Universidad Austral de Chile
Escuela de Ingeniería Civil Industrial
Sede Puerto Montt

PROFESOR PATROCINANTE: OSCAR GUEVARA ARIAS
ESCUELA DE INGENIERÍA CIVIL INDUSTRIAL

"Modelo Integral para la implementación de un Plan de Continuidad de Negocio en Chile"

Trabajo de Titulación
para optar
al título de **Ingeniero Civil Industrial**

VÍCTOR ALEJANDRO SÁEZ VARGAS

PUERTO MONTT – CHILE

RESUMEN

La progresiva competencia entre las organizaciones empresariales, las demandas cada vez más exigentes de clientes y las partes interesadas (stakeholders*)*, o las obligaciones regulatorias cada vez más restrictivas, son factores que hoy en día comprometen a las empresas a demostrar la firmeza que deben tener las actividades del negocio, para permanecer activas ante cualquier contingencia grave. Son múltiples las organizaciones que, independientemente de su tamaño, fracasan o incluso desaparecen por la falta de procesos, mecanismos y técnicas que mitiguen los riesgos a los que están expuestos y garanticen una alta disponibilidad en las operaciones de su negocio. Es por esto que se hace imperante para las empresas la realización de un Plan de Continuidad de Negocio (Business Continuity Plan, BCP siglas en inglés), el cual consiste en un proceso de dirección que identifica los impactos potenciales que amenazan a la organización y proporciona el marco adecuado para desarrollar la capacidad de dar una respuesta efectiva, que permita proteger los intereses, imagen y valor de las actividades realizadas por la misma.

Uno de los principales inconvenientes o barreras a las que se enfrenta una organización cuando decide abordar cualquier tipo de iniciativa relacionada con la continuidad de negocio es la falta de conocimiento, la falta de instrucciones claras y concisas que detallen por dónde empezar y qué aspectos se deben tener en cuenta para garantizar el éxito. Es por esto, que este trabajo de grado tiene por objetivo crear una propuesta metodológica para la implementación de un Plan de Continuad de Negocio adaptada a la cultura organizacional de las empresas chilenas y la cual pretende satisfacer los siguientes interrogantes:

- ¿Cómo y cuáles son los pasos a seguir para realizar la implementación de un BCP en Chile?
- ¿Cómo mantener y actualizar el BCP?

Para poder lograrlo, será necesario contar con el apoyo de un estudio detallado sobre Administración y la influencia de la cultura en los proyectos empresariales, además de estudiar las metodologías utilizadas a nivel mundial en la actualidad y los estándares referentes a continuidad de Negocio, identificando los puntos más fuertes de cada uno y reforzando o modificando algunos de estos para obtener una mejor adaptabilidad.

Además este trabajo de grado, pretende sembrar la inquietud de que hay algo pendiente por hacer y que puede ser absolutamente vital para la organización; más aún, que puede hacer que su carencia haga peligrar la supervivencia de la misma, para que se comience cuanto antes a elaborar el Plan de Continuidad de Negocio, ya que son muchas las tareas que se deben realizar.

Las principales partes que comprende el trabajo de grado son los siguientes:

En el capítulo 2.1: se contextualiza y se estudia el significado y la importancia de los Planes de continuidad de negocio, además de analizar la situación que vive chile con respecto a este tema.

En el capítulo 2.2: se presenta un análisis de la cultura organizacional, con las características que la integran y la manera en que esta influye en los proyectos empresariales. El capítulo también abarca los temas que deben ser entendidos para llevar a cabo una efectiva implementación del Plan de continuidad de negocio.

En los capítulos 2.3 y 2.4: se analizan los estándares, metodologías y guías para implementar el BCP más utilizadas a nivel mundial, cada uno de los documentos son analizados y comparados, con la finalidad de identificar sus fortalezas que podrían formar parte del modelo que propone el presente trabajo de grado.

En el capítulo 3: se explican los procedimientos que se aplicarán para alcanzar los objetivos del trabajo de grado, es decir corresponde al planteamiento de una serie de actividades sucesivas y organizadas, en las cuales se indican los pasos y las técnicas a utilizar para recolectar y analizar la información.

El capítulo 4: es la propuesta del trabajo de grado, acerca de un modelo para implementar un Plan de Continuidad de Negocio en Chile, obtenida sobre un análisis de conceptos teóricos, mejores prácticas a nivel mundial, metodologías y estándares internacionales.

Finalmente es importante mencionar que la validación de este trabajo de grado es teórica, ya que no es posible esperar implementar esta metodología y ver los resultados. Más adelante se busca que éste sirva para llevar a cabo una implementación de un Plan de Continuidad de Negocio en Chile, con la finalidad de validar sus resultados.

ÍNDICE DE CONTENIDOS Página

1.ANTECEDENTES GENERALES 1

1.1 INTRODUCCIÓN 1

1.2 PLANTEAMIENTO DEL PROBLEMA 3

1.3 OBJETIVOS 4

1.3.1 OBJETIVO GENERAL 4

1.3.2 OBJETIVOS ESPECÍFICOS 4

2.MARCO TEÓRICO 5

2.1 PLAN DE CONTINUIDAD DE NEGOCIO (BCP) 5

2.1.1 DEFINICIÓN DE BCP 5

2.1.2 EVOLUCIÓN DEL PLAN DE CONTINUIDAD DE NEGOCIO 5

2.1.3 BENEFICIOS DEL BCP Y COMO SE RELACIONA CON LA COMPETITIVIDAD EN LAS ORGANIZACIONES 6

2.1.4 BCP EN EL MUNDO 8

2.1.5 BCP EN CHILE 9

2.1.6 EMPRESAS QUE HAN IMPLEMENTADO UN BCP 12

2.2 ADMINISTRACIÓN E INFLUENCIA DE LA CULTURA EN LOS PROYECTOS EMPRESARIALES 14

2.2.1 ADMINISTRACIÓN DE PROYECTOS. 14

2.2.2 ADMINISTRACIÓN DE RIESGOS 16

2.2.3 COMPORTAMIENTO ORGANIZACIONAL 19

2.2.4 CULTURA ORGANIZACIONAL 20

2.2.5 CULTURA ORGANIZACIONAL CHILENA 20

2.2.6 LIDERAZGO 23

2.3 METODOLOGÍAS Y ESTÁNDARES PARA LA ELABORACIÓN DE UN PLAN DE CONTINUIDAD DE NEGOCIO 25

2.3.1 BS 25999 26

2.3.2 BS 25777 28

2.3.3 ITIL 29

2.3.4 NFPA 1600 30

2.3.5 ISO 27002 32

2.3.6 ISO 22301 34

2.4 BUENAS PRÁCTICAS PARA LA ELABORACIÓN DE UN PLAN DE CONTINUIDAD DE NEGOCIO 36

2.4.1 GUÍA DE BUENAS PRÁCTICAS (GPG) 36

2.4.2 CENTRO DE OPERACIONES DE EMERGENCIA (EOC) 39

2.4.3 PRÁCTICAS GENERALMENTE ACEPTADAS (GAP) 40

2.5 PROPUESTA DE ANÁLISIS FINANCIERO DE ORACLE 41

3.DISEÑO METODOLÓGICO 44

3.1 TIPO DE INVESTIGACIÓN 44

3.2 MÉTODOS Y TÉCNICAS DE INVESTIGACIÓN 44

3.3 METODOLOGÍA PARA LA ELABORACIÓN DEL MODELO INTEGRAL DE BCP 44

3.3.1 ANÁLISIS DE LA SITUACIÓN ACTUAL REFERENTE A MODELOS UTILIZADOS A NIVEL MUNDIAL. 46

3.3.2 PLANIFICACIÓN Y POLÍTICA DE CONTINUIDAD DE NEGOCIO. 46

3.3.3 COMPRENSIÓN DE LA ORGANIZACIÓN Y ANÁLISIS DE RIESGOS 47

3.3.4 MEDIDAS PREVENTIVAS 48

3.3.5 ESTRATEGIAS DE RECUPERACIÓN 48

3.3.6 DEFINICIÓN DE RESPONSABILIDADES Y DESARROLLO DE LOS PLANES DE CONTINGENCIA. 48

3.3.7 PRUEBAS, REVISIÓN Y MANTENIMIENTO DEL BCP 49

3.3.8 ANÁLISIS DE LA CULTURA ORGANIZACIONAL CHILENA Y LA INCORPORACIÓN DE LA CULTURA DE BCP A ÉSTA. 49

4.RESULTADOS Y ANÁLISIS 50

4.1 ANÁLISIS DE LA SITUACIÓN ACTUAL REFERENTE A MODELOS UTILIZADOS A NIVEL MUNDIAL. 50

4.2 ACTIVIDADES NECESARIAS PARA DISEÑAR, IMPLEMENTAR Y MANTENER UN PLAN DE CONTINUIDAD DE NEGOCIO (BCP) EN CHILE. 52

4.2.1 PLANIFICACIÓN Y POLÍTICA DE CONTINUIDAD DE NEGOCIOS 52

4.2.2 COMPRENSIÓN DE LA ORGANIZACIÓN Y ANÁLISIS DE RIESGOS 55

4.2.3 MEDIDAS PREVENTIVAS 63

4.2.4 ESTRATEGIAS DE RECUPERACIÓN 65

4.2.5 DEFINICIÓN DE RESPONSABILIDADES Y DESARROLLO DE LOS PLANES DE CONTINGENCIA 69

4.2.6 PRUEBAS, REVISIÓN Y MANTENIMIENTO DEL BCP 71

4.3 ANÁLISIS DE LA CULTURA ORGANIZACIONAL CHILENA Y LA INCORPORACIÓN DE LA CULTURA DE BCP A ÉSTA. 74

4.4 PROPUESTA METODOLÓGICA PARA LA IMPLEMENTACIÓN DE UN PLAN DE CONTINUAD DE NEGOCIO EN CHILE. 76

4.5 ANÁLISIS DE RESULTADOS **77**

4.5.1 ACERCA DEL OBJETIVO GENERAL DE LA INVESTIGACIÓN 77

4.5.2 ACERCA DE LOS OBJETIVOS ESPECÍFICOS DE LA INVESTIGACIÓN 77

CONCLUSIONES Y RECOMENDACIONES **78**

BIBLIOGRAFÍA **80**

LINKOGRAFÍA **83**

ANEXOS **86**

ÍNDICE DE TABLAS **Página**

Tabla Nº 2.1: Número de Quiebras Publicadas en el período 01/01/2005 al 31/12/2012 9
Tabla Nº 2.2: Dotación de trabajadores en declaratoria de quiebra del 01/01/2005 al 31/12/2012 10
Tabla Nº 2.3: Matriz de correlación para determinar los grados de riesgos o niveles de impacto 18
Tabla Nº 2.4: Datos Generales de las metodologías de BCP 25
Tabla Nº 2.5: Cuadro comparativo de la Gestión de Riesgos v/s Gestión de Continuidad de Negocio 36
Tabla Nº 2.6: Componentes de la Guía de buenas prácticas 37
Tabla Nº 3.1: Marco metodológico para el desarrollo del modelo 44
Tabla Nº 4.1: Comparación de los elementos utilizados por cada metodología 49
Tabla Nº 4.2: Ventajas y desventajas de los estándares, metodologías y buenas prácticas 50
Tabla Nº 4.3: Registros de las actividades 58
Tabla Nº 4.4: Categorización de los Riesgos 69
Tabla Nº 4.5: Análisis de Riesgos 60
Tabla Nº 4.6: Descripción de los Campos 60
Tabla Nº 4.7: Ejemplos de medidas preventivas 63
Tabla Nº 4.8: Ejemplos de estrategias de recuperación 64

ÍNDICE DE FIGURAS **Página**

Figura Nº 2.1: Ciclo de vida del Plan de Continuidad de Negocio 26
Figura Nº 2.2: Gestión y Análisis de Riesgos 30
Figura Nº 3.1: Metodología para la elaboración de un Modelo Integral de BCP 45
Figura Nº 4.1: Mapa para análisis de riesgos y categorías para evaluar 59
Figura Nº 4.2: Ejemplo de visualización de riesgos en la Organización 61
Figura Nº 4.3: Relación de la cultura organizacional chilena con el Plan de Continuidad de Negocio 74
Figura Nº 4.4: Resumen del Modelo propuesto para el BCP 75

ÍNDICE DE FÓRMULAS **Página**

Fórmula 2.1: El Riesgo de acuerdo a su magnitud y frecuencia 18
Fórmula 2.2: Costo de pérdida de productividad (P) 42
Fórmula 2.3: Valor de pérdida por ventas (S) 42
Fórmula 2.4: Costo de Recuperación de Servicio (R) 43
Fórmula 2.5: Costo Estimado de Downtime (T) 43
Fórmula 4.1: Costo de pérdida de productividad (P) 57
Fórmula 4.2: Valor de pérdida por ventas (S) 57
Fórmula 4.3: Costo de Recuperación de Servicio (R) 57
Fórmula 4.4: Costo Estimado de Downtime (T) 57

ÍNDICE DE ANEXOS

Anexo A: Ejemplo de registro de las actividades críticas.

Anexo B: Ejemplo de Plan de Contingencia Operacional para una actividad crítica**.**

Anexo C: Ejemplo de un Plan de Pruebas.

Anexo D: Ejemplo de un Plan de Comunicación interna.

1. ANTECEDENTES GENERALES

1.1 Introducción

La progresiva competencia entre las organizaciones empresariales, las demandas cada vez más exigentes de clientes y las partes interesadas (stakeholders*)*, o las obligaciones regulatorias cada vez más restrictivas, son factores que hoy en día comprometen a las empresas a demostrar la firmeza que deben tener las actividades del negocio, para permanecer activas ante cualquier contingencia grave.

En una época de crisis como la que se vive en estos momentos, es necesario desarrollar ventajas competitivas que permitan satisfacer las exigencias del mercado. Una de ellas es garantizar la disponibilidad de los servicios a los clientes, aún después de ocurrir un incidente.

Un estudio realizado por el Emergency Management Forum en Estados Unidos dice lo siguiente (ITEAM, 2013):

"De cada 100 empresas que afrontan un desastre sin contar con un Plan de Continuidad del Negocio, el 43 por ciento nunca reabren, el 51 por ciento sobrevive pero están fuera del mercado en dos años y sólo el 6 por ciento logra sobrevivir a largo plazo".

Una vez ocurrido algún incidente en la empresa, trae como consecuencia problemas financieros, además de daños intangibles como disminución de la productividad, estrés, recursos desviados, y todo ello genera una mala imagen de la empresa. En el entorno de la mala reputación de la empresa, el nombre de los ejecutivos responsables es lo que se pone en juego. No hay que olvidar que las empresas que sufren este tipo de incidentes son la noticia al día siguiente, la prensa es la responsable de señalar con nombres y apellidos a los responsables. Además, por si fuera poco, los directores corporativos pueden ser demandados por las consecuencias de interrupción del negocio.

El Plan de Continuidad de Negocio (BCP, siglas en inglés) es un proceso de dirección que identifica los impactos potenciales que amenazan a la organización y proporciona el marco adecuado para desarrollar la capacidad de dar una respuesta efectiva, que permita proteger los intereses, imagen y valor de las actividades realizadas por la misma.

El BCP tiene como objetivo garantizar una respuesta frente a incidentes que pueden poner en riesgo la operación de la organización, brindar seguridad a los empleados, proteger activos de la organización como procesos y tecnología, minimizar el tiempo de interrupción y asegurar la buena reputación de la organización.

Pero el problema que se presenta en Chile, es que muchas de las empresas aún no cuentan con un plan adecuado, que asegure la continuidad operativa de su negocio ante eventuales desastres que afecten sus procesos e infraestructura tecnológica.

Por todo lo anterior el presente trabajo de grado, tiene por objetivo proponer una metodología para elaborar un Plan de Continuidad de Negocio en Chile.

Para llevar a cabo este trabajo, se analizaron y se evaluaron las características principales de la cultura organizacional chilena con el fin de identificar y aprovechar aquellas positivas y tratar de evitar las negativas, se analizaron también las metodologías utilizadas a nivel mundial en la actualidad para implementar un BCP, con el objetivo de extraer lo mejor de cada una.

Además la metodología de este trabajo de grado comprendió un análisis teórico sobre: administración de proyectos, administración de riesgos, comportamiento organizacional, cultura corporativa, y liderazgo, ya que estos apoyan de forma directa los proyectos empresariales, ligados a la influencia que tiene la cultura en la administración.

Las fuentes bibliográficas de los estándares y guías utilizadas, corresponden a instituciones internacionales enfocadas al estudio e implementación del Plan de Continuidad de Negocio.

1.2 Planteamiento del Problema

El atentado terrorista de las “Torres Gemelas” en el 2001, el accidente nuclear ocurrido en la Central nuclear “Fukushima I” en el 2011 y como no mencionar el terremoto que sufrió Chile el 27 de febrero de 2010, en donde el 45 por ciento de las empresas presentó daños graves o medianos en la continuidad de su negocio, según indicó el Centro de Estudios en Retail de la Universidad de Chile, deja en evidencia una grave falencia en el mundo empresarial.

