y las vulnerabilidades identificadas, más el catálogo de riesgos genéricos, se construye un catálogo de escenarios de riesgos.
12) Registro de incidentes de TI	Brindar información de incidentes de TI para calcular, según historia, posibles afectaciones en los escenarios de riesgos.
13) Evaluación de controles	Información para valoración de escenarios de riesgos.
14) Análisis de riesgos de TI	Se analiza cuáles riesgos aplican a TI.
15) Evaluación de riesgos de TI	Se evalúan los riesgos para determinar prioridad a atender en TI.
16) Estrategia de tratamiento de riesgos	Se proponen planes de acción para los riesgos que sobrepasen el apetito establecido.
17) Diseño de estrategia de recuperación	Compensatorio ante eventos de impacto de TI que afecten a negocio.
18) Implementación de estrategia de recuperación	Compensatorio ante eventos de impacto de TI que afecten al negocio.
19) Validación de estrategia de recuperación	Compensatorio ante eventos de impacto de TI que afecten al negocio.
20) Monitoreo y control de riesgos	Constante monitoreo para asegurar el ambiente de control.

Tabla 13. Pasos para actualizar plan de continuidad

Fuente: elaboración propia.

Para la identificación de riesgos debe considerarse como mínimo los escenarios que se presentan a continuación

Descripción de la amenaza	Factores de riesgo	Control para reducir impacto	Control para reducir probabilidad
Confidencialidad comprometida			
Acceso lógico no autorizado por externos sin credenciales legítimas	Intrusión, SQL *Injections*, Cyberespionaje, *Sniffing*, *Backdoors*	Cifrado, IDS, Auditorías, Gestión de Incidentes, Revisión de *Logs*	Clasificación de la Información, Validación en *input* de datos, *Hardening* de Servidores, Gestión de Parches, IPS, Política de Seguridad, WAF
Acceso de terceros no autorizados a información usando credenciales legítimas	Ing. Social, *Keyloggers*, *Phishing*, *Spoofing*, *Malware*, Robo credenciales, Reenvíos no autorizados	Cifrado, Auditorías, Gestión de incidentes, Revisión de *Logs*	Concientización, 2° factor de autenticación, DLP, Políticas, WAF, *Whitelists*, Antivirus, Filtros Correo, Verificación positiva, Ctrles de acceso
Fuga de información de origen interno usando credenciales legítimas	*Insider* (abuso, robo, código malicioso/*Backdoors*, *Screenshot*), Negligencia	Auditorías, Gestión de incidentes, Revisión de *Logs*, Cámaras de Seguridad	Capacitación, Concientización, DLP, Política, Revisión de Código, Ctrls de acceso físico/lógico.

Descripción de la amenaza	Factores de riesgo	Control para reducir impacto	Control para reducir probabilidad
			Selección c/verificación de antecendentes.
Acceso físico no autorizado a activos de TI (descarte, extravío, robo, traslado)	Forense post evento voluntario o forzado (con/sin intrusión física)	Cifrado, borrado remoto, geolocalización, MDMs, alertas por cambios de SIM, Cámaras de seguridad	Controles de acceso Físico, Sanitización de equipos, Concientización, Contraseña de acceso, Política BYOD
Pérdida de integridad (incluye Trazabilidad y No repudio)			
Errores de Desarrollo (ej.: fórmulas, cálculos, integración, interfases, parámetros, etc.)	Falta de Metodología de Desarrollo, Falencias de Pruebas, Complejidad IT	Pruebas UAT, Totales de Control	Metodología de Desarrollo de Software, Proceso de Gestión de Cambios, Automatización de interfases, *Testing*, Revisión de Código
Errores de usuarios en la operación de los sistemas y/o ejecución de los procesos	Falta de Manuales de Usuario, Operación manual de procesos	Procedimientos ante cancelaciones y reprocesos, Totales de control	Manuales de Usuario, Capacitación, *Scheduler* automatización de procesos,

Descripción de la amenaza	Factores de riesgo	Control para reducir impacto	Control para reducir probabilidad
			Controles preventivos de integridad
Corrupción de bases de datos que provocan fallas de integridad		Copias de respaldo, Procedimiento *Rollback*, Comprobación de integridad del motor de la DB	Reglas de integridad referencias preventivas, Modelo de Arquitectura de Datos
Alteración de información no autorizada por externos sin credenciales legítimas	Intrusión, SQL *Injections*, *Backdoors*, *Defacement* Web/Redes Sociales	Cifrado, IDS, Auditorías, Gestión de Incidentes, Revisión de *Logs*	Clasificación de la Información, Validación en *input* de datos, *Hardening* de Servidores, Gestión de Parches, IPS, Política de Seguridad, WAF
Alteración de información no autorizada por externos con credenciales legítimas	Ing. Social, *Keyloggers*, *Phishing*, *Spoofing*, *Malware*, Clientes con ID falsa	Cifrado, Auditorías, Gestión de incidentes, Revisión de *Logs*	Concientización, Autenticación fuerte, Política, WAF, *Whitelists*, Antivirus, Filtros de Correo, Verificación positiva

Descripción de la amenaza	Factores de riesgo	Control para reducir impacto	Control para reducir probabilidad
Alteración de información de origen interno usando credenciales legítimas	*Insider* (abuso, insertar código malicioso/*Backdoors*), Negligencia	Auditorías, Gestión de incidentes, Revisión de *Logs*	Capacitación, Concientización, Política de Seguridad, Revisión de Código. Selección de personal con verificación de antecendentes.
Trazabilidad no garantizada sobre las actividades y eventos relevantes		*Backups* de *logs* no regrabables, Seguridad Física sobre *Backups* de *Logs*, Controles de integridad sobre *Logs*	Definición de eventos a auditar, Política de supervisión de eventos de auditoría, Gestión de accesos lógicos sobre repositorio de *logs*
Repudio de transacciones/actividades legítimas		Firma Holográfica Digitalizada, Registros de auditoría	Verificación positiva, Doble factor de autenticación, Llave pública/privada, PGP

Descripción de la amenaza	Factores de riesgo	Control para reducir impacto	Control para reducir probabilidad
Ciberataques a usuarioso no usuarios, suplantando la marca de la Empresa	*Phishing*, Ing. Social, *Sniffing*, *Fake WiFis*, Falsos recursos Web de la Empresa	Monitoreo activo de suplantación de la marca	Concientización a Clientes y Público en general, Verificación de cuentas oficiales en Redes Sociales, Difusión de canales oficiales
Interrupción del Procesamiento/Degradación de *Performance*			
Ataque externo para provocar Interrupción del Procesamiento o Degradar *Performance*	Ataque DDoS, Borrado, *Ramsomware*, *Doxware*, Robo de cred., *Hijacking*	Monitoreo de tráfico de Red. Redireccionamiento (*Sinkhole*). Plan de Contingencia. Copias de respaldo. Gestión de Incidentes	Prevención *Black Hole* de Ataque DDoS, Gestión de Accesos, Antivirus, *Firewalls*, WAF, *Whitelists Applications*, Filtrado de correo malicioso
Capacidado *Performance* insuficiente de TI para brindar el *Business as Usual*	Procesamiento, ancho de banda, *storage*, desempeño de personal	Alertas automáticas ante umbrales de capacidad. Gestión de incidentes.	Proceso de Gestión de Capacidad con *Capacity Planning*
Fallas lógicas/físicas de activos de TI que afectan la Continuidad de TI	Obsolescencia, averías lógicas/físicas, incompatibilidad	Alertas automáticas ante Fallas. Gestión de incidentes. Plan de Contingencia.	Mantenimiento preventivo de activos de TI. Utilización de equipamiento de

Descripción de la amenaza	Factores de riesgo	Control para reducir impacto	Control para reducir probabilidad
		Copias de respaldo. Equipamiento alternativo	marcas reconocidas
Acciones internas (intencionales o errores) que afectan la Continuidad de TI)	*Insiders* (Sabotaje), Errores (configuración, cambios), Incompatibilidad	Gestión de incidentes. Plan de Contingencia. Copias de respaldo. Equipamiento alternativo	Proceso de Gestión de Cambios, *Testing*, Controles de Acceso, Gestión de Identidades. Selección RRHH con verificación de antecendentes.
Pérdida de programas fuentes o de correspondencia con ejecutables	Manipulación, Borrado accidental/intencional, mala gestión de versiones	Procedimientos *Rollback*. Copias de Respaldo.	Software de gestión de versiones. Proceso de Gestión de Cambios.
Interrupciones al procesamiento o afectación de *Performance* originadas por Proveedores	Tercerizaciones, Suministro de energía, TELCOs, SLAs mal gestionados	Auditorías a Proveedores. Monitoreo de SLAs. Reportes de control. Plan de Contingencias. Depósito de código fuente.	Casos de éxito previos. Contratos con penalidades. Acuerdos de Niveles de Servicio. Certificaciones. Plan de

Descripción de la amenaza	Factores de riesgo	Control para reducir impacto	Control para reducir probabilidad
			Contingencia del Proveedor.
Instalaciones de procesamiento no disponibles (fuego, desastres, conflictos, etc.)	Sabotaje, Huelgas, Conflictos sociales, Desastres naturales, Incendios	Instalaciones opcionales de procesamiento. Plan de Contingencias.	Ubicación del CPD primario en sitio seguro. Controles de acceso físico. Guardias de seguridad.

Tabla 14. Catálogo riesgos genérico

Fuente: https://www.udemy.com/gestion-agil-integrada-riesgos-de-tioperativoscontinuidad

Para actualizar el plan de continuidad se requiere contemplar los siguientes criterios:

Antes de un evento de impacto

Parámetros para actualizar plan de continuidad	Descripción
Periódicamente, al menos una vez al año	Según lo indicado en la política se debe revisar y si es requerido actualizar al menos una vez al año
Al iniciar un proyecto importante	En la metodología de proyectos se debe considerar cuáles proyectos impactan de manera importante a la organización, antes de iniciar estos proyectos se requiere revisar la idoneidad del plan de continuidad, si hay algo que no esté contemplado, debe documentarse una prueba y actualizar los planes
Una nueva regulación	Al ser notificados de una nueva regulación se debe revisar el plan para garantizar que esta no comprometa la continuidad
Cambios de personal clave	El personal clave forma parte de los planes de continuidad, al haber un cambio se debe valorar si afecta el plan, en caso de no afectar, se debe capacitar al nuevo recurso
Cambios en la estructura organizacional	Cuando hay un cambio en la estructura organizacional, principal en altos mandos, se debe revisar el plan y considerar estos cambios para la toma de decisiones
Luego de realizar pruebas de continuidad	Los resultados de las pruebas de continuidad indican cuán idóneo es el plan, en caso de encontrar brechas será necesario actualizar los planes
Identificación de nuevos riesgos	Al identificar un riesgo importante para la organización, se debe evaluar si tiene impacto en la continuidad, en caso de ser así, se requiere revisar que esté ese escenario incluido en los planes

Tabla 15. Criterios para actualizar plan antes de evento

Fuente: elaboración propia.

Después de un evento de impacto

Parámetros para actualizar plan de continuidad	Descripción
Incidentes de TI	Luego de un incidente de TI de alto impacto se debe revisar los planes de continuidad y recuperación, no solo incidentes que afecten servicios críticos; pues al compartir infraestructura tecnológica, lo ocurrido en un servicio no crítico, puede replicarse en servicios críticos
Incidentes operativos	
Desastre natural	Si hubo afectación en la operativa, se necesita documentar lo ocurrido y revisar los planes
Evento acción industrial	Luego de una huelga o manifestación, si hubo afectación en la operativa, es indispensable documentar lo ocurrido y revisar los planes
Eventos geopolíticos	Interferencia por parte del gobierno en asuntos relacionados al mercado, si hubo afectación en la operativa, es requerido documentar lo ocurrido y revisar los planes
Imagen de Cooperativa comprometida	Cualquier evento que afecte la imagen de la cooperativa es un disparador para la revisión y actualización del plan de continuidad y en especial para los planes de comunicación
Incumplimiento regulatorio	Ante cualquier incumplimiento con el regulador, se debe revisar los planes de continuidad

Tabla 16. Criterios para actualizar plan después de evento

Fuente: elaboración propia.

f) Proporcionar formación en el plan de continuidad

El encargado de continuidad de negocio, en conjunto con la jefatura de TI, son responsables de elaborar un plan de capacitación para todas las partes implicadas,

internas y externas, las cuales contemplen los procedimientos, sus roles, responsabilidades en caso de disrupción y concientización para toda la cooperativa. El plan de capacitación se registra en el formulario oficial qua la entidad ha establecido para este fin y debe quedar evidencia de la participación y entendimiento de cada capacitación brindada.

g) Ejecutar revisiones post-reanudación

El encargado de continuidad de negocio, en conjunto con la jefatura de TI, son responsables de evaluar la adecuación del plan de continuidad, después de reanudar en forma exitosa los procesos de negocio y servicios luego de una disrupción o la ejecución de pruebas, para esto se debe documentar lo ocurrido en el formulario de pruebas de continuidad y completar la sección de evaluación de efectividad.

Capítulo VI

6. Conclusiones y recomendaciones

6.1. Conclusiones

De acuerdo con las necesidades de Coopecaja, se elabora una propuesta para la implementación de un procedimiento; además, con el fin de elaborar el plan de continuidad de TI. Tal procedimiento abarca la gestión completa de continuidad de TI alineado al proceso de negocio.