De acuerdo a los ejemplos mencionados anteriormente, la interrogante que se puede plantear es la siguiente: ¿qué hacer para garantizar la continuidad de las actividades de la organización tras impactos de esta magnitud? La respuesta a esta interrogante existe: los Planes de Continuidad de Negocio, conocidos como BCP (Business Continuity Plan). Mediante estos planes, las organizaciones identifican su exposición a las amenazas internas y externas, seleccionan los activos afectados (materiales e inmateriales) y desarrollan una prevención eficaz, estableciendo acciones contingentes para la rápida recuperación de la actividad de la organización.

Pero el problema que se presenta en Chile, es que muchas de las empresas aún no cuentan, con un plan adecuado que asegure la continuidad operativa de su negocio ante eventuales desastres que afecten sus procesos e infraestructura tecnológica.

En Chile muy pocas empresas, salvo el sector bancario, que está regulado, tiene ejecutivos designados full time a abordar la continuidad operativa. A modo de ejemplo, recién en enero de 2009 el Banco Central de Chile, publica bases de licitación para “contratación del servicio orientado a la implementación de mejoras al Sistema de Gestión de Continuidad de Negocios” (BANCO CENTRAL DE CHILE, 2013).

Del mismo modo, todavía no existen en Chile compañías certificadas en continuidad de negocios, es decir, ninguna organización a nivel local cumple con la norma ISO 22301; y a nivel de organismos internacionales, en el país prácticamente no se conocen las entidades dedicadas a regular la continuidad operativa, como el DRI (Disaster Recovery Institute) en Estados Unidos; y el BCI (Business Continuity Institute) en Inglaterra.

Un indicador demuestra los serios problemas que presenta Chile en Continuidad de Negocio es la gran cantidad de quiebras observadas entre los años 2005 – 2012 promediando aproximadamente 140 organizaciones quebradas anualmente (SQUIEBRAS, 2013).

En síntesis, debido a la historia y el presente de Chile, que evidencia serios problemas de continuidad de negocios de las empresas y que a pesar de la complejidad de la geografía de Chile y la cantidad de amenaza que afectan a las distintas actividades económicas, no se encuentra literatura sobre el tema del BCP y la modesta información encontrada, se refiere al tema, como una herramienta para los sistemas de información, es por esto que surge la necesidad de que las empresas chilenas se pongan a trabajar en lo

que a continuidad de negocios se refiere cuanto antes, ya que en países desarrollados de Europa es prácticamente un estándar. Además las metodologías de BCP existentes a nivel mundial actualmente, son poco prescriptivas, carecen de contenidos claros y lineamientos específicos, poseen muy pocos ejemplos que ilustren de mejor forma su comprensión y están adaptadas principalmente a los países europeos y norteamericanos. Otro problema que se presenta en estas metodologías es que poseen ciertas carencias, algunas no poseen un foque integral de todo el proceso, otras entregan poca o nula información referente a sitios alternos, tecnologías de la información, medidas preventivas, etc.

Bajo este escenario se pretende crear una propuesta metodológica para la implementación de un Plan de Continuad de Negocio en Chile, en el que se expone de forma clara y sencilla los aspectos a considerar y las actividades a desarrollar por cualquier organización que desee estar preparada ante posibles incidencias de seguridad que puedan paralizar la entrega de sus productos y/o servicios. el cual de respuesta a tantos profesionales que ya sea por petición de sus superiores o por iniciativa propia, se plantean la elaboración de un BCP y como a muchos les suele suceder “no saben cómo empezar”.

Con esto se busca contribuir la masificación de los Planes de Continuidad de Negocios en Chile, adquiriendo de entre sus múltiples beneficios potenciar la competitividad y lograr además disminuir la quiebra de empresas chilenas, lo que traería como consecuencia una disminución en el desempleo y una mejor estabilidad laboral.

En síntesis, lo que se pretende es dar respuesta a las siguientes interrogantes: ¿Cómo y cuáles son los pasos a seguir para realizar la implementación de un Plan de Continuidad de Negocio (BCP) en Chile? y ¿Cómo mantener y actualizar el BCP?

1.3 Objetivos

1.3.1 Objetivo General

Crear una propuesta metodológica para la implementación de un Plan de Continuad de Negocio en Chile.

1.3.2 Objetivos Específicos

- Analizar las metodologías existentes y estándares internacionales para la implementación de un Plan de Continuidad de Negocio y extraer sus principales fortalezas.
- Identificar las actividades necesarias para diseñar, implementar y mantener un Plan de Continuidad de Negocio (BCP) en Chile.
- Analizar la cultura organizacional de las empresas chilenas, con el fin de detectar las características más importantes, para así aprovecharlas al momento de la implementación y gestión del BCP.

2. MARCO TEÓRICO

En este capítulo se exponen conceptos y teorías que serán utilizadas posteriormente en el desarrollo de la metodología propuesta.

2.1 Plan de Continuidad de Negocio (BCP)

En los contenidos de este punto se realizó una investigación de la evolución del Plan Continuidad de Negocio, su significado, la actualidad que vive el mundo y la actualidad de Chile con respecto al BCP, además de los beneficios que aporta a la organización el contar con un BCP y los problemas que se pueden generar por no contar con un Plan de Continuidad de Negocio.

2.1.1 Definición de BCP

Capacidad estratégica y táctica de la organización para planificar y responder ante los incidentes e interrupciones del negocio con el fin de permitir la continuidad de las actividades comerciales en un nivel aceptable previamente definido (BSI GROUP, 2007).

Una definición más completa de BCP es la realizada por ITEAM (2013), una empresa consultora especializada en Planes de Continuidad de Negocio, Plan de Manejo de Crisis y Riesgo Empresarial. Esta señala que el BCP es una metodología interdisciplinaria, que se basa en procedimientos y medidas de seguridad, utilizadas para crear y validar planes logísticos, para que en la práctica la empresa pueda recuperar sus funciones críticas parcial o totalmente, después de una interrupción o desastre. Además consiste en los pasos que el personal de la empresa debe realizar, según los manuales y procedimientos del BCP, para hacer frente a situaciones y ambientes inesperadas, que pueden afectar la continuidad y el normal funcionamiento del negocio. El BCP busca asegurar que los productos o servicios continúen siendo entregados, a los diferentes canales de distribución durante una interrupción no planeada. Un plan de Continuidad de Negocio tiene como objetivo el sostenimiento de los servicios de la empresa y de los procesos críticos, así como la disminución de impactos ante eventos inesperados o desastres. El BCP está orientado a la obtención de un plan metodológico, que garantice la cobertura técnica y organizativa de las áreas críticas del negocio.

2.1.2 Evolución del Plan de Continuidad de Negocio

El término Plan de Continuidad de Negocio o Business Continuity Plan (BCP por sus siglas en inglés), cada vez expande más su alcance. Esto se compara con términos utilizados anteriormente que sólo estaban enfocados a áreas específicas como Disaster Recovery y Contingency Planning que han pasado a formar parte del BCP(BSI GROUP, 2007).

En el siglo pasado, en los setenta Norman L. Harris, Edward S. Devlin y Judith Robey, al tratar de encontrar un método de planificación y gestión que evitara la continua atención de los problemas de

forma aleatoria, dieron inicio a una actividad que llamaron Disaster Recovery Planning. Con esto se aseguraba la planeación de cómo reaccionar en caso de un desastre. Más tarde, esa actividad fue llamada Contingency Planning, término que resultó ser más universal puesto que la Contingencia es algo que puede suceder o no suceder o puede también denominarse “riesgo” (GASPAR, 2004).

En los inicios de la utilización de este enfoque de analizar las contingencias empresariales, cuando se conocía como Disaster Recovery, la actividad estaba dirigida a áreas de Tecnologías de información. Más adelante, cuando las tecnologías de la información comenzaron a formar parte de las áreas de soporte de las operaciones de toda la empresa, el Disaster Recovery expandió su alcance, llamándose ahora Business Continuity Plan (BCP), traducido como Plan de Continuidad de Negocio y Business Continuity Management (BCM), traducido como Gestión de la Continuidad de Negocio. En la actualidad el concepto de continuidad de negocio es aplicado a toda la organización, es un concepto global, que incorpora a toda la cadena logística, es decir desde el cliente hasta el proveedor de insumos.

2.1.3 Beneficios del BCP y como se relaciona con la competitividad en las organizaciones

Los beneficios que se pueden alcanzar al tener implementado de forma correcta un Plan de Continuidad de Negocio son:

- **Ventaja competitiva frente a otras organizaciones:** el hecho de mostrar que se toman medidas para garantizar la continuidad de negocio mejora la imagen pública de la organización y revaloriza la confianza frente a accionistas, inversores, clientes y proveedores.
- **Previene o minimiza las pérdidas de la organización en caso de desastres:** es capaz de identificar de forma proactiva los posibles impactos e inconvenientes que una interrupción de sus actividades de negocio puede provocar.
- **Asegurar que las actividades del negocio soporten y se recuperen ante interrupciones:** aumentando la disponibilidad de los servicios dispuestos para el cliente.
- **Menor riesgo de sufrir sanciones económicas:** al adaptarse a requerimientos regulatorios.
- **Asignación más eficiente de las inversiones en materia de seguridad:** gracias al análisis de riesgos (BIA), el cual permite priorizar las actividades críticas y fijar los esfuerzos y los presupuestos en las áreas más necesitadas (GASPAR, 2004).

Dentro de las estrategias que la organización debe desarrollar para estar en un buen nivel de competitividad en el mercado actual, se tienen las siguientes:

- **Maximización de capacidades:** Como actividad del BCP está, que en cada área se comparta el conocimiento sobre las actividades que realiza cada trabajador, esto con la finalidad de que todo el equipo conozca las tareas y en caso de que la empresa tenga que declarar un estado de

contingencia, se comunique con el personal identificado como personal clave, para continuar las operaciones del negocio, pero además se tenga una segunda y tercera alternativa (BASSI, 1999).

- **Mejora de procesos:** Con el Análisis de Impacto al Negocio (BIA por sus siglas en inglés) se obtienen como resultado un informe sobre los procesos clave de la organización, los cuáles deben ser prioridad, monitoreando que en todo momento se cuente con los recursos necesarios para no detenerlos. Logrando así un incremento en la satisfacción del cliente y mejora de la calidad (BASSI, 1999).
- **Buena imagen corporativa:** estar preparado para responder a cualquier interrupción, teniendo formas alternas de atender a los clientes, habla muy bien de cualquier organización. Los clientes siempre van a preferir a un proveedor que tenga buena imagen en cuanto al nivel de servicio a otra que tenga reputación de que se caigan sus sistemas y no conteste cuando se necesiten (BASSI, 1999).
- **Conocimiento del contexto dónde se desarrolla:** Durante la planeación de los procesos clave de la empresa, se estudia el marco legal en cual se opera, empezando desde las multas que ocasionaría no entregar un informe a alguna institución reguladora en el sector, o cuales podrían ser las situaciones en las que no se permitiría hacer una prórroga para entregar la información más tarde. Así, cuando acontezca una situación contingente, tendremos conocimiento sobre lo que se puede esperar, para poder atender de forma normal a los clientes, en lugar de preocuparse por elaborar los reportes a las instituciones reguladoras (BASSI, 1999).
- **Capacidad de servicio en situación de crisis:** El personal de una organización que ha planeado como actuar en una situación emergente y ha tenido una capacitación de qué hacer y cómo hacerlo, tendrá una mejor capacidad de trabajar bajo esa presión que otra organización que no ha mencionado a sus empleados, el tipo de situaciones catastróficas que pueden suceder en la organización. Aun sabiendo que los planes no se seguirán detalle a detalle cómo se han planeado, pues en cada situación es posible tener una variable que lleve consigo el cambio de planes, el haber instruido al personal sobre estas situaciones sirve pues ellos tienen la idea de que en cualquier momento la empresa puede estar en esta situación. Ello lleva al desarrollo de la habilidad para trabajar ante los cambios (BASSI, 1999).
- **Disponibilidad:** Con la implantación de un Plan de Continuidad de Negocio, la empresa se ve obligada a estudiar la forma de tener en cualquier momento la disponibilidad de sus servicios ante sus clientes. Para esto puede apoyarse con estrategias como redundancia de datos, virtualización, implementar el trabajo desde casa de sus empleados con la finalidad de que en cualquier momento puedan atender las solicitudes necesarias, etc. (BASSI, 1999).
- **Protección de la marca:** Con la Continuidad de Negocio después de ocurrido un incidente, se mantiene la credibilidad de la empresa. Mediante la capacitación y concientización al personal, se logra que los empleados puedan ser conscientes de lo importante que es trabajar en equipo. Esto trae como resultado dentro de la operación diaria, un excelente clima laboral y aumento de la

productividad, en un escenario de contingencia, esto ayuda a facilitar la comunicación entre el personal, dando como resultado un excelente trabajo y continuidad al negocio (BASSI, 1999).

2.1.4 BCP en el Mundo

En una época de crisis como la que se vive en estos momentos, es necesario desarrollar ventajas competitivas que permitan satisfacer las exigencias del mercado. Una de ellas es garantizar la disponibilidad de los servicios a los clientes, aún después de ocurrir un incidente.

Un estudio realizado por el Emergency Management Forum en Estados Unidos dice lo siguiente (ITEAM, 2013):

"De cada 100 empresas que afrontan un desastre sin contar con un Plan de Continuidad del Negocio, el 43 por ciento nunca reabren, el 51 por ciento sobrevive pero están fuera del mercado en dos años y sólo el 6 por ciento logra sobrevivir a largo plazo".

Una vez ocurrido algún incidente en la empresa, trae como consecuencia problemas financieros, además de daños intangibles como disminución de la productividad, estrés, recursos desviados, y todo ello genera una mala imagen de la empresa. En el entorno de la mala reputación de la empresa, el nombre de los ejecutivos responsables es lo que se pone en juego. No hay que olvidar que las empresas que sufren este tipo de incidentes son la noticia al día siguiente, la prensa es la responsable de señalar con nombres y apellidos a los responsables. Además, por si fuera poco, los directores corporativos pueden ser demandados por las consecuencias de interrupción del negocio.

A nivel mundial existen organizaciones especializadas en el apoyo a este tema. Dentro de las más sobresalientes están (ITEAM, 2013):

- A nivel de consultaría: Deloitte, KPMG, Risk México, Price Water House Coopers y AON.
- A nivel de servicios de apoyo, como hardware, software, sitios alternos o centro de llamadas: Sungard, IBM, EMC, Symantec, Veritas, CITRIX y CISCO.
- A nivel de disciplina: Business Continuity Institute (BCI), Business Standar Institute (BSI), Disaster Recovery Institute Internacional (DRII), ISO 27002, ITIL, ISO 22301 y NFPA.

Una encuesta realizada por "Chartered Management Institute" sobre manejo de continuidad de negocios a 1257 gerentes de empresas del Reino Unido, arroja que sólo en la mitad de sus empresas tiene un BCP, esto a pesar que más de un 94 por ciento de ellos están de acuerdo con su importancia (WOODMAN, 2007).

2.1.5 BCP en Chile

En Chile se está recién comenzando con este tema, muy pocas empresas, salvo el sector bancario, que está regulado, tiene ejecutivos designados full time a abordar la continuidad operativa. A modo de ejemplo, recién en enero de 2009 el Banco Central de Chile, publica bases de licitación para "contratación del servicio orientado a la implementación de mejoras al Sistema de Gestión de Continuidad de Negocios", Es relevante mencionar que el Banco usa como referencia el estándar internacional de Continuidad de Negocios BS 25999-1 y que están en proceso de actualización al estándar ISO 22301, adoptado también por la Banca Comercial. Actualmente, el sistema de gestión de continuidad del Banco Central administra 51 actividades calificadas como críticas, para las cuales se realizan alrededor de 60 pruebas periódicas en un año. Los escenarios bajo los cuales se han definido planes alternativos incluyen escenarios de desastres e indisponibilidad de instalaciones, falla de proveedores claves, acción maliciosa y ausencia de personal crítico. El calendario de pruebas se planifica al inicio del año y las fechas específicas de cada prueba se definen de acuerdo a calendarios establecidos por las unidades responsables de las actividades críticas. El calendario de pruebas, también incluye pruebas frente a la indisponibilidad de instalaciones (oficinas habituales en las cuales el Banco desarrolla sus funciones), motivo por el cual se traslada la operación de los funcionarios críticos a un Sitio de Operación Alternativo (BANCO CENTRAL DE CHILE, 2013).

Además, todavía no existen compañías certificadas en continuidad de negocios, es decir, ninguna organización a nivel local cumple con la norma ISO 22301; y a nivel de organismos internacionales, en el país prácticamente no se conocen las entidades dedicadas a regular la continuidad operativa, como el DRI (Disaster Recovery Institute), en Estados Unidos; y el BCI (Business Continuity Institute), en Inglaterra. Un indicador que se puede utilizar para ver la carencia de la continuidad de los negocios de las empresas en Chile, es la cantidad de quiebras observadas entre los años 2005 – 2012 y que son presentadas a continuación en la Tabla Nº 2.1 (SQUIEBRAS, 2013):

Tabla Nº 2.1: Número de Quiebras Publicadas en el período 01/01/2005 al 31/12/2012.