Al comparar el actual flujograma del procedimiento de continuidad de TI de Coopecaja, con el propuesto basado en riesgos, se concluye que existen serias debilidades con respecto al marco de referencia COBIT 5; pues deja por fuera aspectos relevantes, tales como: los criterios para actualizar un plan de continuidad necesarios para una adecuada gestión de continuidad de negocio y TI.

Al analizar las distintas configuraciones, para la implementación de un procedimiento de continuidad de TI, se determina que cualquiera de ellas puede ser adoptada por Coopecaja; pues cuenta con las estructuras y los recursos necesarios.

Una vez considerado el resultado del estudio de factibilidad, se observa que resulta más viable efectuar un procedimiento de continuidad de TI integrado al procedimiento de continuidad de negocio.

Si se toma en cuenta la necesidad de Coopecaja, se elabora el diseño para el procedimiento de continuidad de TI, el cual se halla integrado al procedimiento de continuidad de negocio al utilizar COBIT 5 como marco de referencia.

6.2. Recomendaciones

Se recomienda a Coopecaja formalizar el procedimiento para gestionar la continuidad de TI como procedimiento único, tanto para TI como negocio; pues abarca toda la gestión de continuidad requerida desde el punto de vista operacional y tecnológico, de tal manera que involucra todas las áreas de control de la entidad.

Adoptar el flujograma propuesto que integra distintas áreas de control a la gestión de continuidad, tanto de negocio como de TI, siempre y cuando se haga uso del marco de referencia COBIT 5.

Agregar al estudio de factibilidad otras variables que aporten un mayor peso a la validez de los resultados para facilitar la toma de decisiones.

Implementar un procedimiento de continuidad de TI basado en el procedimiento de continuidad de negocio; pues es más viable y se aprovecha además recurso humano ya capacitado en el tema.

Analizar la necesidad de actualizar el diseño del procedimiento de continuidad para Coopecaja, con el fin de garantizar su vigencia en el tiempo.

Dar seguimiento al procedimiento para gestionar continuidad de TI aplicando las mejoras aplicables, basado en las necesidades de negocio y las nuevas tendencias tecnológicas.

Capítulo VII

7. Referencias bibliográficas

7.1. Anexos

7.1.1. Acuerdo SUGEF 14-17

A continuación, se presentan algunos artículos del acuerdo SUGEF 14-17, los cuales se relacionan en forma directa con el procedimiento propuesto. En la siguiente dirección se encuentra el acuerdo completo:

https://www.sugef.fi.cr/normativa/normativa_vigente/documentos/SUGEF%2014-17%20(v2_%2017abr2017).pdf

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1. Objeto

Este Reglamento establece los requerimientos mínimos para la gestión de la tecnología de información que deben acatar las entidades supervisadas y reguladas del sistema financiero costarricense.

Artículo 2. Alcance

Las disposiciones establecidas en este Reglamento son de aplicación para:
a) Supervisados por SUGEF:

1. Bancos comerciales del Estado;

2. Bancos creados por ley especial;

3. Bancos privados;

4. Empresas financieras no bancarias;

5. Organizaciones cooperativas de ahorro y crédito;

6. Mutuales de ahorro y préstamo y

7. Caja de ahorro y préstamos de la ANDE;

8. Cualquier otro intermediario financiero sujeto a supervisión por SUGEF.

b) Supervisados por SUGEVAL:

1. Puestos de Bolsa y Sociedades Administradoras de Fondos de Inversión;
2. Bolsas de Valores;
3. Sociedades de compensación y liquidación;
4. Proveedores de Precio;
5. Entidades que brindan servicios de custodia;
6. Centrales de Valores;
7. Sistemas de Anotación Electrónica en Cuenta, y
8. Sociedades titularizadoras y fiduciarias.

c) Supervisados por SUGESE:

1. Entidades Aseguradoras y sociedades Reaseguradoras;

2. Sucursales de entidades aseguradoras extranjeras.

d) Supervisados por SUPEN:

1. Operadoras de Pensiones Complementarias;

2. Fondos complementarios creados por leyes especiales o convenciones colectivas;

3. Regímenes públicos sustitutos del Régimen de Invalidez, Vejez y Muerte de la Caja Costarricense de Seguro Social.

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

Artículo 4. Lineamientos Generales

Los superintendentes deben emitir conjuntamente, mediante acuerdo de alcance general, los Lineamientos Generales para la aplicación de este Reglamento.

Artículo 5. Coordinación entre superintendencias

Las superintendencias deben coordinar los procesos regulados en este reglamento cuando la gestión de TI sea corporativa, cuando existan razones técnicas y de oportunidad que justifican dicho accionar.

El proceso de intercambio de información entre superintendencias se hará en los términos dispuestos en la Ley Orgánica del Banco Central de Costa Rica.

CAPÍTULO II

ORGANIZACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN Artículo 6. Unidad de TI

La unidad de TI es individual, cuando esta forma parte de la estructura organizativa de la entidad supervisada, o es un proveedor de TI domiciliado en el territorio nacional o en el extranjero, que brinda servicios en forma particular a una entidad supervisada.

La unidad de TI es corporativa, cuando el servicio lo realiza una unidad que forma parte de la estructura organizacional de una empresa integrante del mismo grupo o conglomerado financiero al que pertenece la entidad supervisada, o bien, es un proveedor de TI domiciliado en el territorio nacional o en el extranjero, que brinda servicios a varias empresas integrantes de un mismo grupo o conglomerado financiero.

La responsabilidad del gobierno, la gestión y de la seguridad de información en los servicios que estén tercerizados recaerá en las entidades supervisadas.

Artículo 7. Gobierno de TI

Las entidades supervisadas deben establecer una estructura de gobierno de TI con actividades y propósitos orientados a la generación de valor, a la consecución de

beneficios acorde a los niveles de riesgo aceptables y al uso óptimo de los recursos de las tecnologías de la información.

Las entidades supervisadas deben procurar que las necesidades de las partes interesadas sean evaluadas respecto a las metas corporativas establecidas; instituir una dirección del gobierno y de la gestión de TI priorizada; y asegurar que sea monitoreado el rendimiento y el cumplimiento respecto a la dirección y las metas acordadas.

Artículo 8. Gestión de TI

Las entidades supervisadas son responsables de planificar, implementar, controlar y mantener un marco de gestión de TI, conforme a los procesos descritos en los Lineamientos Generales y considerando los riesgos de TI establecidos en la gestión integral de riesgos aprobada por el Órgano de Dirección de cada una de las entidades.

El marco de gestión de TI debe formularse, considerando las particularidades de cada entidad supervisada, en atención a su naturaleza, complejidad, modelo de negocio, volumen de operaciones, criticidad de sus procesos y la dependencia tecnológica. Cualquier otra particularidad o aspecto puede ser considerada por la entidad supervisada o por la Superintendencia. Los procesos del marco de gestión de TI que no aplican para su modelo de negocio deberán ser justificados razonadamente mediante un estudio técnico.