	Ene.	Feb.	Mar.	Abr.	May.	Jun.	Jul.	Ago.	Sep.	Oct.	Nov.	Dic.	Totales.	Al 31.12.2012	Variación al 31 de Diciembre del año anterior
2005	17	1	19	16	16	8	7	9	5	11	14	12	**135**	135	***
2006	12	1	11	13	14	10	12	13	14	9	5	18	**132**	132	**-2,22%**
2007	13	3	17	10	14	17	9	9	10	24	10	7	**143**	143	**8,33%**
2008	20	0	8	10	15	17	10	16	9	20	12	13	**150**	150	**4,90%**
2009	22	1	24	13	22	9	13	19	16	14	9	11	**173**	173	**15,33%**
2010	12	1	5	8	5	21	14	18	10	13	11	13	**131**	131	**-24,28%**
2011	17	0	17	10	8	11	12	8	13	6	17	14	**133**	133	**1,53%**
2012	8	6	16	17	9	9	8	17	6	15	8	11	**130**	130	**-2,26%**

Fuente: Superintendencia de quiebras Chile, 2013.

En la siguiente Tabla Nº 2.2, se puede observar la cantidad de trabajadores existentes al momento de la declaratoria de quiebra de la empresa.

Tabla Nº 2.2: Dotación de trabajadores al momento de la declaratoria de quiebra del 01/01/2005 al 31/12/2012.

	Ene.	Feb.	Mar.	Abr.	May.	Jun.	Jul.	Ago.	Sep.	Oct.	Nov.	Dic.	Totales.
2005	166	0	199	280	139	237	7	46	6	30	133	31	1.274
2006	143	14	90	94	289	30	172	40	490	278	2	413	2.055
2007	112	54	157	46	0	224	28	10	16	407	12	6	1.072
2008	1.333	0	204	93	709	16	102	175	342	596	214	158	3.942
2009	548	15	92	373	518	113	59	36	258	261	64	208	2.545
2010	73	5	1.001	59	30	233	50	255	68	111	332	30	2.247
2011	163	0	613	1.952	58	57	33	48	236	56	85	39	3.340
2012	63	274	1.206	608	34	8	16	388	6	148	0	390	3.141

Fuente: Superintendencia de quiebras Chile, 2013.

*Nota: Los meses que figuran con 0 trabajadores, quiere decir que no habían trabajadores con contrato vigente al momento de la incautación y/o no se pudo determinar el número de éstos.

Cabe destacar que todas estas quiebras declaradas son porque estas empresas no pudieron enfrentar sus compromisos económicos, las reales causas de las mismas son diversas, desde deficiente gestión, pérdidas de competitividad, siniestros, etc. Este simple análisis señala que existen problemas de continuidad de negocios en las empresas chilenas.

A continuación se presentan algunos casos de catástrofes que han ocurrido en Industrias Chilenas, y que de haber contado con un eficiente Plan de Continuidad de Negocio, sus impactos hubiesen sido mucho menores:

- **Industria Salmonera:** Desde julio de 2007, cuando se confirmó el primer caso de anemia infecciosa del salmón (conocida por su sigla en inglés ISA) en un vivero en la isla de Chiloé, el sector ha estado en problemas. Obligando a las empresas a rediseñar el proceso productivo (LONG, 2009).

- **Caso Farmacias**: Problemas legales de monopolio, han gatillado una serie de reacciones de la comunidad y legisladores que pueden modificar la normativa del rubro y eventualmente poner en riesgo la continuidad del negocio farmacéutico, tal como sucedió con las pequeñas farmacias cuando ingresaron al mercado. En este caso la causa de la crisis tienes sus orígenes desde el interior de las empresas, afectando en forma directa la imagen de estas. Finalmente dos son las caras que grafican el desenlace en el llamado Caso Farmacias, mientras el Tribunal de Defensa de la Libre Competencia (TDLC) multó a Salcobrand y Cruz Verde por cerca de US $40 millones (el monto más alto de la historia de Chile en un caso de colusión de precios), por otro lado los diez imputados aceptaron el ofrecimiento del Ministerio Público de suspender condicionalmente el proceso. Las condiciones que deberán cumplir son el pago a modo de indemnización de un total de $255 millones en beneficio de organizaciones como: Cruz Roja, Coaniquem, el Instituto Nacional del Cáncer y la

Liga Chilena Contra la Epilepsia, además de asistir y aprobar un curso de ética empresarial, buenas prácticas de gobierno corporativo o responsabilidad social de la empresa, entre otras medidas (CASO FARMACIAS, 2013).

- **Industria Alimentaria:** En el año 2008 se encontró carne de cerdo contaminada con dioxinas, cerrando temporalmente mercados de Japón y Korea que representan el 80% de las exportaciones de carne de cerdo, por un monto de US$ 400.000.000. En el año 2009 se tiene problemas con la Listeriosis, el primer producto afectado es el queso, luego es afectado los embutidos, que obligó a la empresa involucrada a retirar del mercado su producción, generando desconfianza de los consumidores principalmente en el consumo de embutidos (CHILE POTENCIA ALIMENTARIA, 2013).

- **El sector Forestal**: La crisis internacional afectó en distintas magnitudes a los subsectores de la industria forestal. Ya desde principios de 2008 comenzó a golpear la disminución de demanda de EEUU, principal mercado chileno para madera sólida. El índice de construcción de casas se desplomó en 45,2% en mayo de 2008 respecto del mismo mes del año anterior, y casi un 80% desde 2006. Esto afectó a las empresas elaboradoras de madera, que exportan a ese mercado, pero, después de la caída de Lehman Brothers, la contracción de la demanda se extendió a otros mercados, tales como Europa, Asia y Medio Oriente, impactando a su vez en la demanda de madera aserrada. En 2008, 148 aserraderos, principalmente medianos y pequeños, paralizaron sus actividades en Chile. El último trimestre de 2008 le tocó el turno a la industria de celulosa, cuya demanda internacional prácticamente se detuvo para Chile por más de cuatro meses, para regresar debilitada y a precios a los cuales ninguna planta del Hemisferio Norte podría producir. Sin embargo, industrias como la de papel y productos sanitarios recibieron impactos mucho menos severos. Las empresas grandes debieron reducir las producciones de sus aserraderos y la cosecha de sus bosques en 2009, y disminuir el ritmo de producción de celulosa. La celulosa, por su parte, ha mejorado sus volúmenes en virtud de mayores compras de China, aún con precios bajos pero mostrando leves alzas (RAGA, 2009).

- **Terremoto y tsunami del 27 de febrero de 2010:** Un estudio realizado por la Organización Panamericana de la Salud (2010), comenta lo siguiente: el día 27 de febrero a las 03:34 horas, hora local, se registró un terremoto de magnitud 8,8 en la escala MW que tuvo una duración aproximada de tres minutos. El epicentro se situó en la costa de la región del Maule, aproximadamente a 8 km al oeste de Curanipe y 115 km al noreste de Concepción. A continuación se puede observar los efectos o consecuencias que dejó el terremoto (OPS, 2010):

- **Efectos en la población:** En Maule y Bío Bío, las regiones más golpeadas por el terremoto y tsunami, habitan 2.769.659 personas, el 19% de la población total del país. El desastre ocasionó 512 muertos, 16 desaparecidos y 800 mil personas damnificadas. La mayor cantidad de fallecidos fue debido al tsunami, por ejemplo en la comuna de Pelluhue se registraron 47 muertos, 6 eran pobladores de este lugar y 41 fueron turistas chilenos (OPS, 2010).
- **Energía:** Como resultado del sismo, se produjo un apagón total del área cubierta por el Sistema Interconectado Central (SIC), que abastece de energía desde Taltal en Antofagasta hasta la Isla Grande de Chiloé, y una indisponibilidad de capacidad de generación. La electricidad fue restablecida paulatinamente en el país dentro de las primeras cuatro horas posteriores al sismo, a excepción de Bío Bío donde al cabo de seis horas sólo el 40% de la región contaba con suministro (OPS, 2010).
- **Agua y saneamiento:** De acuerdo a la Superintendencia de Servicios Sanitarios (SISS), el terremoto y el tsunami afectaron los sistemas de agua potable, las redes de alcantarillado y de descarga de aguas servidas, y las plantas de tratamiento en zonas urbanas y rurales. Hubo roturas en las redes de distribución, daños estructurales en estanques de regulación, y fallas en los sistemas de bombeo e impulsión por la falta de electricidad. A ello, se sumó la disminución en la disponibilidad de cloro en el país, por los daños producidos en la principal planta productora -Occidental Chemical Chile- ubicada en la bahía de Talcahuano (OPS, 2010).
- **Transportes y comunicaciones:** El Ministerio de Obras Públicas registró daños en 1.154 km de caminos, 191 puentes y 9 aeródromos o aeropuertos. El terremoto y tsunami también afectaron, en distintos grados, la vialidad urbana en 40 comunas entre las regiones de Valparaíso y La Araucanía. Ante la ausencia de la energía eléctrica, el país quedó sin comunicación en la red de teléfonos fijos y en la de celulares, y se produjo un prolongado corte de las comunicaciones de las radio emisoras tanto de FM como AM. Las líneas de telefonía fija comenzaron a recuperar su normalidad en las horas posteriores reaccionando en general mejor que la telefonía móvil, que estuvo varios días sin servicio (OPS, 2010).
- **Empleo:** Según la Organización Internacional del Trabajo OIT, 93.928 trabajadores perdieron su empleo, de los cuales 34.437 en Bío Bío y 28.090 en Maule, principalmente en la pesca, el comercio y la agricultura. La catástrofe se ensañó con las pequeñas empresas, que concentran el 81% de los empleos perdidos (OPS, 2010).

2.1.6 Empresas que han implementado un BCP

- **WAL-MART STORES INC.**

En Agosto del 2005 cuando Katrina cambió su categoría de tormenta tropical a huracán, Jason Jackson, Director de Continuidad del Negocio de Wal-Mart cambio su ubicación al centro de comando de emergencias de Wal-Mart. Dos días después cuando el huracán llegó a Florida, Jackson estaba acompañado de 50 gerentes y personal de apoyo, antes de que el huracán tocara tierra en el

Golfo de México, Jackson ordenó a las bodegas de Wal-Mart entregar provisiones a áreas de almacenamiento designadas para tener la capacidad de abastecer a las tiendas cuando fuera posible. Cuando el sistema computarizado que actualiza los inventarios de la zona de Wal-Mart quedo sin señal, Jackson atendió las llamadas de las tiendas para saber lo que necesitaban, para el siguiente martes, camiones de Wal-Mart fueron a abastecer generadores y toneladas de hielo seco a lo largo de las tiendas ubicadas en el golfo. Inicialmente 126 sucursales fueron cerrados por encontrarse en el paso de Katrina, a pesar de las pérdidas reportadas por las tiendas, 15 días después, todas a excepción de 15 tiendas, volvieron a abrir sus puertas (ZIMMERMAN, 2005).

- **COMPAREX ESPAÑA S.A.**

En febrero de 2005 tuvo lugar un incendio en el Edificio de Windsor, dónde estaban los servidores centrales, después de 6 horas todo el inmueble quedo devastado. Ante esta situación Comparex activa su Plan de Continuidad de Negocio (BCP). Dentro de las estrategias que puso a pruebas están: Backups de información, lugares de trabajo para que los empleados puedan reanudar sus operaciones desde otro sitio, accediendo a las aplicaciones críticas utilizando como base de acceso el internet, infraestructura que le permitió la comunicación de voz y datos entre los centros (MUR, 2013).

El BCP le permitió a la organización poder reaccionar la misma noche del incendio, se identificaron los elementos tecnológicos (servidores, sistemas de almacenamiento, puestos de trabajo conectados a la red, comunicaciones, etc.) que se encontraban disponibles y en funcionamiento, así como los inactivos. Se recurrió a las copias de información que la organización tenía en resguardo en Madrid y Barcelona, verificando si podía hacerse la recuperación completa al último día hábil de actividad. Se activó el alquiler de las oficinas alternas, dotándolas de equipo necesario para trabajar y se contactó a los clientes notificándoles la situación de la compañía. El plan resulto un éxito para la compañía (MUR, 2013).

- **BANKINTER**

El 18 de julio de 2012, BSI realizó la entrega de su primer certificado a nivel internacional de la nueva norma ISO 22301:2012 de Continuidad de Negocio a Bankinter. El certificado avala que la entidad mantiene operativo un Sistema de Gestión de Continuidad de Negocio conforme a los requisitos de la nueva norma. Este certificado es el primer certificado ISO 22301 emitido por BSI a nivel internacional. Además Bankinter pasa a ser la primera entidad financiera a nivel mundial certificada en ISO 22301. Según los requisitos que exige esta norma, el certificado acredita el Sistema de Gestión de Continuidad de Negocio (SGCN) de Bankinter para los procesos de identificación, autentificación y firma de operaciones financieras y sus evidencias electrónicas a través de Internet, Teleproceso Operativo y la infraestructura de routing de Renta Variable para sus centros de Tres Cantos y Alcobendas en Madrid. (BSI GROUP, 2012).

2.2 Administración e influencia de la cultura en los proyectos empresariales

Es de suma importancia proporcionar un panorama general sobre temas y conceptos de la administración que apoyan de forma directa los proyectos empresariales, ligados a la influencia que tiene la cultura en la administración, ya que un Plan de Continuidad de Negocio es un proyecto empresarial y como tal va a estar influenciado por la cultura organizacional (ROMERO, 2008).

2.2.1 Administración de Proyectos.

Hoy en día, la mayoría de las organizaciones reconocen que la Administración de Proyectos como disciplina, tiene mucho que ofrecer al crecimiento y éxito de sus estrategias de negocio. “Los proyectos son la clave en esta nueva era de competencia global” (FORSBERG, 2000).

Por pequeño que sea el proyecto, se requieren habilidades de administración del mismo para sortear las diferentes situaciones que se presenten, y además garantizar el cumplimiento de los objetivos dentro de los tiempos estipulados. Estas habilidades van desde la definición del proyecto, hasta la administración de sus medidas de avance. Adicionalmente, se deben incorporar técnicas para el manejo de contratos y el manejo de proveedores (DACCACH, 2007).

José Daccach (2007), especializado en servicios de administración de proyectos, identifica 12 actividades para la administración de proyectos, que se detallan a continuación.

1) **Definición del proyecto:** Pequeño o grande el proyecto, es necesario definir su alcance, las decisiones se toman y se califican mediante valoración del impacto que tienen en su resultado final, dado por esta etapa de definición, cuanto más grande sea el proyecto, la importancia de dejar esta información explícitamente estipulada aumenta (DACCACH, 2007).
2) **Planeación del Trabajo:** Se definen las actividades a realizar y la dependencia entre ellas. También se identifican los recursos con los que se cuenta para realizar las actividades, los recursos incluyen personal, presupuesto y elementos requeridos (DACCACH, 2007).
3) **Administración de Contratos:** Hay que identificar dos temas fundamentales: la entrega de los resultados (entregables) y el cumplimiento de las fechas para estas entregas. Para ambos se establecen criterios y requerimientos que permiten controlar el cumplimiento de los dos temas (DACCACH, 2007).
4) **Administración de Proveedores:** Es imperante establecer cómo se manejarán los incumplimientos, normales hasta cierto punto, entre lo programado inicialmente y lo que realmente está entregando el proveedor (DACCACH, 2007).
5) **Administración del Plan de trabajo:** Describe lo que hay que hacer, el orden del trabajo, el esfuerzo requerido y quien está asignado a cada tarea, pero sólo representa el mejor estimado de cómo completar el trabajo que queda por hacer en un momento dado de un proyecto (DACCACH, 2007).

6) **Administración de situaciones:** Por lo general, un proyecto se administra en dos instancias: una a nivel de gerente y equipo de proyecto, y la segunda a nivel de gerencia de la compañía (DACCACH, 2007).
7) **Administración del Alcance:** El alcance de un proyecto describe sus límites y lo que el proyecto va a entregar, qué información se necesita y qué partes de la organización se verán afectadas (DACCACH, 2007).
8) **Administración de Riesgos:** El riesgo es una condición futura que existe fuera del control del grupo del proyecto, y que puede tener un impacto negativo sobre el resultado del proyecto si se llega a dar la condición. Administradores reactivos esperan a resolver la situación cuando ésta suceda. Los administradores proactivos tratan de identificar y resolver problemas potenciales antes de que ocurran (DACCACH, 2007).
9) **Administración de la comunicación:** Hay dos niveles de comunicación en un proyecto. Todos los proyectos deben comunicar su estado. Adicionalmente, si el proyecto es complejo o más grande, se necesita un nivel más sofisticado de comunicación definido en un Plan de Comunicaciones (DACCACH, 2007).
10) **Administración de la documentación:** Aunque esta es una de las tareas que puede ser asistida por tecnologías como un depósito documental, estas herramientas pueden ser difíciles de administrar e incorporan mayores problemas al proyecto. Otra decisión es el formato estándar para los documentos, se recomienda utilizar el PDF para los documentos que no variarán una vez que se publiquen, y crear un sitio Web para su almacenamiento (DACCACH, 2007).
11) **Administración de la calidad:** La calidad de un proyecto se mide bajo el tiempo necesario para cumplir con las expectativas entregables del cliente, por lo tanto el objetivo central del equipo del proyecto es tratar de cumplir y exceder los requerimientos del cliente. La medición de la calidad no es un evento, sino un proceso continuo y un estado mental (DACCACH, 2007).
12) **Administración de las métricas:** Para fijar las métricas para el proyecto, se sugiere identificar los criterios de éxito en términos de entregables y ejecución, determinar cómo medir tanto el logro final como el avance, seleccionar un número balanceado de métricas, y recoger la información. Es de vital importancia colocar parámetros de comparación mediante metas ya que la métrica por sí sola, no dice mucho. En general, este proceso es de poca importancia para proyectos pequeños, ya que no hay ni el tiempo para recolectar los valores, y menos para analizar y tomar correctivos (DACCACH, 2007).