Cuando la gestión de TI sea tipificada como corporativa, la entidad puede coordinar, aplicar y mantener un único marco de gestión de TI corporativo, el cual debe contemplar los riesgos de TI establecidos en la gestión integral de riesgos aprobada por el Órgano de Dirección de cada una de las entidades.

De acuerdo con las necesidades de supervisión, el riesgo identificado, o cuando se determine que el marco de gestión de TI no es acorde a las particularidades de la entidad supervisada, las Superintendencias pueden requerir, mediante resolución razonada, la inclusión de procesos en el marco de gestión de TI establecido por las entidades supervisada

CAPÍTULO III

DE LA SUPERVISIÓN Y AUDITORÍA EXTERNA DE TI

Sección I: Perfil tecnológico y tipo de gestión de TI

Artículo 9. Perfil tecnológico

Cada entidad supervisada debe elaborar y mantener actualizado su perfil tecnológico. El formulario de perfil tecnológico, la fecha de envío a la Superintendencia respectiva, forma y medio serán establecidos en los Lineamientos Generales.

Cuando la unidad de TI es corporativa debe remitirse un único perfil y coordinar que ese perfil tecnológico se ajuste al marco de gestión de TI. El perfil tecnológico debe identificar las particularidades de cada una de las entidades.

Artículo 10. Tipo de gestión de TI

Las entidades supervisadas pueden solicitar que su gestión de TI sea tipificada como corporativa cuando la unidad de TI provee servicios a dos o más entidades integrantes del grupo o conglomerado financiero. Los aspectos a considerar en la justificación de la solicitud y el plazo de resolución serán establecidos en los Lineamientos Generales.

Sección II: Auditoría Externa de TI

Artículo 11. Auditoría de las Tecnologías de Información

El supervisor solicitará a las entidades supervisadas la contratación de una auditoría externa de TI sobre el marco de gestión de TI y su aplicación, lo anterior según se determine en el alcance de la auditoría definido por el supervisor.

El intervalo entre una y otra solicitud no puede ser menor a dos años ni mayor a cuatro años, excepto, cuando el supervisor considere, con base en los resultados de la supervisión, la necesidad de adelantarla.

La auditoría externa de TI debe cumplir con el ciclo de auditoría de TI conforme a las Normas de Auditoría y Aseguramiento de Sistemas de Información emitidas por ISACA.

Sin embargo; los superintendentes pueden establecer mediante los Lineamientos Generales criterios complementarios para la ejecución del ciclo de la auditoría. El auditor externo de TI que lleve a cabo esta auditoría debe estar inscrito en el Registro de Auditores Elegibles que forma parte del Registro Nacional de Valores e Intermediarios, dispuesto en la Ley Reguladora del Mercado de Valores de conformidad con el reglamento correspondiente.

El contrato con el auditor externo de TI debe incluir una cláusula que obligue a éste a entregar al supervisor, copia de la información recopilada y procesada que sirve como respaldo de las labores de auditoría, así como los papeles de trabajo, en un plazo máximo de cinco días hábiles contados a partir de recibida la solicitud de entrega.

Si la unidad de TI es corporativa le corresponde a los Órganos de Dirección asegurarse que el alcance de la auditoría incluya todo aquello que corresponde a cada una de las entidades supervisadas, de tal forma, que los productos a entregar evalúen la gestión de TI a nivel de los procesos, pero también incluya aquellos riesgos particulares del negocio que desarrolla cada entidad supervisada. En caso de que se contrate una auditoría externa corporativa, los Órganos de Dirección de las entidades supervisadas deben dejar constancia de la aprobación del contrato de servicios, el cual debe cumplir con todos los requisitos establecidos en las regulaciones vigentes.

Artículo 12. Alcance y plazo de la auditoría

El supervisor debe comunicar a las entidades supervisadas el alcance y plazo de remisión de los productos entregables de la auditoría externa de TI. El alcance lo establece el supervisor mediante la definición de al menos los aspectos siguientes:

a) Procesos y objetivos de control a evaluar, con base en el marco de gestión de TI aplicables en el momento de la solicitud de la auditoría externa de TI.

b) Entidades supervisadas y áreas de negocio a considerar en cada proceso.

c) Servicios de TI suministrados por proveedores de TI.

d) El periodo de cobertura. El plazo otorgado para la remisión de los productos entregables será definido en los Lineamientos Generales.

Artículo 13. Productos entregables

Las entidades supervisadas deben remitir al supervisor los productos siguientes: **a)** El informe de auditoría externa de TI, según el formato establecido en los Lineamientos Generales.

b) La matriz de evaluación de los procesos auditados.

c) Copia del acta del Órgano de Dirección de la entidad, en el cual aprueba el informe de la auditoría externa de TI.

Artículo 14. Presentación de resultados de la auditoría externa de TI

Las entidades supervisadas deben convocar, previa coordinación con el supervisor, una reunión de salida para la presentación de los resultados de la auditoría externa de TI. El plazo otorgado para convocar la presentación de resultados de la auditoría externa será definido en los Lineamientos Generales.

El auditor externo de TI debe presentar los resultados de la auditoría externa de TI.

Los contenidos mínimos de la presentación se establecen en los Lineamientos Generales.

En la presentación de resultados de la auditoría externa deben participar al menos las personas siguientes:

a) Los colaboradores que estimen las superintendencias.

b) El Gerente General de las entidades supervisadas.

c) El responsable de la unidad de TI, o similar, de las entidades supervisadas.

d) El auditor interno, cuando exista, de cada una de las entidades supervisadas.

e) El presidente del comité de vigilancia, cuando exista, de cada una de las entidades supervisadas.

Sección III: Reporte supervisor y plan de acción

Artículo 15. Reporte de Supervisión

De los resultados de las auditorías externas de TI de las entidades supervisadas, las superintendencias elaborarán un reporte de supervisión. Este reporte debe elaborarse y actualizarse con los productos entregables indicados en los incisos a) y b) del Artículo 13. En este reporte se determinan los hallazgos y riesgos que deben ser atendidos por la entidad supervisada, así como la estrategia y actividades de seguimiento que se realizarán.

Asimismo, los resultados de cualquier actividad de supervisión realizada directamente por las superintendencias, se incorporarán en el proceso de supervisión.

Cuando haya una auditoría externa de TI y el o los supervisores se aparten de la opinión emitida por el auditor externo de TI debe incluirse la debida justificación. El plazo otorgado para remitir a la entidad supervisada el reporte de supervisión sobre los resultados de la auditoría externa, será definido en los Lineamientos Generales.

El supervisor puede declarar inadmisibles los productos entregables indicados en los incisos a) y b) del Artículo 13 cuando incumplan las disposiciones establecidas en este Reglamento o sus Lineamientos Generales. En este caso, la entidad supervisada debe remitir los productos entregables corregidos y realizar la reunión de salida en el plazo indicado en la nota de remisión del reporte de supervisión.