Para el inicio y futuras actualizaciones del ciclo de vida del Plan de Continuidad de Negocio es necesario tomar en cuenta los puntos que se han mencionado anteriormente con el fin de generar un plan eficiente para la operación del negocio. En este punto hay información que no se debe pasar por alto, pero ¿qué sucede cuando algo se sale de lo planeado?, y ¿cuándo una situación cambia la dirección del trabajo?, para dar respuesta a estas y más interrogantes, es necesario estudiar sobre administración de riesgos,

logrando con ello estar preparado ante una situación que puede cambiar el rumbo del proceso administrativo en caso de ocurrir.

2.2.2 Administración de Riesgos

La administración de riesgos es una herramienta que ayuda en el proceso de toma de decisiones que convierte la incertidumbre en oportunidades, evita el suicidio financiero y catástrofes de graves consecuencias (DE LARA, 2005).

La palabra riesgo viene del latín "risicare", que significa atreverse a transitar por un sendero peligroso, tiene un significado negativo, relacionado con peligro, daño, siniestro o pérdida. Sin embargo, el riesgo es parte inevitable de los procesos de toma de decisiones en general y de los procesos de inversión en particular. La medición cuantitativa del riesgo se asocia con la probabilidad de una pérdida en el futuro. Los seres humanos deben conocer y responder intuitiva o cuantitativamente a las probabilidades que confrontan en cada decisión (DE LARA, 2005).

Alfonso de Lara Haro (2005), comenta que la clave para una correcta evaluación de riesgos consiste en:

- Identificar el riesgo (Clasificar los tipos de riesgo relevantes para el negocio).
- Definir cómo serán tratados (Evitar el riesgo, contratar seguros, utilizar coberturas con instrumentos financieros, implantar metodologías para riesgos cuantificables, etc.).
- Establecer controles (Definir procedimientos para no exceder los límites de cada riesgo).
- Monitorear y reportar la situación del riesgo (informar periódicamente sobre la evolución de los riesgos).

La Administración de Riesgos concierne a todos los miembros de una entidad e involucra a todos sus niveles de organización. Su actividad no es estática, ya que siempre habrá nuevos y diferentes riesgos al estar dentro de un entorno cambiante. Para que una empresa tenga una administración completa, es necesario estudiar los incidentes que pueden afectar su operación. Es como surge la necesidad de tener un área dedicada al estudio sistemático de los problemas y que este estudio, consiga determinar las estrategias adecuadas para reducir a su nivel mínimo el daño que puede ocurrir (DE LARA, 2005).

En cuanto a lo relevante para el Plan de Continuidad de Negocio de lo que Alfonso de Lara (2005) comenta en su libro "Medición y Control de Riesgos Financieros" sobre las medidas que podrían minimizar los riesgos, se destacan los siguientes:

- **Transferir a un tercero la función causante del riesgo:** Por ejemplo, para un carpintero que debe entregar muebles a sus clientes, pero está consciente de los riesgos que existen en el transporte de mercancías, decide contratar un proveedor que le brinde el servicio de transporte de la mercancía a sus clientes (DE LARA, 2005).

- **Comprar un contrato de derivados para atenuar el riesgo:** Se refiere al conocimiento que se debe tener sobre el aumento de un precio, para evitar pagar ese aumento, se elabora un contrato para mantener el precio actual (DE LARA, 2005).
- **Disminuir la probabilidad de que ocurra el evento negativo:** La pérdida atribuible de un riesgo depende de la probabilidad de ocurrencia y de la pérdida monetaria, si existe. En algunas ocasiones es posible aminorar la posibilidad de ocurrencia. Un ejemplo seria aminorar la probabilidad de un incendio, sustituyendo el cableado eléctrico (DE LARA, 2005).
- **Reducir la pérdida relacionada con el evento negativo:** Con el ejemplo del incendio, el costo del incendio puede aminorarse instalando sistemas de rociado, diseñar instalaciones con zonas de incendio, etc. (DE LARA, 2005).
- **Prescindir las actividades que originen el riesgo:** Por ejemplo, una compañía puede interrumpir un producto o línea de servicios en caso de que la utilidad sea menor que el riesgo (DE LARA, 2005).

Cuando se identifican los riesgos, existen diferentes posibilidades para las acciones que se emprenderán con los resultados del análisis de riesgos, de las cuales destacan las siguientes (DE LARA, 2005):

- Una de las alternativas es evitarlos, para lo cual se debe eliminar completamente la fuente del riesgo.
- Otra alternativa es mitigar los riesgos, lo cual es una acción preventiva para reducir el daño. Para lograr esto, Alfonso Haro sugiere elaborar las siguientes tareas:
  - Cambios estratégicos (metodología de trabajo, herramientas, proveedores).
  - Cambios logísticos.
- La tercera alternativa, es aceptarlos, lo que implica elegir entre las opciones que se mencionan a continuación:
  - Pasiva: no se toma ninguna medida, sólo se monitorea el riesgo de forma regular.
  - Activa: se implementa o usa un Plan de contingencia, en caso de que el riesgo suceda.

A continuación en la Tabla Nº 2.3, se presenta un ejemplo de matriz de correlación en la que intervienen los principales parámetros que facilitan la caracterización y análisis de riesgos, realizada por Jesús G. Martínez (2001):

Tabla Nº 2.3: Matriz de correlación para determinar los grados de riesgos o niveles de impacto.

Zona o Actividad Analizada:	**Caracterización o tipo de Riesgo:**	**Elaboro:** **Revisión:** **Fecha:**
Clasificación de Frecuencias	**Durabilidad o tipo de Impacto**	**Niveles o grados de Riesgo**
• Constante: 3 o más veces por año. • Frecuente: 1 - 2 veces por año. • Periódica: 1 vez cada 2 años. • Ocasional: 1- 3 veces cada seis años. • Eventual: 1 -3 veces cada 7 a 14 años.	a. Irreversible. b. Reversible con tratamiento. c. Prolongado. d. Duradero. e. Momentáneo. f. Instantáneo.	I. Crítico. II. Muy Alto. III. Alto. IV. Controlable. V. Aceptable o Permisible. VI. Bajo.

Magnitudes y tipos de Impactos	
1. Catastrófica. 2. Muy Grave. 3. Grave. 4. Moderada. 5. Baja. 6. Mínima.	a. Irreversible. b. Reversible con tratamiento. c. Prolongado. d. Duradero. e. Momentáneo. f. Instantáneo.

	Relaciones de Magnitud del Impacto					
	1	2	3	4	5	6
Frecuencias	**Niveles de Riesgo**					
Constante	I	I	I	II	III	III
Periódica	I	I	I	III	III	III
Frecuente	I	II	II	III	IV	IV
Ocasional	II	II	III	IV	IV	V
Eventual	III	III	III	IV	V	VI
Remota	III	IV	IV	V	V	VI

Fuente: Martínez, 2001.

De la anterior Tabla Nº 2.3 se puede analizar que los eventos que se comportan entre los niveles de riesgo I y II, implican la obligación o necesidad de actuar de inmediato. Esta matriz ofrece la oportunidad de cambiar los parámetros de análisis (riesgo o impacto), además siempre será conveniente que el riesgo se defina fácilmente por la relación de la magnitud y la frecuencia (MARTÍNEZ, 2001):

$$\boxed{Riesgo = (magnitud)(frecuencia)} \quad (2.1)$$

2.2.3 Comportamiento organizacional

El estudio de este punto es garantizar que la metodología a elaborar será parametrizada a las necesidades de la empresa, pero básicamente a los empleados y a su comportamiento en la organización.

El comportamiento organizacional es un campo de estudio en el que se investiga el impacto de la conducta que individuos, grupos y estructuras tienen dentro de las organizaciones, con el propósito de aplicar los resultados en el mejoramiento de la eficacia de una organización (ROBBINS, 2004).

Dentro del comportamiento organizacional es muy importante realizar un estudio de los grupos que surgen dentro de una organización ya que esto colaborará en pleno beneficio para alcanzar las metas y los objetivos que se planteen (GONZÁLEZ, 1994).

Entre otras actividades, un grupo puede orientar y resolver problemas, explotar posibilidades o alternativas en forma creativa o ejecutar planes bien elaborados (GONZÁLEZ, 1994).

En la terminología de los sistemas, se define al grupo como: “Conjunto de sistemas de comportamiento mutuamente independientes que no sólo se afectan entre sí, sino que responden también a las influencias exteriores” (HUSE, 1980).

Stephen P. Robbins (2004), hace la siguiente clasificación de grupos:

- **Formales:** se tienen normas y estatus, esto es, que cuentan con una sanción oficial y han sido organizados por una autoridad administrativa o de otro tipo, con el propósito de que cumplan con las metas de la organización (ROBBINS, 2004).
- **Informales:** estos no tienen una estructura muy definida, a la vez que no cuentan con un estatus específico. Surgen de manera espontánea en alguna organización o grupo formal. Estos se pueden formar en razón de la amistad de los integrantes o de intereses similares (ROBBINS, 2004).
- **De Mando:** los integrantes comparten la responsabilidad de administrar el grupo u organización, para lograr con mayor eficacia las metas propuestas (ROBBINS, 2004).
- **De Tarea:** conjuntos de individuos que se forman en grupo, para plazos breves, con tiempos especificados con anterioridad a fin de realizar una singular serie de tareas o proyectos (ROBBINS, 2004).
- **De Interés:** enfocados a la búsqueda de una meta común, los integrantes de este tipo de grupo se ocupan de una o varias tareas conjuntamente y logran intereses particulares para cada uno (ROBBINS, 2004).
- **De Amistad:** los integrantes tienen características comunes entre sí, cada quien escoge a los integrantes, o bien lo hacen en conjunto (ROBBINS, 2004).

De los tipos de grupo que se han comentado anteriormente se debe analizar cuales pueden apoyar de forma más positiva la implementación de un Plan de Continuidad de Negocio.

2.2.4 Cultura Organizacional

La cultura organizacional se ha definido como "una suma determinada de valores y normas que son compartidos por personas y grupos de una organización y que controlan la manera que interaccionan unos con otros y ellos con el entorno de la organización. Los valores organizacionales son creencias e ideas sobre el tipo de objetivos y el modo apropiado en que se deberían conseguir. Los valores de la organización desarrollan normas, guías y expectativas que determinan los comportamientos apropiados de los trabajadores en situaciones particulares y el control del comportamiento de los miembros de la organización de unos con otros" (HILL, 2011).

Una de las características de la cultura organizacional es su carácter simbólico. La cultura es algo intangible, aunque sus manifestaciones sí son observables. En este sentido, la cultura de una organización está constituida por una red de símbolos o costumbres que guían y modulan, en distinto grado, los comportamientos de quienes trabajan en ella y, sobre todo, de las personas que se van incorporando. Estos elementos simbólicos se manifiestan en todos los niveles y departamentos de la organización, desde las relaciones personales y sociales hasta las normas de contabilidad. Mediante los elementos simbólicos de la cultura, la organización y sus miembros establecen procesos de identidad y exclusión (HOFSTEDE, 2010).

La cultura organizacional tiene varios efectos sobre el comportamiento de sus miembros. En primer lugar, en los procesos de atracción y selección, lo que perpetua aún más la cultura existente. También tendrá efectos sobre los procesos de retención y rotación voluntaria, de manera que en la medida que haya una mayor correspondencia entre los valores de los trabajadores y la cultura organizacional, mayor será el compromiso del trabajador hacia la organización, y menor la tasa de rotación o abandono voluntario. Los estilos de liderazgo y toma de decisiones se verán también afectados por contingencias culturales así como las conductas emprendedoras (BRETONES, 2009)

En conclusión la cultura desempeña numerosas funciones dentro de la organización. Primero, tiene un papel de definición de fronteras; es decir, crea distinciones entre una organización y las demás. Segundo, transmite un sentido de identidad a los miembros de la organización. Tercero, la cultura facilita la generación de un compromiso con algo más grande que el interés personal de un individuo. Y cuarto, incrementa la estabilidad del sistema social (ROBBINS, 2004).

2.2.5 Cultura Organizacional chilena

Diferentes estudios han planteado, desde la década de los noventa, que las características históricas y culturales de Chile han determinado que la relación tradicional entre personas y organizaciones se haya

basado en el paternalismo, la existencia de una jerarquía respetada y el conformismo (RODRÍGUEZ, 2008).

Este modelo ha sufrido importantes cambios en las últimas décadas, lo que ha llevado al planteamiento de una transición hacia una relación más impersonal y basada en la eficiencia y el mérito. Los mismos estudios han planteado una tensión entre individualismo y gregarismo. Además plantearon que en la cultura chilena es posible ser solidario, pero sin perder su centro individual. En esta dirección, Abarca, Majluf y Rodríguez (1998) plantearon que el estilo de administración chileno favorece la conducta individualista sobre formas gregarias de trabajo y participación. El individualismo sería la norma, mientras que el trabajo en equipo sería la excepción (ABARCA, 1998).

Otros estudios han destacado la alta distancia con el poder como un rasgo de la cultura latinoamericana, incluyendo a Chile. Esta distancia, en parte, sería reflejo de la distancia social entre superior y subordinado, y afectaría en prácticas como la dificultad para delegar autoridad, para descentralizar y entregar poder en la toma de decisiones (DÁVILA, 2005).

Gómez y Rodríguez (2009) indican el fuerte sentido de jerarquía presente en el contexto organizacional chileno, donde los subordinados asumen sin críticas las opiniones, mandatos e instrucciones de quienes tienen poder y se acepta ser controlado estrechamente y supervisado en aras de ser aceptado.

Además han señalado que algunos de los elementos principales de la dinámica del trabajo en Chile son:

- La existencia de gran presión de trabajo, ejercida por los jefes y gerentes.
- Foco sostenido en altos niveles de eficiencia organizacional, como un elemento aislado, que usualmente no considera a las personas.
- Inexistencia de autonomía en el trabajo y empoderamiento.
- Consideración de que la lealtad, la dedicación, la obediencia y el profesionalismo son cualidades deseadas en los trabajadores.

Rodríguez (2008) en un trabajo que se ha convertido en uno de los más importantes que se han realizado sobre cultura organizacional chilena, señaló que el modelo se encontraba en transición. Indicó, por ejemplo, la creciente aplicación de una racionalidad técnica en el proceso de reclutamiento y selección. También señaló que el trato paternalista de protección a cambio de lealtad estaba en retirada, siendo reemplazado por un modelo en que prevalece una relación impersonal, en que la racionalidad y la funcionalidad determinan el comportamiento que tendrá cada individuo en la organización. En su descripción, donde comparó el estilo latinoamericano-chileno con el japonés y el estadounidense, planteó al aumento del individualismo en las relaciones con la empresa y a la presencia de comunicaciones verticales y específicas en lo formal, complementadas con otras instancias informales amplias y grupales. Indicó además la existencia de responsabilidades difusas en los cargos y una participación casi

inexistente en la toma de decisiones, planteando que la incorporación de trabajadores más jóvenes y con mejores niveles educacionales podría hacer cambiar esa situación.

Los planteamientos presentados por todos estos autores, tienen en común que están basados en observaciones cualitativas y observadores externos a la relación laboral. Complementar estas opiniones desde la perspectiva de los ejecutivos que aplican las prácticas de gestión de personas y de los trabajadores, permitiría tener una visión global del estilo nacional, es por esto que a continuación se presenta un estudio realizado por David E. Hojman y Gregorio Pérez (2005), en el cual, se realizó una encuesta a más de 1.300 visitantes del mall Parque Arauco en el sector oriente de Santiago.

El Parque Arauco no es perfectamente representativo de la opinión nacional, porque sus clientes son de ingresos medios y altos. Pero de todas maneras, estos datos permiten formar por lo menos una idea, y en muchas preguntas el signo (positivo o negativo) del sesgo respectivo será más o menos evidente. La mayoría de los entrevistados son típicos empleados de empresas chilenas (entre las excepciones se encuentran estudiantes, dueñas de casa, empleadores, trabajadores por cuenta propia, y personas que residen en el extranjero). Los entrevistados estaban conscientes que tanto la inestabilidad económica como las nuevas tecnologías habían afectado a los empleados. Los encuestados estaban, igualmente, divididos entre aquellos que opinaban que el empleo típico ofrecía posibilidades para el desarrollo personal, y aquellos que creían lo contrario. También estaban divididos entre aquellos que pensaban que los beneficios del trabajo habían mejorado, y aquellos que creían que habían disminuido. La mayoría de los entrevistados, tres de cada cuatro, creía que el acceso al empleo dependía de amistades o contactos familiares, y no de la publicación de avisos en medios de comunicación y concursos abiertos (HOJMAN, 2005).

Resumiendo, la percepción general era de cambio corporativo e introducción de nuevas tecnologías que, sin embargo, no habían logrado beneficiar, compensar y reconocer a los empleados adecuadamente. La visión de la abrumadora mayoría era pesimista, fatalista y paternalista. La percepción que tenían los entrevistados acerca de las relaciones industriales no era particularmente buena. Un 63% pensaba que las compañías trataban a sus empleados exactamente como la ley lo ordenaba, ni mejor ni peor. Otro 31% pensaba que los empleados eran tratados como desechables o prescindibles. Solamente 5% creía que los empleados eran tratados como un recurso valioso (HOJMAN, 2005).

En cuanto a la opinión que tenían los entrevistados acerca de los empleados, tampoco era especialmente buena. El 75% de la muestra estuvo de acuerdo en que el trabajador chileno no corre riesgos; el 57%, que es flojo; el 73%, que no acepta críticas, y el 59%, que al trabajador chileno le gusta que le digan lo que hay que hacer. Pero hay que reconocer que, si es que la gerencia quiere que al trabajador le “guste” que le digan lo que hay que hacer, posiblemente a éste no le queda más remedio que “gustarle”, o pretender que le “gusta” (HOJMAN, 2005).

Finalmente gracias a la información anteriormente mencionada, se pueden conseguir bastantes datos que logren favorecer la implementación y mantenimiento de un Plan de Continuidad de Negocio en Chile, como por ejemplo la forma en la que se debe entregar las tareas y obligaciones a los demás, las cuales deben ser de una forma impersonal y formal, también la importancia de la delegación de autoridad y toma de decisiones, con lo cual se busca obtener que los colaboradores se sientan parte de la empresa y como un recurso valioso para la misma.

2.2.6 Liderazgo

Debido a que el Plan de Continuidad de Negocio (BCP) es un proceso que se trabaja en gran parte de forma teórica y que se basa principalmente en la concientización que se logre entre los empleados, ya que durante su trabajo diario deben elaborar ciertas tareas que apoyen al BCP, es fundamental que el responsable posea liderazgo frente al grupo que participa en el Plan (BASS, 1997).

Existe un modelo para evaluar el comportamiento del liderazgo en las organizaciones, llamado Inventario de las prácticas de Liderazgo elaborado por James Kouzes y Barry Posner (2007), el análisis del liderazgo se lleva a cabo por medio de la evaluación de cinco comportamientos (KOUZES, 2007):

- **Desafiar los procesos:** El líder se hace responsable de los riesgos que conllevan los procesos administrativos y operativos, además de la dinámica interna y externa que juegan los procesos (KOUZES, 2007).
- **Inspirar una visión compartida:** Se refiere a la imaginación apasionante del líder sobre escenarios futuros (KOUZES, 2007).
- **Habilitar a los demás a que actúen:** Esta característica se refiere a la facultad del líder para desarrollar un ambiente participativo y cooperativo, haciendo del equipo de trabajo, compañeros pro-activos (KOUZES, 2007).
- **Modelar el camino:** Se refiere a una alta jerarquía de valores y de igual forma una alta moralidad. Coloquialmente podría decirse: “El líder predica con el ejemplo” (KOUZES, 2007).
- **Dar aliento con el corazón:** Es un comportamiento transaccional integrado en el Inventario de las prácticas de liderazgo. Este comportamiento se refiere a la retroalimentación positiva que el líder da a los seguidores, reconociendo públicamente las contribuciones individuales y celebrando los logros del equipo (KOUZES, 2007).

De acuerdo a los puntos citados anteriormente, se puede hacer una selección de la persona más idónea para el cargo de Coordinador del Plan de Continuidad de Negocio.

- **El liderazgo como función dentro de la Organización**

Operacionalmente, un grupo tiende a actuar o hablar a través de uno de sus miembros, cuando todos tratan de hacerlo simultáneamente el resultado por lo general es confuso o ambiguo. La necesidad de un

líder es evidente y real, y esta aumenta conforme los objetivos del grupo son más complejos y amplios (DAFT, 2006).

Por ello, para organizarse y actuar como una unidad, los miembros de un grupo eligen a un líder. Este individuo es un instrumento del grupo para lograr sus objetivos y, sus habilidades personales son valoradas en la medida que le son útiles al grupo (GIL, 1990).

Como el liderazgo está en función del grupo, es importante analizar no solo las características de este sino también el contexto en el que el grupo se desenvuelve. Pues se considera que estas características determinan quien se convertirá en el líder del grupo (GIL, 1990).

Dependiendo si la situación requiere acción rápida e inmediata o permite deliberación y planeación, los liderazgos pueden caer en personas diferentes (GIL, 1990).

En síntesis, " el líder es un producto no de sus características, sino de sus relaciones funcionales con individuos específicos en una situación específica" (DAFT, 2006).

- **Características de un líder**

En la dirección de las organizaciones se encuentran las elites formada por líderes.

Se identifica al líder por las siguientes características (DAFT, 2006):

- El líder debe tener el carácter de miembro del grupo, es decir, debe pertenecer al grupo que encabeza, compartiendo con los demás miembros los patrones culturales y significados que ahí existen (DAFT, 2006).
- La primera significación del líder no resulta por sus rasgos individuales únicos, universales (estatura alta o baja, aspecto, voz, etc.) (DAFT, 2006).
- Sino que cada grupo considera líder al que sobresalga en algo que le interesa, o más brillante, o mejor organizador, el que posee más tacto, el que sea más agresivo, más santo o más bondadoso. Cada grupo elabora su prototipo ideal y por lo tanto no puede haber un ideal único para todos los grupos (DAFT, 2006).
- En cuarto lugar. El líder debe organizar, vigilar, dirigir o simplemente motivar al grupo a determinadas acciones o inacciones según sea la necesidad que se tenga (DAFT, 2006).

Estas cuatro cualidades del líder, son llamadas también carisma.

- Por último, otra exigencia que se presenta al líder es la de tener la oportunidad de ocupar ese rol en el grupo, si no se presenta dicha posibilidad, nunca podrá demostrar su capacidad de líder (DAFT, 2006).

2.3 Metodologías y estándares para la elaboración de un Plan de Continuidad de Negocio

En este punto se presentan algunas de las Metodologías que existen actualmente sobre Continuidad del Negocio desde diferentes enfoques y entre los documentos que pueden servir de apoyo en la elaboración del Plan de Continuidad de Negocio, se tienen estándares que son reconocidos a nivel mundial. Los estándares son avalados por instituciones especializadas en el tema de Continuidad de Negocio. En las páginas siguientes se analizan cada una de las metodologías.

A continuación en la Tabla Nº 2.4, se pueden observar los datos generales de las metodologías utilizadas a nivel mundial de continuidad de negocio, las cuales se explican en los puntos siguientes.

Tabla Nº 2.4: Datos Generales de las metodologías de BCP.

Organización	Estándar y/o Metodología	Alcance	Año de Actualización	Origen
BSI	BS 25999-1 BS 25999-2	BCM (Business Continuity Management)	2007	Inglaterra
BSI	BS 25777	ITDR (Information Technology Disaster Recovery)	2008	Inglaterra
BCI	Guía de las Buenas Prácticas	BCM identificando el ITDR como estrategia	2008	USA
ITIL	Gestión de la continuidad del servicio	Gestión de Servicios Informáticos	2007	Inglaterra
DRJ	Emergency Operation Center (EOC)	Centro alterno de operaciones para BCM como para ITDR	2012	USA
DRI DRJ	Prácticas Generalmente Aceptadas	BCM	2007	USA
National Fire Protection Association	NFPA 1600	BCM	2013	USA
ISO	ISO 27002	Seguridad de la información	2005	Ginebra (Suiza)
ISO	ISO 22301	BCM	2012	Ginebra (Suiza)

Fuente: Elaboración propia.

Como muestra la Tabla N º 2.4, las metodologías han surgido en diferentes zonas geográficas, por lo cual es importante analizarlas en detalle para identificar los puntos de cada una que pueden aplicarse en Chile. Las diferentes metodologías fueron escritas cada una enfocada a diferentes situaciones, como comunicación de crisis, tecnología, procesos de negocio y sitio alterno entre otras, debido a esto es importante estudiar cada una de ellas, con la finalidad de identificar el tema en el que cada una se especializa y de esta forma, fortalecer la metodología que se diseñará para ser aplicada en Chile.

2.3.1 BS 25999

La norma británica BS 25999 de la Institución Británica de Normas, toma la idea de un plan de continuidad de negocios y amplía su alcance para abarcar en su totalidad a la compañía. BS 25999 está dividida en dos partes: BS 25999-1 y BS 25999-2. La BS 25999-1, o Código de Práctica fue publicado en diciembre de 2006 y es un documento general que explica el propósito de la norma, es básicamente un documento orientativo que proporciona las recomendaciones prácticas para las el BCP. BS 25999-2, o la especificación, fue liberada en noviembre de 2007 y establece los requisitos para un Sistema de Gestión de la Continuidad (BCM). Esta es la parte de la norma que se certifica a través de una etapa de implementación, de auditoría y posterior certificación (PJR, 2013).

El estándar proporciona una breve introducción de lo que es la Continuidad de Negocio, explica porque las organizaciones deben contar con un Plan de Continuidad de Negocio detallando los beneficios que se adquieren con la implantación de éste. Además explica la importancia de contar con un Análisis de riesgos y como ayuda éste al Plan de Continuidad de Negocio. Las etapas que el estándar maneja, son conocidas como el ciclo de vida del BCP, el cual se puede observar en la Figura Nº 2.1.

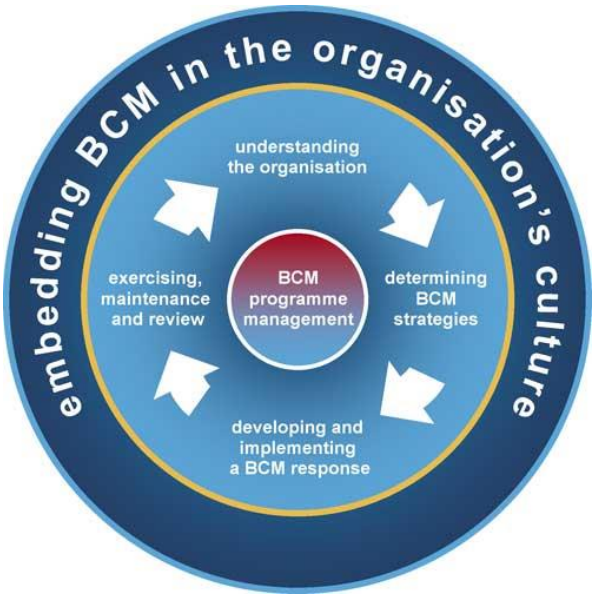

Figura Nº 2.1: Ciclo de vida del Plan de Continuidad de Negocio.

Fuente: BS 25999-1, 2006.

A continuación se explican brevemente las etapas de este ciclo de vida (BS 25999-1: 2006):

- **Plan de Administración de Continuidad de Negocio:** Establece la importancia de contar con una administración del Plan de Continuidad de Negocio, en el que se lleve el monitoreo de todas las actividades que integran el Plan y que permita identificar desde una forma general los puntos que falta especializar (BS 25999-1: 2006).
- **Entendiendo la organización:** Uno de los puntos iniciales y más importantes para realizar el BCP es conocer y entender de forma detallada el negocio al que se dedica la organización, para así obtener como resultado un plan de continuidad óptimo .Es en esta fase dónde se aplica el Análisis de Impacto al Negocio (Business Impact Analysis, BIA por sus siglas en inglés), se determina el Tiempo Objetivo de Recuperación (RTO por sus siglas en inglés) y el Punto Objetivo de Recuperación (RPO por sus siglas en inglés) (BS 25999-1: 2006).
- **Determinando la estrategia de Continuidad de Negocio:** Plan de Recuperación de Tecnología en caso de Desastre, sitios alternos para la recuperación de tecnología y para la continuidad de las operaciones, estrategias para el trabajo desde casa, un Plan de Comunicación interna y externa durante y después del incidente, respaldo de información en otro sitio, etc. (BS 25999-1: 2006).
- **Implementación de un programa de responsabilidades para la Continuidad de Negocio: I**dentificar el equipo para la Continuidad de Negocio y cuáles son las actividades que deben realizar frecuentemente, para estar preparados en cualquier momento ante una crisis. Así, como las tareas que se deben realizar cuando el incidente sea declarado. En esta etapa se identifica el equipo de Administración de Crisis y el equipo de Administración de Incidentes (BS 25999-1: 2006).
- **Pruebas y mantenimiento del Plan de Continuidad de Negocio:** Es de vital importancia realizar pruebas para determinar la eficacia con la que puede continuar el negocio ante la presencia de una posible interrupción, además el proceso de mantenimiento del plan es trascendental, para obtener un Plan de continuidad de negocio actualizado y vigente, considerando que el negocio continúa y está en constante cambio. En esta fase se detalla la importancia de probar los planes que se han desarrollado para verificar la capacidad que tiene y encontrar mejoras que puedan ayudar a aumentar el nivel de madurez del Plan de Continuidad de Negocio (BS 25999-1: 2006).
- **Desarrollando una cultura de Continuidad de Negocio**: Esta fase busca desarrollar en todos los empleados de la organización, la concienciación de que la organización puede tener en cualquier momento algún incidente que interrumpa la operación normal de la empresa, ante lo cual se debe estar preparados psicológica, tecnológica y técnicamente para poder dar continuidad al negocio con los recursos que cuenta la empresa, (BS 25999-1: 2006).

Cada una de las fases que se han descrito de forma breve, sirven para formar la base de la metodología propuesta para el presente trabajo de grado, esto debido a la forma tan completa del Estándar BS-25999.

2.3.2 BS 25777

En muchas organizaciones, la ejecución de los procesos críticos depende de los servicios de información y tecnología de comunicaciones, definido en el BS 25777 como ICT (Information and Communications Technology) (BS 25777: 2008).

La finalidad del BS 25777 es apoyar a las organizaciones a implementar una correcta estrategia para los servicios de información y tecnología de comunicaciones. Los principios que componen el estándar son (BS 25777: 2008):

- **Protección:** El análisis de los servicios de información y comunicación permiten conocer las amenazas y vulnerabilidades, identificando con ello, los riesgos que pueden aminorarse (BS 25777: 2008).
- **Detección:** Este principio se refiere a identificar los servicios que soportan los procesos claves del negocio, para tenerlos como prioridad para su recuperación (BS 25777: 2008).
- **Reacción:** Mediante la planeación de un programa de continuidad como el ICT, se logra la reacción de la organización ante los incidentes, minimizando así, el Downtime (BS 25777: 2008).
- **Recuperación:** Sobre los requerimientos del negocio de las tecnologías de información y los tiempos en que se requieren, se puede definir un plan de acción sobre las tecnologías que se recuperan primero y las que se recuperarán después (BS 25777: 2008).
- **Operación:** Este principio se refiere a dar soporte a la operación contingente que la empresa desarrolle después de la ocurrencia del incidente (BS 25777: 2008).
- **Regreso:** El ICT hace énfasis a lograr la operación del negocio después de un incidente, pero es necesario diseñar la mejor estrategia para migrar la operación de la organización de regreso al Edificio principal (BS 25777: 2008).

El ICT debe contar con algunos elementos que le permitan desarrollarse de la mejor manera, estos son (BS 25777: 2008):

- **Personal:** Además de apoyar en la operación diaria, el personal de Tecnologías de Información y Comunicaciones debe empezar a desarrollar las habilidades para apoyar en caso de un escenario de contingencia. Esto se logra a través de la capacitación y práctica del ICT (BS 25777: 2008).
- **Localidades:** Se debe identificar el equipo necesario para llevar a cabo la restauración de las tecnologías de información así como los lugares alternos que se utilizaran en un escenario de contingencia (BS 25777: 2008).

- **Tecnología:** Dentro de la tecnología pueden identificarse algunos rubros como (BS 25777: 2008):

    - Servidores, forma de respaldos de la información, medios de almacenamiento de información que se utilizan y cualquier otro hardware necesario para la recuperación.
    - Redes, servicios de voz, switches y routers.
    - Software, incluyendo las aplicaciones de terceros utilizados en la operación normal, en este punto se debe tener claramente identificadas las relaciones lógicas entre aplicaciones.
    - Información, este punto cuida que cualquier tipo de información necesaria para la recuperación se tenga lista, siempre cuidando la confidencialidad, integridad y disponibilidad.
    - Procesos, se refiere a tener bien definido y detallado un programa que permita recuperar los servicios de información con tan sólo tener servidores y equipos de cómputo en blanco. Empezando desde la instalación del Sistema Operativo.
    - Proveedores, otro componente para que los servicios que ofrece el área de Tecnologías de Información y Comunicaciones se puedan mantener continuos aún después de ocurrido un incidente, son los proveedores especializados en el área como el carrier de internet, proveedores de telefonía, entre otros (BS 25777: 2008).