Cuando los productos de la auditoría sean admisibles y se incorporen al reporte de supervisión, pero se determinen hallazgos y riesgos, el supervisor debe requerir en la nota de remisión un plan de acción para la gestión de éstos.

Artículo 16. Plan de Acción

La entidad supervisada debe presentar el plan de acción con el formato y plazo establecidos en los Lineamientos Generales.

El plan de acción debe ser aprobado por el Órgano de Dirección de la entidad supervisada y debe estar firmado por su representante legal o gerente general. Las actividades incluidas en el plan de acción deben solventar los hallazgos o mitigar los riesgos indicados en el reporte de supervisión.

Los supervisores pueden hacer observaciones al plan de acción, sugerir mejoras o advertir sobre riesgos significativos. Si a criterio de los supervisores las actividades incluidas en el plan de acción no atienden adecuadamente los hallazgos y riesgos, el plazo solicitado es mayor al razonablemente necesario o la frecuencia de presentación de los informes de avances no permite un adecuado seguimiento al plan de acción, los supervisores deben solicitar las modificaciones pertinentes a la entidad supervisada.

La entidad supervisada debe ejecutar las modificaciones solicitadas por el supervisor y comunicar a éste las variaciones en el plazo requerido. El plan de acción, así modificado, debe ser comunicado al Órgano de Dirección de la entidad supervisada, y debe estar firmado por su representante legal o gerente general. Las Superintendencias pueden coordinar el reporte y proceso de supervisión. La aprobación de los planes de acción por parte del supervisor procederá en aquellos casos en que así lo defina su regulación específica.

Sección IV: Prórrogas y calificación de riesgos de TI

Artículo 17. Prórrogas

La entidad supervisada puede presentar una solicitud de prórroga ante el supervisor, para la remisión de los productos entregables de la auditoría externa de TI o para el plan de acción. El plazo otorgado para presentar una solicitud de prórroga ante el supervisor, a fin de que la misma pueda ser conocida y resuelta por la respectiva superintendencia, será definido en los Lineamientos Generales. La solicitud debe estar firmada por el representante legal o gerente general de la entidad solicitante y debe indicar la fecha propuesta de remisión de los productos de auditoría externa de TI o acompañarse de un nuevo plan de acción aprobado por su Órgano de Dirección según corresponda. Además, debe contener los motivos y las pruebas, si fuere del caso, que imposibilitan a la entidad para cumplir con el plazo original, y deberá demostrar, que los motivos para su petición se basan en caso fortuito o fuerza mayor, u otras causas fuera de su control.

El superintendente del respectivo órgano supervisor conocerá y valorará los fundamentos presentados y, en los casos que corresponda, otorgará prórroga por escrito, mediante resolución motivada, indicando el plazo adicional concedido. Cuando la unidad de TI es corporativa, las superintendencias coordinarán la concesión de la citada prórroga.

Artículo 18. Calificación de riesgos de TI

El superintendente, cuando corresponda a su modelo de supervisión definido reglamentariamente y aprobado por el CONASSIF, debe emitir la calificación sobre el riesgo de TI de la entidad supervisada. La metodología para determinar dicha calificación se establece en las regulaciones particulares de cada Superintendencia.

Sección V: Bases de datos

Artículo 19. Bases de datos

Las bases de datos actualizadas y las aplicaciones vigentes que procesan o dan acceso a estas bases deben estar accesibles al ente supervisor correspondiente, sin ningún tipo de restricción o condición.

Con este fin, cuando la unidad de TI no forme parte de una entidad supervisada o cuando existan proveedores de TI, la entidad debe establecer un contrato con esa unidad de TI y con cada uno de los proveedores de TI. Las condiciones que deben observarse en los instrumentos legales en que se pacten los servicios de TI, tendientes a cumplir el objetivo señalado en esta norma, serán definidas en los Lineamientos Generales.

Las bases de datos actualizadas, así como, las aplicaciones vigentes que procesan o dan acceso a estas bases, pueden mantenerse en servicios de computación en la nube, siempre y cuando se cumplan con los requisitos legales, de seguridad y de acceso del supervisor, de acuerdo con la normativa aplicable por cada superintendencia. La respectiva superintendencia puede requerir un modelo de gestión de infraestructura tecnológica diferente al de los servicios de computación en la nube, cuando en estos: la entidad no cumpla los requisitos legales y de seguridad; no se brinde acceso al supervisor; la información que la entidad desea mantener sea sensible o crítica para la continuidad del negocio; la computación en la nube represente un riesgo para el sistema financiero; o cuando afecte los intereses de los clientes.

7.1.2. Procedimiento de continuidad de TI Actual

3.1.1 Paso 1

Jefe de TI Solicita la información del Análisis de Impacto del Negocio (BIA) al área del negocio, y deberá revisar al menos la siguiente información:

- Listado de los procesos críticos del negocio.
- Los tiempos de recuperación objetivo (RPO) de los procesos críticos del negocio
- Los puntos de recuperación objetivo (RPO) de los procesos críticos del negocio.
- Los recursos necesarios para su recuperación.
- La priorización de recuperación de los procesos críticos del negocio.
- El impacto financiero y cualitativo por proceso crítico.
- Períodos críticos de operación.

3.1.2 Paso 2

Jefe de TI En caso de que no se cuente con un BIA actualizado se le informará al negocio, y se le solicitará los requerimientos de la información faltante.

3.1.3 Paso 3

Jefe de TI Prepara la sesión con los expertos de recuperación de TI para definir la plataforma tecnológica que soporta los procesos de críticos del negocio para definir:

- Aplicaciones que soportan los procesos críticos.
- Componentes tecnológicos que soportan las aplicaciones.
- Personal crítico.
- Los recursos vitales tales como (instaladores, procedimientos, otros).
- Proveedores críticos.

3.1.4 Paso 4

Jefe de TI Recopilar y analizar la información recolectada por el personal experto de recuperación y se elaborará un informe que al menos contendrá:

- Objetivos.
- Alcance.
- Enfoque metodológico.
- Hallazgos.
- Recomendaciones.

Y este será aprobado por el Comité de TI.

3.1.5 Paso 5

Jefe de TI Solicita la inclusión o actualización de la plataforma crítica en la CMDB a la unidad de soporte técnico.

3.1.6 Paso 6

Jefe de TI Una vez aprobado el Análisis de Impacto Tecnológico (TIA), este deberá ser distribuido al personal requerido y almacenado en el repositorio de información primario y contingente.

3.1.7 Paso 7

Jefe de TI Prepara las sesiones con los funcionarios de TI para identificar los riesgos del área de continuidad de TI.