El BS 25777: 2008, resulta ser un estándar altamente efectivo en el área de IT, pues está completamente detallado para no perder de vista ningún punto. Además tiene la ventaja que esté alineado al BS 25999-1: 2007 de la misma institución, y el cual, está enfocado a los procesos del negocio, es por esto que este estándar, juega un papel crucial al momento de desarrollar los planes de contingencias tecnológicos, pertenecientes al Plan de Continuidad Operacional.

2.3.3 ITIL

La Biblioteca Infraestructuras de Tecnologías de la Información (ITIL), contiene un punto que es muy interesante para la formulación del Modelo de Plan de Continuidad de Negocio y se encuentra en el apartado llamado Gestión de Continuidad de servicios de TI (ITSCM por sus siglas en ingles)**,** que tiene los siguientes objetivos (OSIATIS, 2013):

- Garantizar la pronta recuperación de los servicios (críticos) de TI tras un desastre.
- Establecer políticas y procedimientos que eviten, en la medida de lo posible, las perniciosas consecuencias de un desastre o causa de fuerza mayor.

ITSCM está dirigido al área responsable de la información, buscando garantizar una rápida recuperación de los servicios críticos de TI (Tecnologías de Información) después de un incidente.

Dentro de la Continuidad de Negocio es indispensable elaborar un estudio de Riesgos. ITIL con la Gestión de Continuidad del Servicio tiene una forma de llevar a cabo una Gestión y Análisis de Riesgos, para lo cual se basa en la siguiente Figura Nº 2.2 (OSIATIS, 2013):

Figura Nº 2.2: Gestión y Análisis de Riesgos.
Fuente: OSIATIS, 2013.

Actividades propuestas por ITIL (OSIATIS, 2013):

- Establecer las estrategias de continuidad del servicio TI.
- Adoptar medidas proactivas de prevención del riesgo.
- Desarrollar los planes de contingencia.
- Poner a prueba dichos planes.
- Formar al personal sobre los procedimientos necesarios para la pronta recuperación del servicio.
- Revisar periódicamente los planes para adaptarlos a las necesidades reales del negocio.

De acuerdo con ITIL cuanto mayor sea el impacto asociado a la interrupción de un servicio, mayor debe ser el esfuerzo para la prevención.

Estudiando a detalle cada uno de los puntos que marca ITIL se pueden obtener beneficios para el Plan de Recuperación de Tecnología en caso de Desastre, siempre que puedan implementarse con los recursos existentes.

2.3.4 NFPA 1600

The North American Business Continuity Standard publica la Norma NFPA 1600, que es otro punto de vista sobre cómo puede llevarse a cabo el tema de Continuidad de Negocio y cada una de sus fases (NFPA, 2013).

La norma NFPA 1600, presenta los siguientes puntos indispensables para la efectiva Administración de Continuidad de Negocio (NFPA, 2013):

- **Programa de Administración**. Documentar cuál es la visión y misión del Plan de continuidad de Negocio. Establecer un formato para registrar los objetivos del personal que participa en el programa y hacer revisiones periódicas que permitan monitorear el avance, cumplimiento y evaluación de los objetivos (NFPA, 2013).
- **Leyes y autoridades.** En esta fase se identifican las leyes y regulaciones a las cuáles se debe alinear el Programa de Continuidad del Negocio (NFPA, 2013).
- **Evaluación de Riesgos.** El estándar enfatiza en esta fase la correcta identificación de riesgos, es decir, naturales, humanos y tecnológicos (NFPA, 2013).
- **Prevención de Incidentes.** Esta fase se indica el desarrollo de una estrategia para prevenir incidentes de acuerdo a los recursos humanos, infraestructura y presupuesto que se tenga asignado al proyecto (NFPA, 2013).
- **Mitigación.** Se deben identificar los riesgos que pueden ser eliminados e implementar la mejor estrategia que permita terminar con ellos (NFPA, 2013).
- **Administración de recursos y logística.** En esta fase se definen los procedimientos para la traslación al sitio alterno, en caso de requerirse, en que tiempos se debe ir trasladando cada equipo de recuperación de tecnología o continuidad de operaciones. Se establece con el proveedor de recursos de papelería sobre el lugar y horario de atención (NFPA, 2013).
- **Asistencia y ayuda mutua.** Se debe especificar el nivel de servicio y atención de los proveedores en caso de contingencia (NFPA, 2013).
- **Planeación.** Para cada contacto que se identifique, que deba realizar alguna actividad en un escenario de contingencia, se debe tener bien definida una línea de comunicación con el proveedor o dependencia, con nombres, números de teléfono y correo electrónico (NFPA, 2013).
- **Administración de incidentes.** Contar con una política en el que se identifiquen las responsabilidades, los procedimientos para realizar la recuperación de tecnologías de información y dar continuidad a la operación del negocio (NFPA, 2013).
- **Comunicados y alertas.** Establece la implementación de protocolos, software, procesos y pruebas periódicas de los mismos protocolos. En este punto, la organización determina las necesidades de comunicación (NFPA, 2013).
- **Instalaciones.** Identificar y documentar la ubicación de los sitios con los que cuenta la organización, tanto de operación normal, como sitio alterno y alguna otra ubicación que se utilice para que el personal reanude operaciones críticas en estado de contingencia (NFPA, 2013).
- **Entrenamiento y capacitación.** EL plan de capacitación debe buscar en todo momento, el desarrollo, implementación, mantenimiento y ejecución del plan. La frecuencia y alcance debe quedar clara en el Programa (NFPA, 2013).

- **Ejercicios, evaluación y acciones correctivas.** Los ejercicios deben estar dirigidos a ejercicios diferentes en cada prueba, esto, con la intención de probar el plan ante diversas situaciones que han sido definidas en las fases anteriores (NFPA, 2013).
- **Comunicación de crisis e información pública.** El equipo de comunicación corporativa debe tener un plan para elaborar comunicados externa e internamente, que tipo de información puede publicar, como deben estar escritos los mensajes que se publiquen, en que medios, en fin, toda una campaña publicitaria que se active con el escenario de contingencia (NFPA, 2013).
- **Finanzas y Administración**. Para la Administración y finanzas del Proceso de continuidad del negocio es importante marcar un antes, un ahora y un después del incidente. Es importante hacer la planeación para contar con una reserva destinada a este programa (NFPA, 2013).

Esta norma puede servir para reforzar algún punto del Plan de Continuidad de Negocio. Como se puede observar, la Norma NFPA 1600 está enfocada al tema de la seguridad de los empleados y de la misma organización. Algunas de las fases pueden ayudar a fortalecer las fases de comunicación entre empleados en un escenario de contingencia y administración de incidentes principalmente.

2.3.5 ISO 27002

La norma ISO 27002 es un código de prácticas para la seguridad de la información. La base de la norma fue originalmente un documento publicado por el gobierno del Reino Unido, que se convirtió en un estándar "adecuado" en el año 1995, cuando fue re-publicada por BSI según BS 7799. En el año 2000 de nuevo se volvió a publicar, esta vez por la ISO, como ISO 17799. Una nueva versión de ésta apareció en el año 2005, junto con una nueva publicación, la norma ISO 27001 (DIRECTORIO ISO 27000, 2013).

La versión de 2005 del estándar incluye las siguientes 11 secciones principales (ISO 27002: 2005):

1) Política de Seguridad de la Información.
2) Organización de la Seguridad de la Información.
3) Gestión de Activos de Información.
4) Seguridad de los Recursos Humanos.
5) Seguridad Física y Ambiental.
6) Gestión de las Comunicaciones y Operaciones.
7) Control de Accesos.
8) Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.
9) Gestión de Incidentes en la Seguridad de la Información.
10) Gestión de Continuidad del Negocio.
11) Cumplimiento.

La sección más interesante para el presente trabajo de grado se centra básicamente en Gestión de la Continuidad de Negocio, en el cual se integran aspectos de seguridad de la información de la Gestión de

la Continuidad de Negocio. Este dominio tiene la finalidad de contrarrestar la operación del negocio y proteger los procesos críticos ante desastres y fallas menores en los sistemas de información. Con esto se asegura el restablecimiento oportuno.

Dentro del Dominio Gestión de la Continuidad del Negocio se solicitan algunos puntos como:

- **Incluir la seguridad de la información en el proceso de Gestión de Continuidad del Negocio.** Las actividades relacionadas a esta fase son (ISO 27002: 2005):
    - Comprender los riesgos de la organización, identificar y priorizar, los procesos críticos.
    - Identificar los activos implicados en los procesos críticos.
    - Comprender el impacto que tendrían las interrupciones del Negocio.
    - Considerar la contratación de seguros adecuados.
    - Considerar la implementación de controles adicionales a la prevención.
    - Identificar recursos financieros, organizacionales y técnicos.
    - Asegurar la seguridad de los empleados en las instalaciones.
    - Formular y documentar los planes.
    - Probar y actualizar los planes.
    - Asegurar la incorporación del BCM a los procesos de la organización. Asignar a un responsable.

- **Elaboración del análisis de riesgo.** Basa su principio en identificar los eventos que pueden ocasionar una interrupción en los procesos del negocio, igual que su probabilidad de impacto. Para cumplir con el objetivo de esta sección se deben realizar las siguientes tareas (ISO 27002: 2005):
    - Identificar los Eventos.
    - Evaluar el riesgo determinando la probabilidad e impacto del evento.
    - Desarrollar un plan basándose en los resultados del Análisis de Riesgos.
    - Crear una estrategia sólida.

- **Desarrollar planes de continuidad del negocio incluyendo aspectos de seguridad de la información.** En esta fase se identifican procedimientos de emergencia y acuerdos sobre las responsabilidades. Algunos otros puntos que se consideran en esta fase son (ISO 27002: 2005):
    - Identificación de pérdidas aceptables de información y servicios.
    - Implementación de procedimientos que permitan la recuperación y restauración de las operaciones del negocio, dependencias internas y externas.
    - Documentación de procedimientos.
    - Formación del personal del área de tecnologías de información para desarrollar la capacidad de implementar los procedimientos.

- Desarrollar en el personal la prueba y mantenimiento de los planes.

- **Alinearse al marco referencial para la planeación de continuidad del negocio.** El marco referencial indica tener identificadas ciertas tareas (ISO 27002: 2005):
  - Condiciones para activar los planes y las tareas a realizar antes de la activación.
  - Descripción de tareas que deben realizarse tras la ocurrencia de un incidente.
  - Procedimiento para realizar un respaldo de información.
  - Calendario de mantenimiento.
  - Actividades para efectuar la capacitación.
  - Responsabilidades de las personas.
  - Recursos críticos necesarios.

- **Prueba, mantenimiento y actualización de los Planes de Continuidad del Negocio.** La prueba de los Planes de continuidad se lleva a cabo con la finalidad de verificar su vigencia y eficiencia. Para este punto deben considerarse algunas actividades importantes (ISO 27002: 2005):
  - Identificación y prueba de varios escenarios.
  - Desarrollar simulacros para entrenar al personal.
  - Desarrollar pruebas de Recuperación en un lugar alterativo.
  - Pruebas de servicios de proveedores en el lugar alterno.

El estándar está enfocado mayormente a la información, por lo que puede ser de gran ayuda para el Plan de Continuidad de Negocio al momento de tomar en cuenta la continuidad de la seguridad que la información debe tener.

2.3.6 ISO 22301

La norma ISO 22301 es, a nivel mundial, la primera norma internacional para la gestión de la continuidad de negocio (GCN) y ha sido desarrollada para ayudar a las organizaciones a minimizar el riesgo de sufrir interrupciones. La estandarización de la continuidad de negocio evoluciona con ISO 22301, tomando como base la norma BS 25999-2 y agregando (BSI GROUP, 2013):

- Mayor énfasis en el establecimiento de objetivos, seguimiento del desempeño y de los indicadores.
- Expectativas más claras sobre la Dirección.
- Planificación y preparación más cuidadosas de recursos requeridos para el aseguramiento de la continuidad de negocio.

Las clausulas claves de la norma son las siguientes (ISO 22301: 2012):

- **Contexto de la organización:** Determinar temas internos y externos que son relevantes para el propósito de la organización y que afectan su habilidad de alcanzar los resultados esperados de su SGCN. Identificar el alcance del SGCN, tomando en cuenta los objetivos estratégicos de la organización, sus productos y servicios claves, su tolerancia al riesgo y cualquier obligación reglamentaria, contractual o de sus partes interesadas, también forma parte de esta cláusula (ISO 22301: 2012).
- **Liderazgo:** La alta dirección debe demostrar un compromiso continuo con el SGCN, a través de su liderazgo y acciones. La dirección puede crear un ambiente en el cual distintos miembros del personal estén completamente involucrados y el sistema de gestión pueda funcionar de manera eficaz en sinergia con los objetivos de la organización. Una tarea clave es designar un coordinador/líder que se encargará de gestionar y supervisar el proceso de elaboración e implementación del plan de continuidad de negocio, e incluso, si la inversión lo permite y en función del tamaño de la organización y el alcance del plan, es recomendable asignar personal adicional y constituir un equipo de continuidad de negocio (ISO 22301: 2012).
- **Planificación:** Esta es una etapa crítica en la que se establecen objetivos estratégicos y principios para la orientación del SGCN en su totalidad. Los objetivos del SGCN son una expresión del propósito de la organización para el tratamiento de los riesgos identificados y/o para cumplir con los requisitos de las necesidades de la organización (ISO 22301: 2012).
- **Soporte:** La gestión diaria de un sistema de gestión de la continuidad de negocio, se basa en el uso de recursos apropiados para cada actividad. Estos recursos incluyen personal competente en base a formaciones y servicios de soporte, toma de conciencia y comunicación pertinentes (y demostrables), esto debe ser apoyado por información documentada adecuadamente gestionada. Las comunicaciones, tanto internas como externas, deben ser consideradas en esta área, incluyendo su formato, contenido y el momento oportuno de estas comunicaciones. Los requisitos para la creación, actualización y control de la información documentada, también se especifican en esta cláusula (ISO 22301: 2012).
- **Evaluación del desempeño:** Una vez que el SGCN se ha implementado, la norma ISO 22301 requiere un permanente seguimiento del sistema, así como revisiones periódicas para mejorar su operación (ISO 22301: 2012).
- **Mejora:** La mejora continua puede ser definida como todas las acciones, realizadas a lo largo de la organización, para aumentar la eficacia (cumplir objetivos) y la eficiencia (proporción costo/beneficio óptima) de los procesos y controles de seguridad para brindar más beneficios a la organización y a sus partes interesadas. Una organización puede mejorar continuamente la eficacia de su sistema de gestión a través del uso de la política de continuidad de negocio, los objetivos, los resultados de auditorías, el análisis de eventos controlados, los indicadores, las acciones correctivas y preventivas y la revisión por la dirección (ISO 22301: 2012).

En conclusión ISO 22301 no es tan diferente de la BS 25999 en la mayoría de los aspectos más importantes de la continuidad del negocio, como el análisis del impacto y la estrategia o la planificación. Los principales cambios se encuentran en la parte de gestión de la norma ISO 22301, ya que esta sitúa más énfasis en la comprensión de los requisitos, el establecimiento de los objetivos y en la medición del desempeño. Por lo tanto, será aceptada más fácilmente por la alta gerencia que, al mismo tiempo, contribuirá con la aceptación más generalizada de esta norma, como ISO 27001, ISO 9001 o ISO 14001.

2.4 Buenas Prácticas para la elaboración de un Plan de Continuidad de Negocio

Entre los documentos que existen en el mercado para apoyo a la elaboración de un Plan de continuidad del negocio, se cuenta con Buenas Prácticas elaboradas por instituciones con reconocimiento a nivel mundial. Las buenas prácticas para la continuidad del negocio más actuales se comentan a continuación:

2.4.1 Guía de Buenas Prácticas (GPG)

La Guía de buenas prácticas de Continuidad de Negocio o conocido internacionalmente como Good Practice Guidelines (GPG) del Business Continuity Institute (BCI), entrega entre otras cosas una introducción sobre lo que significa contar con un Plan de Continuidad de Negocio, cuales son los beneficios de tener implementado un Plan de Continuidad de Negocio en la organización y la relación que hay entre el BCP y otras disciplinas especialistas (BCI, 2010).

Además el BCI considera de gran importancia la analogía que existe entre Gestión de riesgos y la Gestión de Continuidad de Negocio a través de la siguiente Tabla Nº 2.5:

Tabla Nº 2.5: Cuadro comparativo de la Gestión de Riesgos v/s Gestión de Continuidad de Negocio.