1. Evaluación de riesgos de continuidad de TI

3.2.1	**Paso 8**
Funcionarios de TI	Evaluarán los riesgos relacionados al proceso de continuidad de TI para definir aquellas posibles situaciones que puedan afectar la operación de la infraestructura tecnológica crítica, consecuentemente deberán proponer controles que ayuden a mitigar los riesgos identificados.
3.2.2	**Paso 9**
Jefe de TI	Una vez ejecutada la evaluación de riesgos e identificados los controles, se deberá generar un informe al Comité de TI indicando las actividades realizadas que realizaron, hallazgos, conclusiones y recomendaciones.
3.2.3	**Paso 10**
Comité de TI	En base al informe de la evaluación de riesgos de continuidad de TI, el Comité de TI seleccionará los controles que se deberán implementar para mitigar el riesgo.
3.2.4	**Paso 11**
Jefe de TI	Ejecutará y dará seguimiento a la implementación de los controles de continuidad de TI aprobados, además estará a cargo de actualizar la información de los repositorios y distribuir la evaluación de riesgos de continuidad a los interesados.

2. Análisis de estrategias de continuidad de TI

3.3.1	**Paso 12**
Jefe de TI	Una vez evaluados los riesgos de continuidad de TI se deberá definir las estrategias de continuidad de TI, por lo cual el Jefe de TI verificará que la información del análisis de impacto tecnológico y la identificación de los riesgos de continuidad se encuentren actualizadas, de no ser así deberá coordinar las actividades con su equipo de TI para actualizar la información del TIA y análisis de riesgos.
3.3.2	**Paso 13**
Jefe de TI	Calendarizará las sesiones con el personal experto de recuperación de la plataforma tecnológica crítica para definir las estrategias de continuidad de TI.
3.3.3	**Paso 14**
Expertos de recuperación y Jefe de TI	Ejecutarán las sesiones para definir las estrategias de continuidad de TI y deberán considerar: • Los riesgos clasificados con una probabilidad e impacto alto y medio. • Al menos todos los RTA del área de TI que no cumplen con el RTO solicitado por el negocio.

- Al menos los respaldos cuya frecuencia no cumpla con el RPO solicitado por el negocio.

Para poder definir:

- Las estrategias de continuidad actuales.
- Las estrategias de continuidad propuestas.
- Los costos y detalles de implementación de las estrategias propuestas.
- Ventajas y desventajas de las estrategias de continuidad propuestas.

3.3.4 **Paso 15**

Jefe de TI Enviará un informe con las estrategias de continuidad propuesta al Comité de TI

3.3.5 **Paso 16**

Comité de TI Valorará las estrategias de continuidad propuestas y seleccionará aquellas que se implementarán.

3.3.6 **Paso 17**

Jefe de TI Ejecutará y dará seguimiento a las estrategias de continuidad de TI aprobadas por el comité de TI, e informará al comité de TI el avance de la implementación.

3.3.7 **Paso 18**

Jefe de TI Distribuirá la información de las estrategias de continuidad de TI y actualizará la información de los repositorios donde se encuentra.

3. Plan de continuidad de TI y protocolos de recuperación

3.4.1 **Paso 19**

Jefe de TI Actualizará el plan de continuidad de TI ante cambios significativos en el negocio o la plataforma tecnológica o al menos una vez al año, y este deberá considerar:

- Roles y responsabilidades del personal partícipe del proceso de continuidad de TI.
- Detalle de la activación, recuperación y retorno a la operación normal del área de TI.
- Clasificación de incidentes.
- Canales de notificación de incidentes.
- El TIA, análisis de riesgos y estrategias de continuidad actualizados.
- Información crítica actualizada.
- Información de equipos actualizados.
- Contactos claves actualizados.
- Prioridad de recuperación y protocolos de recuperación actualizados.
- Objetivo, alcance y propósito del Plan de continuidad de TI.

3.4.2 **Paso 20**

Jefe de TI	Definirá la estrategia para actualizar el plan de continuidad de TI y solicitará la información actualizada de los protocolos de recuperación.
3.4.3	**Paso 21**
Expertos de recuperación	Actualizarán la información de los protocolos de recuperación de la plataforma crítica de TI y enviarán la información actualizada al encargado de continuidad de TI.
3.4.4	**Paso 22**
Jefe de TI	Elaborará un informe con los resultados obtenidos en el proceso de documentación del Plan de continuidad de TI y protocolos de recuperación, para exponer los principales hallazgos, conclusiones y recomendaciones al Comité de TI.
3.4.5	**Paso 23**
Comité de TI	Aprobará el plan de continuidad y planes de recuperación, y devolverá los planes de continuidad al Jefe de TI, en caso de que se requiera aplicar ajustes.
3.4.6	**Paso 24**
Jefe de TI	Actualizará la información de los planes de continuidad de TI en los repositorios de información y distribuirá estos documentos al personal de TI partícipe del proceso.

4. Capacitaciones

3.5.1	**Paso 25**
Jefe de TI	Evaluará la necesidad de desarrollar un plan de capacitaciones y deberá ser actualizado en los siguientes casos: • Los expertos de recuperación no atendieron de forma satisfactoria un incidente que afecte la continuidad del servicio de TI. • Al realizar las pruebas de continuidad los funcionarios expertos de recuperación no presentaron las habilidades técnicas necesarias para atender la prueba. • Ingreso de nuevo personal. • Retroalimentación en las capacitaciones.
3.5.2	**Paso 26**
Jefe de TI	Desarrollará un plan de capacitaciones, además deberá coordinar e informar al personal que se le impartirá la capacitación y los recursos logísticos necesarios para poder ejecutar el plan de capacitación.
3.5.3	**Paso 27**
Jefe de TI	Ejecutará la capacitación al personal de TI identificado en el plan de capacitaciones con el objetivo de cubrir las deficiencias encontradas en el desarrollo del proceso de continuidad de TI.
3.5.4	**Paso 28**
Jefe de TI	Evaluará los talleres de capacitación y en base a la retroalimentación obtenida por parte de los participantes, ajustará el plan de continuidad de TI con las mejoras brindadas por el personal capacitado.
3.5.5	**Paso 29**
Jefe de TI	Actualizará la información del plan de capacitación de los repositorios y distribuirá la documentación o material de la capacitación al personal interesado.