	Gestión de Riesgos	Gestión de Continuidad de Negocio
Métodos Claves	Análisis de Riesgo.	Análisis de impacto en el Negocio.
Parámetros Claves	Impacto y probabilidad.	Impacto y tiempo.
Tipo de incidente	Todo tipo de eventos, aunque por lo general segmentados.	Eventos que causan interrupciones significativas en el Negocio.
Tamaño de los eventos	Todos los tamaños de eventos, aunque por lo general segmentados.	Las estrategias están previstas para hacer frente a los incidentes que amenazan la supervivencia, pero puede manejar cualquier tamaño de incidente.
Alcance	Se centran principalmente en la gestión de los riesgos para los principales objetivos de negocio.	Se centran principalmente en la gestión de incidencias en su mayoría fuera de las competencias básicas de la empresa
Intensidad	Todos, de gradual a repentino.	Eventos repentinos o de rápida respuesta (aunque también puede ser apropiado si el incidente que se arrastra es severo).

Fuente: BCI, 2010.

La Gestión de Riesgos es una administración holística de todos los riesgos importantes. Simplificando, es la vista e identificación de riesgos a través de toda la organización y los pasos que son tomados para manejar dichos riesgos (ESCALERA, 2011).

La Gestión de la Continuidad de Negocio por su parte es una iniciativa administrativa continua, que incluye políticas y procesos ligados a los objetivos estratégicos de la organización, para prepararse profesionalmente con el fin de sobrevivir a interrupciones y continuar o reanudar operaciones de negocio diarias, especialmente en eventos considerados por la organización como desastres (ESCALERA, 2011).

La Guía de buenas prácticas menciona algunos componentes que forman una parte muy importante dentro del Plan de Continuidad de Negocio, estos, se muestran en la siguiente Tabla Nº 2.6:

Tabla Nº 2.6: Componentes de la Guía de buenas prácticas

Guía de Componentes	Preguntas a contestar
Introducción	
Precursores	¿Qué hay que hacer antes de esto?
Propósito	¿Por qué tenemos que hacer esto? ¿Qué se va a lograr?
Conceptos y supuestos	¿Qué es lo que tenemos que entender? ¿Qué suposiciones estamos haciendo?
Procesos	¿Qué tenemos que hacer?
Métodos y técnicas	¿Cuáles son las herramientas que necesitamos para hacerlo?
Resultados y entregables	¿Qué debe producir?
Revisar	¿Cuándo se debe hacer?

Fuente: BCI, 2010.

Como se puede observar en la Tabla Nº 2.6, la GPG está estructurada de forma consciente, cada una de las secciones, responde a un cuestionamiento específico, de esta forma, al integrar los componentes: introducción, precursores, alcance, conceptos, procesos, métodos y técnicas, entregables y revisiones, se obtiene un documento completo en su contenido y fácil de entender.

La guía está formada por seis secciones identificadas como:

1) **Política de BCP y Programa de Administración.** La Política de Continuidad de Negocio es un instrumento general para cumplir los objetivos, son los mecanismos puntuales para que funcione bien una actividad de la empresa, además sin políticas no existe un rumbo claro en la organización, es decir se navega sin guía y sin rumbo fijo, los puntos que toca principalmente van enfocados a (BCI, 2010):
   - Asegurar que el programa de BCP esté alineado a los objetivos y cultura de la organización.
   - Establecer el alcance del Plan de continuidad del negocio.
   - Identificar roles y responsabilidades.

2) **Entendimiento de la organización.** Está sección responde a las preguntas: ¿cuáles son los objetivos de la organización? y ¿cómo alcanza la organización sus objetivos? Las respuestas a estas preguntas se obtienen mediante el BIA (Análisis de Impacto al Negocio), el cual además ayuda a identificar (BCI, 2010):
   - Funciones operativas como servicio al cliente, ventas y producción.
   - Funciones de soporte Tecnologías de información, Recursos humanos y servicios externos.
   - Estrategias como administración, proyectos y planeación.

3) **Determinando la estrategia de continuidad del negocio.** En vez de esperar a que un desastre golpee a la organización para ver cómo esta se recupera, las medidas preventivas deben ser aplicadas con el objetivo de incrementar la fortaleza de sus actividades frente a posibles impactos previamente identificados en el BIA. En esta fase se habla de la importancia de contar con un sitio alterno que se encuentre a una hora de distancia del edificio principal. Para comenzar con esta sección, se utiliza como entrada, el resultado del BIA, en el, se identifican los tiempos objetivos de recuperación (RTO por sus siglas en ingles) de las actividades críticas y se determinan los recursos que posee la organización para poner en práctica el Plan de Continuidad de Negocio (BCI, 2010).

4) **Desarrollo e implementación de responsabilidades.** Es muy importante definir las responsabilidades de cada participante, antes, durante y después de la contingencia. Con esto se logra que en un estado crítico dónde la situación se torne difícil, los participantes tengan una idea de lo que deben hacer para apoyar que la operación se lleve de forma adecuada. Cómo principales objetivos, esta fase busca obtener (BCI, 2010):
   - Procedimientos de clasificación de incidentes dentro de la organización.
   - Comunicación con socios del negocio.
   - Planes de trabajo para las actividades que fueron interrumpidas.

5) **Probar, dar mantenimiento y revisión del programa de continuidad del negocio.** Algunos de los objetivos que persiguen las auditorias son: validar el cumplimiento de la organización sobre los estándares y políticas existentes, verificar que los incidentes de las pruebas sean resueltas y verificar que se le esté dando mantenimiento continuo al Programa de Continuidad del Negocio. Para las pruebas, debe formularse un plan de pruebas, en el cuál se identifiquen cada uno de los recursos necesarios para poder dar continuidad a los procesos críticos. Estos recursos pueden ser: el personal designado a cada actividad, telefonía, tecnología, entre otros (BCI, 2010).

6) **Desarrollando una cultura de continuidad del negocio en la organización.** La finalidad de la elaboración de un Plan de Continuidad del Negocio se debe a la necesidad de que los empleados estén sensibilizados a que la organización es vulnerable, como todas las demás, a sufrir algún tipo de incidente que tenga como consecuencia, la interrupción de la operación normal (BCI, 2010).

2.4.2 Centro de Operaciones de Emergencia (EOC)

Además de los estándares existentes, también se encuentra el Disaster Recovery Journal (DRJ), que es una editorial dedicada totalmente al estudio de desastres, así como ayudar a determinar las estrategias más adecuadas para su prevención o solución. Por la importancia que tiene el Centro de Operaciones de Emergencia, conocido internacionalmente como Emergency Operations Center (EOC) o denominado también como sitio alterno, es necesario tomarlo en cuenta para la metodología que propone este trabajo de grado (DRJ, 2012).

En el caso de que una amenaza llegue a materializarse, el EOC apoya a la continuidad de las operaciones de la empresa. El documento publicado por DRJ, marca los lineamientos que deben cumplirse para activar un Centro de operaciones para la Continuidad del Negocio, las funciones que tendrá la organización en caso de declararse el estado de contingencia y de esta forma puede ser una ayuda para el ITDR (Information Technology Disaster Recovery), pues se pueden tomar de él tips sobre los requerimientos de tecnología que pueda tener el negocio e identificar de que forma el Área de Sistemas, en base a los recursos con los que cuenta, puede apoyar a las áreas del negocio (DRJ, 2012).

Adicionalmente el EOC proporciona las siguientes funciones (DRJ, 2012):

- Provee un punto central de contacto.
- Ayuda a llevar un orden para hacer válido el árbol de llamadas.
- Registro de llamadas entrantes y salientes.
- Recopilación de información crítica.
- Identificación de recursos.
- Informe a los directivos clave del estatus de la situación.
- Llevar un control sobre el contacto que se tenga con el Grupo de Recuperación de Tecnología.
- Establecer una estrategia de comunicación y notificación del estatus de la contingencia en la organización hacia todo el personal de la empresa, clientes, proveedores, entidades regulatorias, medios de comunicación, etc.
- Como llevar adecuadamente un registro de las operaciones.
- Preparación para la recuperación.

Emergency Operations Center, es un documento que puede ayudar en gran medida a fortalecer el ITDR detallando cada una de las tareas realizadas en caso de una contingencia en el sitio alterno o simplemente en las pruebas del ITDR.

2.4.3 Prácticas Generalmente Aceptadas (GAP)

Disaster Recovery Institute International (DRII) junto a Disaster Recovery Journal (DRJ), definen lineamientos para la planeación de las operaciones del negocio. Estos publican las Prácticas Generalmente Aceptadas o conocidas internacionalmente como Generally Accepted Practices (GAP) que define ciertos puntos para cada fase del ciclo de vida del BCP, los cuales se presentan a continuación (DRII, DRJ, 2007):

- **Iniciación y Administración del proyecto.** En esta fase se definen las necesidades, el alcance y las metas del Plan de continuidad de negocio, se define la Política de continuidad de negocio, se identifica el comité que apoyará al equipo de continuidad de negocio, se determina el costo del proyecto, se definen los requerimientos para la capacitación del personal y se identifica a que estándares internacionales se alineará el BCP (DRII, DRJ, 2007).
- **Evaluación del riesgo y controles.** Identificar todos los riesgos que pueden implicar una interrupción a las operaciones del negocio, sean naturales, humanos o tecnológicos. Identificar la probabilidad de que ocurra el evento (DRII, DRJ, 2007).
- **Análisis de impacto al negocio.** Se deben identificar las funciones y procesos críticos así como el impacto financiero provocado por la interrupción de las operaciones (DRII, DRJ, 2007).
- **Desarrollo de las estrategias de Continuidad.** Estas estrategias son de vital importancia, pues consisten en identificar las alternativas de recuperación de las operaciones en los marcos de tiempo definidos, realizando una analogía con el cuerpo humano estás son como el corazón del BCP, puesto que permitirán salvar vidas y minimizar o evitar un impacto negativo en el negocio a causa de una crisis o desastre. Identificar los recursos financieros y humanos con los que se cuentan para el proyecto y en base a esto, determinar la estrategia que mejor apoye al Plan (DRII, DRJ, 2007).
- **Respuesta de Emergencia y operaciones.** Identificar a socios y colaboradores de la organización con todos sus datos para poder localizarlos en cualquier momento. De esta fase se deriva el árbol de llamadas que indica quién le notifica a quién sobre la situación en un escenario de contingencia (DRII, DRJ, 2007).
- **Desarrollo e implementación de los planes de Continuidad de Negocio.** De acuerdo con las Prácticas generalmente aceptadas, se deben plasmar todas las soluciones y pasos a abordar en un plan de contingencias, el cual contendrá todas las actividades que permitirán el restablecimiento de las actividades críticas en plazos razonables, en esta fase se documentan todas las etapas para reanudar los procesos claves (DRII, DRJ, 2007).

- **Programas de Sensibilización y formación. D**esarrollar un plan de capacitación del personal, identificando para cada miembro la capacitación necesaria según el rol que desempeña y analizar las opciones corporativas con las que se cuenta para poder implementar la capacitación (DRII, DRJ, 2007).
- **Mantenimiento y pruebas de los Planes de Continuidad de Negocio.** En esta fase se solicita desarrollar un calendario de mantenimiento a los planes y definir los escenarios en los cuales se debe actualizar (DRII, DRJ, 2007).
- **Coordinación con las autoridades públicas.** Identificar las autoridades locales y regionales que revisarán la documentación que se desarrollarán e implementarán (DRII, DRJ, 2007).

Estos puntos son de gran apoyo ya que mencionan detalles específicos que los estándares BCI y BS 25777 mencionan de forma superficial. Lo que contribuye a incrementar el nivel de efectividad del Plan de Continuidad de Negocio.

2.5 Propuesta de análisis financiero de ORACLE

Esta metodología es de gran utilidad para identificar la ventaja o desventaja de implementar un plan. Para el caso del Plan de Continuidad de Negocio es importante tomar en cuenta los números que facilitan el poder ver si es viable implementar el Plan o no. Oracle ha desarrollado una teoría con referencia al Análisis Financiero para la Administración de Continuidad del Negocio.

Miguel Palacios (2009) de Oracle comenta sobre la importancia que tiene conocer el costo del Downtime (tiempo de inactividad), para definir la estrategia del BCP y que para comenzar el proceso de cuantificación del impacto financiero se debe hacer una clasificación entre los impactos tangibles e intangibles.

Clasificación de los impactos (PALACIOS, 2009):

- Tangibles:
  - Reducción de la productividad.
  - Pérdida en la producción.
  - Pérdida de ventas.
  - Pérdida de clientes.
  - Frustración de los empleados.
  - Penalidades de los organismos reguladores.

- Intangibles:
  - Impacto negativo en la reputación.
  - Pérdida de oportunidades.

- Moral de los empleados.
- Impacto en el valor de las acciones.

A continuación se explica en detalle la propuesta de Oracle para la elaboración del Análisis Financiero.

Costo de pérdida de productividad (P)

A = Costo anual de empleados.
B = Número de empleados.
C = Promedio de días trabajados por año.
D = Promedio de horas trabajadas por persona por día.
E = Número de horas de Downtime.
F = Número de empleados afectados.

$$\boxed{(\boldsymbol{P}) = \frac{(\boldsymbol{A}*\boldsymbol{E}*\boldsymbol{F})}{(\boldsymbol{B}*\boldsymbol{C}*\boldsymbol{D})}} \qquad (2.2)$$

La Fórmula anterior es una herramienta que puede apoyar a identificar el costo que genera para la empresa el que la operación normal se descontinúe. Este tema es de gran importancia para las organizaciones y que muy pocas veces se estudia, debido a que se considera poco probable que ocurra (PALACIOS, 2009).

Teniendo en cuenta que el Programa de Continuidad de Negocio es un tema proactivo, es necesario estudiar a fondo las pérdidas que se pueden generar en caso de con contar con este programa. Esto, con la finalidad de conocer los números y prevenir una pérdida financiera grave.

Valor de pérdida por ventas (S)

G = Ingreso por ventas anuales.
H = Número total de ventas por año.
I = Número estimado de pérdidas de ventas por año.

$$\boxed{(\boldsymbol{S}) = \frac{(\boldsymbol{G}*\boldsymbol{I})}{(\boldsymbol{H})}} \qquad (2.3)$$

En la primera fórmula se analizó la pérdida por horas de trabajo pérdidas. En esta segunda fórmula se analiza la pérdida por ventas, que también es importante tomar en cuenta para el análisis financiero (PALACIOS, 2009).

Costo de Recuperación de Servicio (R)

J = Trabajo de horas de soporte de TI.

k = Costo hora de personal de soporte.

$$\boxed{(\boldsymbol{R}) = (\boldsymbol{J} * \boldsymbol{K})} \qquad (2.4)$$

Costo Estimado de Downtime (T)

$$\boxed{(\boldsymbol{T}) = (\boldsymbol{P} + \boldsymbol{S} + \boldsymbol{R})} \qquad (2.5)$$

Para el caso del Plan de Continuidad de Negocios es importante elaborar un estimado de lo que costará la recuperación de la operación. Esto, con la finalidad de identificar la viabilidad y/o conveniencia de implementar el Plan de Continuidad de Negocio para la operación analizada.

3. DISEÑO METODOLÓGICO

3.1 Tipo de Investigación

Según el análisis y alcance de los resultados, esta investigación es de carácter exploratoria ya que el objetivo es examinar un tema o problema poco conocido del cual se puede inferir la posibilidad de continuar el estudio para profundizarlo o crear nuevas investigaciones a partir de la existente, en este caso es la creación de un nuevo Modelo de Plan de Continuidad de Negocio.

3.2 Métodos y Técnicas de Investigación

El método utilizado para esta investigación fue el uso de los métodos teóricos, los cuales crean las condiciones para ir más allá de las características superficiales de la realidad, explicar los hechos y profundizar en las relaciones esenciales y cualidades fundamentales de los procesos no observables directamente. La técnica utilizada para la investigación es la documental, puesto que sirve para consultar diferentes libros u otras fuentes a fin de obtener información en torno a las problemáticas que se plantean en el presente trabajo de grado.

3.3 Metodología para la elaboración del Modelo Integral de BCP

Las siguientes actividades han sido elaboradas, basadas principalmente en el ciclo de vida del plan de continuidad del negocio (Figura Nº 2.1) presentada en la norma BS 25999 y combinada además con la ISO 22301, debido a que esta norma es reconocida internacionalmente y puede ser certificable, se ha escogido adoptar esta estructura, para que en el futuro las empresas que opten por realizar su implementación del Plan de Continuidad de Negocio basados en este trabajo de grado, puedan cumplir con las auditorias de certificación de estas instituciones. Además se han incluido los puntos fuertes de otros estándares y buenas prácticas para la continuidad del negocio, con esto se busca obtener una mejor comprensión y una mejor adaptabilidad a la cultura organizacional chilena.

Para comprender de una forma más clara la propuesta metodológica, se presenta a continuación en la Figura Nº 3.1, el planteamiento de las actividades a seguir en la elaboración de la propuesta metodológica que plantea este trabajo de grado, además en las páginas siguientes se presenta cada uno de sus pasos y técnicas utilizadas para su creación.