5. Pruebas de continuidad de TI

3.6.1	**Paso 30**
Jefe de TI	Al menos una vez al año programará un plan de pruebas de continuidad en caso de que se presente los siguientes casos: • Se genere nueva información. • Los planes de los sistemas críticos hayan sido modificados. • Resultados de pruebas anteriores. • Ingreso de nuevo funcionarios identificados como críticos.
3.6.2	**Paso 31**
Jefe de TI	Elaborará un plan de pruebas para evaluar los sistemas críticos del negocio, y estos contendrán la fecha de ejecución, el personal que participará y todos los elementos logísticos necesarios para llevar a cabo la ejecución de la prueba, y este plan de pruebas será aprobado.
3.6.3	**Paso 32**
Comité de TI	Enviará al encargado de continuidad las correcciones del plan de pruebas y será encargado de aprobarlo.
3.6.4	**Paso 33**
Jefe de TI	Informará al personal que participará en las pruebas de continuidad aprobadas y coordinará la obtención de los recursos necesarios para llevar ejecutar el plan.
3.6.5	**Paso 34**
Jefe de TI **Expertos de recuperación**	Ejecutarán las pruebas de continuidad programadas documentarán todos los hallazgos, conclusiones y recomendaciones durante la fase de ejecución.
3.6.6	**Paso 35**
Jefe de TI	Evaluará la prueba de continuidad ejecutada para verificar si se cumplieron los objetivos establecidos y su efectividad, puntos tales (factores que interrumpieron la ejecución de la prueba, factores de éxito, otros).
3.6.7	**Paso 36**
Jefe de TI	Establecerá un plan de acción en base a los hallazgos recolectados con el fin de mejorar el plan de continuidad de TI.
3.6.8	**Paso 37**
Jefe de TI	Elaborará un informe con los resultados obtenidos en la ejecución de las pruebas de continuidad realizadas y se lo presentará al Comité de TI.
3.6.9	**Paso 38**
Jefe de TI	Actualizará la información en todos los repositorios y distribuirá la información del plan de pruebas al personal interesado.

6. Mantenimiento del proceso de continuidad de TI

3.7.1	**Paso 39**
Jefe de TI	Analizará al menos una vez al año la información que soporta el procedimiento de continuidad de TI y documentará las necesidades de cambio identificadas.
3.7.2	**Paso 40**

Jefe de TI	Elaborará y presentará un informe al Comité de TI con la información relevante identificada en el proceso de mantenimiento al plan.
3.7.3	**Paso 41**
Comité de TI	Aprobará los cambios identificados en el proceso de continuidad de TI.
3.7.4	**Paso 42**
Jefe de TI	Distribuirá la información del proceso de continuidad de TI a las partes interesadas y actualizará la información con la nueva versión en los repositorios.

7.2. Apéndices

7.2.1. Lista de chequeo

Practica de Gestión	Actividad	Cumple	No Cumple
DSS04.01 Definir la política de continuidad de negocio, objetivos y alcance.	1. Identificar procesos de negocio internos que son críticas para las operaciones de la empresa o necesarias para cumplir con las obligaciones legales y/o contractuales.		
	1.1. Identificar procesos de negocio subcontratados que son críticas para las operaciones de la empresa o necesarias para cumplir con las obligaciones legales y/o contractuales.		
	1.2. Identificar actividades de servicio que son críticas para las operaciones de la empresa o necesarias para cumplir con las obligaciones legales y/o contractuales.		
	2. Identificar las partes interesadas clave para definir y acordar la política de continuidad y su alcance.		
	2.1. Identificar los roles y responsabilidades para definir y acordar la política de continuidad y su alcance.		

Practica de Gestión	Actividad	Cumple	No Cumple
	3. Definir y documentar los objetivos mínimos acordados de la política de continuidad del negocio e imbricar la planificación de continuidad en la cultura empresarial.		
	3.1. Definir y documentar el alcance mínimo acordados de la política de continuidad del negocio e imbricar la planificación de continuidad en la cultura empresarial.		
	4. Identificar procesos de soporte al negocio esenciales y servicios TI relacionados.		
DSS04.02 Mantener una estrategia de continuidad.	1. Identificar escenarios potenciales probables que puedan dar pie a eventos que puedan causar incidentes disruptivos importantes.		
	2. Realizar un análisis de impacto en el negocio para evaluar el impacto en tiempo de una disrupción en funciones críticas del negocio y el efecto que tendría en ellas.		
	3. Establecer el tiempo mínimo necesario para recuperar un proceso de negocio y su soporte de TI, basándose en una duración aceptable de interrupción del negocio y la interrupción máxima tolerable.		
	4. Analizar la probabilidad de amenazas que puedan causar pérdidas de continuidad de negocio e identificar medidas que puedan reducir la probabilidad y el impacto, mejorando la prevención e incrementando la resiliencia.		
	5. Analizar los requerimientos de continuidad para identificar las posibles estrategias de negocio y opciones técnicas.		

Practica de Gestión	Actividad	Cumple	No Cumple
	6. Determinar las condiciones de decisiones clave que puedan causar la invocación de los planes de continuidad.		
	6. Determinar los responsables de decisiones clave que puedan causar la invocación de los planes de continuidad.		
	7. Identificar los requerimientos de recursos y costes para cada opción técnica estratégica y realizar recomendaciones estratégicas.		
	8. Obtener la aprobación de los ejecutivos de negocio para las opciones estratégicas seleccionadas.		
DSS04.03 Desarrollar e implementar una respuesta a la continuidad del negocio.	1. Definir las acciones y comunicaciones de respuesta a incidentes que deben ser realizadas en un evento de disrupción.		
	1.1. Definir los roles y responsabilidades relacionados, incluyendo la responsabilidad para la política y la implementación que deben ser realizadas en un evento de disrupción.		
	2. Desarrollar planes de continuidad de negocio operativos que contengan los procedimientos que deben ser seguidos para permitir continuar operando los procesos críticos de negocio y/o planes temporales de proceso, incluyendo enlaces a los planes de proveedores de servicio externalizados.		
	2.1. Mantener planes de continuidad de negocio operativos que contengan los procedimientos que deben ser seguidos para permitir continuar operando los procesos críticos de negocio y/o planes temporales de proceso, incluyendo enlaces		

Practica de Gestión	Actividad	Cumple	No Cumple
	a los planes de proveedores de servicio externalizados.		
	3. Asegurar que los proveedores clave tengan implantados planes de continuidad efectivos. Obtener evidencias auditadas si es necesario.		
	3.1. Asegurar que los socios externos clave tengan implantados planes de continuidad efectivos. Obtener evidencias auditadas si es necesario.		
	4. Definir las condiciones de recuperación que permitan la reanudación de los procesos de negocio, incluyendo la actualización y conciliación de las bases de datos para preservar la integridad de la información.		
	4.1. Definir los procedimientos de recuperación que permitan la reanudación de los procesos de negocio, incluyendo la actualización y conciliación de las bases de datos para preservar la integridad de la información.		
	5. Definir y documentar los recursos necesarios para soportar los procedimientos de continuidad, considerando personas, instalaciones e infraestructura de TI.		
	5.1. Definir y documentar los recursos necesarios para soportar los procedimientos de recuperación, considerando personas, instalaciones e infraestructura de TI.		
	6. Definir y documentar los requerimientos de información de respaldo para soportar los planes, incluyendo planes y documentos en papel, así como ficheros de datos y considerar las necesidades de seguridad y almacenamiento en otra ubicación.		

Practica de Gestión	Actividad	Cumple	No Cumple
	7. Determinar las habilidades necesarias para los individuos implicados en la ejecución de los planes y procedimientos.		
	8. Distribuir los planes y la documentación de soporte de modo seguro a las partes interesadas y apropiadamente autorizadas y asegurar que estén accesibles en escenarios de desastre.		
	8.1. Asegurar que los planes y la documentación estén accesibles en escenarios de desastre.		
DSS04.04 Ejercitar, probar y revisar el BCP.	1. Definir los objetivos para ejercitar y probar los sistemas del plan (de negocio) para verificar la completitud del plan de continuidad de negocio (BCP) para enfrentarse a los riesgos de negocio.		
	1.1. Definir los objetivos para ejercitar y probar los sistemas del plan (técnicos) para verificar la completitud del plan de continuidad de negocio (BCP) para enfrentarse a los riesgos de negocio.		
	1.2. Definir los objetivos para ejercitar y probar los sistemas del plan (logísticos) para verificar la completitud del plan de continuidad de negocio (BCP) para enfrentarse a los riesgos de negocio.		
	1.3. Definir los objetivos para ejercitar y probar los sistemas del plan (administrativos) para verificar la completitud del plan de continuidad de negocio (BCP) para enfrentarse a los riesgos de negocio.		
	1.4. Definir los objetivos para ejercitar y probar los sistemas del plan (procedimentales) para verificar la completitud del plan de continuidad de negocio (BCP) para enfrentarse a los riesgos de negocio.		
	1.5. Definir los objetivos para ejercitar y probar los sistemas del plan (operacionales) para verificar la		

Practica de Gestión	Actividad	Cumple	No Cumple
	completitud del plan de continuidad de negocio (BCP) para enfrentarse a los riesgos de negocio.		
	2. Definir y acordar ejercicios que sean razonables con las partes interesadas, validar los procedimientos de continuidad, e incluir roles y responsabilidades y acuerdos de retención de datos que ocasionen la mínima disrupción en los procesos de negocio.		
	3. Asignar roles y responsabilidades para realizar ejercicios y pruebas del plan de continuidad.		
	4. Planificar ejercicios y actividades de prueba tal como esté definido en el plan de continuidad.		
	5. Realizar un análisis y revisión post-ejercicio para considerar el logro.		
	6. Desarrollar recomendaciones para mejorar el plan de continuidad actual en base a los resultados de la revisión.		
DSS04.05 Revisar, mantener y mejorar el plan de continuidad.	1. Revisar el plan y la capacidad de continuidad de forma regular frente a las asunciones hechas y los objetivos de negocio actuales, tanto estratégicos como operativos.		
	2. Considerar si es necesario una revisión del análisis de impacto en el negocio, dependiendo en la naturaleza de los cambios.		
	3. Recomendar y comunicar los cambios en la política, planes, procedimientos, infraestructura, roles y responsabilidades para la aprobación de la dirección y su realización mediante el proceso de gestión de cambios.		

Practica de Gestión	Actividad	Cumple	No Cumple
	4. Revisar el plan de continuidad regularmente para considerar el impacto de cambios nuevos o mayores en: organización de la empresa.		
	4.1. Revisar el plan de continuidad regularmente para considerar el impacto de cambios nuevos o mayores en: procesos de negocio.		
	4.2. Revisar el plan de continuidad regularmente para considerar el impacto de cambios nuevos o mayores en: acuerdos de externalización.		
	4.3. Revisar el plan de continuidad regularmente para considerar el impacto de cambios nuevos o mayores en: tecnologías.		
	4.4. Revisar el plan de continuidad regularmente para considerar el impacto de cambios nuevos o mayores en: infraestructura.		
	4.5. Revisar el plan de continuidad regularmente para considerar el impacto de cambios nuevos o mayores en: sistemas operativos.		
	4.6. Revisar el plan de continuidad regularmente para considerar el impacto de cambios nuevos o mayores en: sistemas de aplicaciones.		
DSS04.06 Proporcionar formación en el plan de continuidad.	1. Definir y mantener los planes y requerimientos de formación para quienes realicen de manera continuada planificación de la continuidad, análisis de impacto, evaluaciones de riesgos, comunicación con los medios y respuesta a incidentes. Asegurar que los planes de formación consideren la frecuencia de formación y los mecanismos de entrega de la formación.		

Practica de Gestión	Actividad	Cumple	No Cumple
	2. Desarrollar competencias basadas en formación práctica que incluyan la participación en ejercicios y pruebas.		
	3. Supervisar habilidades y competencias basándose en los resultados de los ejercicios y las pruebas.		
DSS04.07 Gestionar acuerdos de respaldo.	1. Hacer copias de seguridad de sistemas, aplicaciones, datos y documentación de acuerdo a una planificación definida, considerando: • Frecuencia (mensual, semanal, diaria, etc.) • Modo de copias de seguridad (por ejemplo, discos espejo para copias de seguridad en tiempo real frente a DVD-ROM para retenciones de larga duración) • Tipo de copias de seguridad (por ejemplo, completa frente a incremental) • Tipo se soporte • Copias de seguridad automatizadas en línea • Tipos de datos (por ejemplo, voz, óptica) • Creación de registros • Datos de cálculos críticos de usuario final (por ejemplo, hojas de cálculo) • Localización física y lógica de las fuentes de los datos • Seguridad y derechos de acceso • Cifrado		
	2. Asegurar que los sistemas, aplicaciones, datos y documentación mantenidos o procesados por terceras partes están adecuadamente respaldados o asegurados de otra forma. Considerar el hecho de requerir el retorno de las copias de seguridad de		

Practica de Gestión	Actividad	Cumple	No Cumple
	terceras partes. Considerar acuerdos de depósito (*escrow*).		
	3. Definir los requerimientos del almacenamiento de las copias de seguridad, dentro y fuera de la propia ubicación, que satisfagan los requerimientos del negocio. Considerar la accesibilidad requerida a las copias de seguridad.		
	4. Extender la concienciación y la formación en Planes de Continuidad de Negocio (BCP).		
	5. Probar y mantener legibles las copias de seguridad y las archivadas periódicamente.		
DSS04.08 Ejectuar revisiones post-reanudación.	1. Evaluar la observancia del Plan de Continuidad de Negocio (BCP) documentado.		
	2. Determinar la efectividad del plan, capacidades de continuidad, roles y responsabilidades, habilidades y competencias, resiliencia a incidentes, infraestructura técnica y estructuras organizativas y relaciones.		
	3. Identificar debilidades u omisiones en el plan y las capacidades y hacer recomendaciones para la mejora.		
	4. Obtener la aprobación de la dirección para los cambios en el plan y aplicarlos mediante el proceso de control de cambios de la empresa.		

Tabla 17: Lista de chequeo

Fuente: Elaboración propia