Análisis de la situación actual referente a modelos utilizados a nivel mundial.

A través de una investigación exploratoria, se consultó diferentes fuentes bibliográficas, como: textos, revistas, libros e internet, para identificar las ventajas, desventajas y fortalezas que poseen las distintas metodologías existentes a nivel mundial.

Actividades necesarias para diseñar, implementar y mantener un BCP en Chile.
Planificación y Política de Continuidad de Negocio: • **Determinar los compromisos que debe adoptar la Dirección:** análisis comparativo de ISO 22301, ITIL y GAP, ya que estos poseen información sólida, de los cuales se han extraído los puntos más fuertes y que además se adapten a la cultura organizacional chilena, en donde por ejemplo las obligaciones se deben entregar de una forma impersonal y formal. • **Fijar cómo designar a un coordinador de continuidad de negocio:** se ha estudiado la cultura organizacional chilena, para que el líder que sea designado esté parametrizado bajo las cualidades y/o características laborales de los trabajadores chilenos, además se ha estudiado sobre liderazgo. • **Determinar la documentación que debe considerarse como evidencia para el BCP:** para determinar la documentación que debe considerarse como evidencia, se ha replicado en su totalidad la documentación exigida por la norma ISO 22301 y el estándar británico B25999. • **Precisar las principales características que debe poseer la Política de Continuidad de Negocio:** análisis con las metodologías que presentan información de mayor calidad en cuanto al tema tratado, estas son: Guía de buenas prácticas, Prácticas generalmente aceptadas, BS 25999 e ISO 22301, tomando como base las metodologías anteriormente mencionadas se procedió a resumir y destacar los puntos más importantes que debe contener un Política de Continuidad de Negocio • **Establecer cómo se debe planificar el BCP:** para establecer el cómo se debe planificar el BCP se realizó un estudio sobre Administración de Proyectos para así determinar los componentes más relevantes del plan de trabajo que debe realizar el coordinador o equipo de continuidad al momento de implementar un BCP.
Comprensión de la Organización y Análisis de Riesgos: • **Determinar cómo se debe realizar un estudio que permita conocer y comprender la organización en su totalidad:** análisis de contenidos de las metodologías que presentan información de mayor calidad: el estándar BS 25999 y la Guía de Buenas Prácticas tomando como base las metodologías anteriormente mencionadas se procedió a resumir y destacar los puntos más importantes que debe contener el estudio. • **Definir como se debe realizar un Análisis de Impacto al Negocio (BIA):** análisis de las diferentes metodologías expuestas en el marco teórico, de las cuales se obtuvo lo mejor de cada una referente al BIA, siendo las siguientes metodologías aquellas que poseían información de mayor calidad: Practicas Generalmente Aceptadas, estándar BS 25999, ISO 27002, análisis financiero de Oracle e ISO 22301.
Medidas Preventivas: • **Explicar cómo se debe realizar un plan de acción, que contempla las tareas que la compañía pretende adoptar para prevenir contingencias:** análisis de los estándares para obtener lo mejor de cada uno, estas son: GPG, ITIL, GAP, NFPA 1600, ISO 27002 e ISO 22301.
Estrategias de Recuperación: • **Establecer cómo deben realizarse las estrategias de recuperación para las actividades críticas de la organización:** profundo análisis de las metodologías y buenas prácticas para un BCP, de estas se obtuvieron las mejores estrategias y recomendaciones.
Definición de responsabilidades y desarrollo de los Planes de Contingencia: • **Establecer cómo se deben definir los cargos o los equipos necesarios para la activación del Plan de Contingencia:** estudio principalmente de la Guía de las buenas practicas (GPG), ya que esta posee un ítem con bastante información referente a los roles que deben existir en la activación y ejecución de los planes de contingencia ante situaciones críticas • **Determinar cómo se deben documentar los planes de contingencia:** análisis comparativo de BS 25999, BS 25777, ITIL, NFPA 1600, GAP, ISO 27002 y EOC, ya que estos poseen información sólida respecto a los planes de contingencia, de los cuales se han extraído los puntos más fuertes, para facilitar su comprensión y eficacia.

Pruebas, revisión y mantenimiento del BCP:

- **Precisar cómo se deben realizar las pruebas, revisiones y actualizaciones del BCP:** se ha estudiado principalmente la ISO 22301, el estándar BS 25999 y la Guía de las Buenas Practicas, ya que estos poseen mayor información y de mejor calidad, referente a las pruebas y el mantenimiento que debe tener un BCP.

Análisis de la cultura de la organizacional chilena y la incorporación de la cultura de BCP a ésta.

Se analizaron y evaluaron las características principales de la cultura organizacional chilena con el fin de identificar y aprovechar aquellas positivas y tratar de evitar las negativas, además se realizó un análisis de contenidos de las diferentes metodologías expuestas en el marco teórico, las metodologías que presentan información de mayor calidad en cuanto al tema tratado son: Guía de buenas prácticas, el estándar BS 25999 y la ISO 22301, tomando como base estas metodologías se procedió a resumir y destacar los puntos más importantes que debe contener un programa de cultura, que logre en el personal una plena concientización sobre la importancia que posee el Plan de Continuidad de Negocio para la Organización.

Propuesta metodológica para la implementación de un Plan de Continuad de Negocio en Chile.

Figura Nº 3.1: Metodología para la elaboración de un Modelo Integral de BCP.

Fuente: Elaboración propia.

A continuación se presenta en detalle la metodología para desarrollar el Modelo Integral de BCP:

3.3.1 Análisis de la situación actual referente a modelos utilizados a nivel mundial.

A través del análisis, síntesis, inducción y deducción, de acuerdo con la información recopilada en el marco teórico, se ha logrado proporcionar un conocimiento verdadero sobre la realidad en cuanto a lo que es un Plan de continuidad de negocio y como se puede implementar y mantener, en donde se analizaron las metodologías utilizadas a nivel mundial en la actualidad para implementar un BCP, con el objetivo de extraer lo mejor de cada una e identificar cuáles son las actividades necesarias para mantener e implementar un BCP.

3.3.2 Planificación y Política de Continuidad de Negocio.

- **Compromiso de la Dirección**

Para determinar los compromisos necesarios que debe adoptar la Dirección, con el fin de conseguir una implementación óptima y adecuada del Plan de continuidad de negocio, se realizó un análisis comparativo de ISO 22301, ITIL y GAP, ya que estos poseen información solida respecto al compromiso

de la Dirección, de los cuales se han extraído los puntos más fuertes y que además se adapten a la cultura organizacional chilena, en donde por ejemplo para la cultura organizacional chilena las tareas y obligaciones se deben entregar de una forma impersonal y formal.

- **Designar un Coordinador de Continuidad de Negocio**

Con el fin de establecer cómo se debe designar a un coordinador de continuidad de negocio se ha estudiado la cultura organizacional chilena, para que el líder que sea designado esté parametrizado bajo las cualidades y/o características laborales de los trabajadores chilenos, como por ejemplo la importancia de la delegación de autoridad y toma de decisiones, con lo cual se busca obtener que los colaboradores se sientan parte de la empresa y como un recurso valioso para la misma, además se ha estudiado sobre liderazgo, para comprender que es el liderazgo y como se puede medir, con el fin de hacer una selección de la persona más idónea que ha de ocupar el cargo de Coordinador del Plan de Continuidad de Negocio.

- **Documentación del BCP**

Para determinar la documentación que debe considerarse como evidencia y que es un recurso altamente valioso para cumplir con las auditorias, se ha replicado en su totalidad la documentación exigida por la norma ISO 22301 y el estándar británico B25999.

- **Elaborar la Política de Continuidad de Negocio**

Para determinar las principales características que debe poseer la Política de Continuidad de Negocio, se realizó un análisis de contenidos de las diferentes metodologías expuestas en el marco teórico, en donde se pudo obtener un filtro con las metodologías que presentan información de mayor calidad en cuanto al tema tratado, estas son: Guía de buenas prácticas, Prácticas generalmente aceptadas, BS 25999 e ISO 22301, tomando como base las metodologías anteriormente mencionadas se procedió a resumir y destacar los puntos más importantes que debe contener un Política de Continuidad de Negocio.

- **Establecer la planificación del BCP**

Para establecer el cómo se debe planificar el BCP se realizó un estudio sobre Administración de Proyectos para así determinar los componentes más relevantes del plan de trabajo que debe realizar el coordinador o equipo de continuidad al momento de implementar un BCP.

3.3.3 Comprensión de la Organización y Análisis de Riesgos

- **Comprensión de la Organización**

Para determinar cómo se debe realizar un estudio que permita conocer y comprender la organización en su totalidad, se realizó un análisis de contenidos de las diferentes metodologías que presentan información de mayor calidad en cuanto al tema tratado, estas son: el estándar BS 25999 y la Guía de Buenas Prácticas tomando como base las metodologías anteriormente mencionadas se procedió a resumir y destacar los puntos más importantes que debe contener el estudio.

- **Análisis de Impacto al Negocio (BIA por sus siglas en inglés)**

Para la construcción de la propuesta de cómo se debe confeccionar un BIA, se realizó un análisis de las diferentes metodologías expuestas en el marco teórico, de las cuales se obtuvo lo mejor de cada una referente al BIA, siendo las siguientes metodologías aquellas que poseían información de mayor calidad: Practicas Generalmente Aceptadas, estándar BS 25999, ISO 27002, análisis financiero de Oracle e ISO 22301.

3.3.4 Medidas Preventivas

Para explicar cómo se debe realizar un plan de acción, que contempla las tareas que la compañía pretende adoptar para prevenir y evitar en la medida de lo posible los riesgos que impactan la disponibilidad de las operaciones, se realizó un análisis comparativo de las metodologías que poseen información más sólida respecto a las medidas preventivas que puede ejecutar la organización, con el fin de obtener lo mejor de cada una, estas son: GPG, ITIL, GAP, NFPA 1600, ISO 27002 e ISO 22301.

3.3.5 Estrategias de Recuperación

Para establecer cómo deben realizarse las estrategias de recuperación para las actividades críticas de la organización, se ha hecho un profundo análisis de las metodologías y buenas prácticas para un BCP, de estas se obtuvieron las mejores estrategias y recomendaciones.

3.3.6 Definición de responsabilidades y desarrollo de los Planes de Contingencia.

- **Definir los cargos o los equipos necesarios para la activación del Plan de Contingencia**

Para establecer cómo se deben definir los cargos o los equipos necesarios para la activación del Plan de Contingencia se hecho un estudio principalmente de la Guía de las buenas practicas (GPG), ya que esta posee un ítem con bastante información referente a los roles que deben existir en la activación y ejecución de los planes de contingencia ante situaciones críticas.

- **Desarrollar Planes de Contingencia**

Para determinar cómo se deben documentar los planes de contingencia, se realizó un análisis comparativo de BS 25999, BS 25777, ITIL, NFPA 1600, GAP, ISO 27002 y EOC, ya que estos poseen

información solida respecto a los planes de contingencia, de los cuales se han extraído los puntos más fuertes, para facilitar su comprensión y eficacia.

3.3.7 Pruebas, revisión y mantenimiento del BCP

Para establecer el cómo deben realizarse las pruebas, revisiones, actualizaciones y poder de este modo prevenir que los documentos realizados queden obsoletos con el paso de los años, se han estudiado las metodologías y estándares presentes en el marco teórico, basándose principalmente en la ISO 22301, el estándar BS 25999 y la Guía de las Buenas Practicas, ya que estos poseen mayor información y de mejor calidad, referente a las pruebas y mantenimientos que debe tener un BCP.

3.3.8 Análisis de la cultura organizacional chilena y la incorporación de la cultura de BCP a ésta.

Para determinar cómo se debe incorporar el BCP la cultura de la organización, se analizaron y se evaluaron las características principales de la cultura organizacional chilena con el fin de identificar y aprovechar aquellas positivas y tratar de evitar las negativas, además se realizó un análisis de contenidos de las diferentes metodologías expuestas en el marco teórico, las metodologías que presentan información de mayor calidad en cuanto al tema tratado son: Guía de buenas prácticas, el estándar BS 25999 y la ISO 22301, tomando como base estas metodologías se procedió a resumir y destacar los puntos más importantes que debe contener un programa de cultura, que logre en el personal una plena concientización sobre la importancia que posee el Plan de Continuidad de Negocio para la Organización.

4. RESULTADOS Y ANÁLISIS

De acuerdo al Marco metodológico planteado en el capítulo 3, se presenta a continuación el Modelo para la implementación de un Plan de continuidad de Negocio en Chile, la cual se detalla a continuación.

4.1 Análisis de la situación actual referente a modelos utilizados a nivel mundial.

A continuación se presenta la Tabla Nº 4.1, que muestra el resultado del análisis hecho sobre las metodologías existentes a nivel mundial, en el cual se comparan los elementos más importantes que desarrollan y se identifican los puntos más fuertes que tocan cada una de ellas, para implementarlas en el Modelo de Plan Continuidad de Negocio, según lo que se ha estudiado se puede observar lo siguiente:

Tabla Nº 4.1: Comparación de los elementos utilizados por cada metodología.

Elementos	Metodología									
	BS 25999	**BS 25777**	**GPG**	**ITIL**	**EOC**	**GAP**	**NFPA 1600**	**ISO 27002**	**ISO 22301**	**ORACLE**
Administración BCP.	x		x		x	x		x	x	x
Análisis de Riesgos.	x	x	x	x	x	x	x	x	x	x
Análisis para entender lo que compone la organización.	x		x	x		x			x	
Estrategia para la continuidad de negocio.	x		x		x	x	x	x	x	
Administración de Incidentes.	x		x	x	x	x	x	x	x	
Plan Recuperación T.I.		x		x						
Plan de Pruebas.	x	x	x	x		x		x		
Plan de Mantenimiento del BCP.	x		x			x			x	x
Desarrollar la cultura de BCP	x		x						x	
Política BCP.	x		x			x			x	
Programa de Capacitación.	x	x	x						x	
Acuerdos de Servicio con los proveedores.	x	x		x	x	x	x		x	x
Política de Seguridad de la información.		x		x				x	x	
Contratación de seguros.						x	x		x	x

Fuente: Elaboración propia.

Lo anterior facilita observar de una forma más rápida el enfoque que poseen las distintas metodologías, con el fin de obtener lo mejor de cada una y agregar lo que se considere pertinente. Además en la Tabla anterior Nº 4.1, se puede observar que el BS 25999 junto a la ISO 22301 cuentan con un enfoque más generalizado sobre lo que es un BCP, desarrolla más puntos sobre lo que es necesario para llevar a cabo una buena práctica, por lo cual pueden servir para formar la estructura general de la metodología y de acuerdo con esto obtener de cada uno de los otros estándares mencionados, el punto que tienen más fortalecido.

A continuación se presenta la Tabla Nº 4.2, que contiene las ventajas y desventajas de los estándares, metodologías y buenas prácticas para emprender un Modelo de Plan de Continuidad de Negocio.

Tabla Nº 4.2: Ventajas y desventajas de los estándares, metodologías y buenas prácticas.

Estándares, Metodologías y Buenas Prácticas	Ventajas	Desventajas
BS 25999	Orientada a la Gestión de la Continuidad del Negocio.	Contempla parcialmente el tema de Recuperación ante desastres de TI (Tecnologías de la Información).
BS 25777	Establece un marco para crear y mejorar un sistema de gestión de continuidad de servicios en los Sistemas de TI.	Contempla parcialmente el tema de Continuidad del Negocio, se usa el estándar BS 25999 como complemento.
ITIL	Guía de buenas prácticas destinadas a facilitar la entrega de servicios de TI de alta calidad abarcando la infraestructura, desarrollo y operaciones de TI.	Contempla la mayoría de los procesos relacionados con la continuidad del servicio, no tiene un enfoque integrado de todo el proceso.
NFPA 160	Manejo de Desastres/Emergencias y Programas de Continuidad del Negocio.	Dirigido a Técnicos y profesionales encargados del control y seguridad contra incendios.
ISO 27002	Orientada a la Gestión de la Seguridad de la Información.	Contempla parcialmente el tema de Recuperación ante desastres de TI en la Continuidad del Negocio.
ISO 22301	Orientada a la Gestión de la Continuidad del Negocio con más más énfasis en la comprensión de los requisitos, el establecimiento de los objetivos y en la medición del desempeño.	Menos prescriptiva que la normas británicas, lo que deja una puerta abierta a interpretaciones por parte de las organizaciones que aplican la norma, así como por parte de los auditores.
GPG	Promociona normas en materia de competencias profesionales, ética de las prestaciones, mantenimiento de servicios y planificación de la continuidad de negocios.	Comprende parcialmente el tema de Recuperación ante desastres de TI.
EOC	Marca los lineamientos que deben cumplirse para activar un Centro de operaciones de emergencia para la Continuidad del Negocio.	Contempla la mayoría de los procesos relacionados con la continuidad del servicio, no tiene un enfoque integrado de todo el proceso.
GAP	Desarrolla una base de conocimientos en la planificación de contingencias y el manejo de riesgos. Administra los principales programas de certificación de la industria.	Estudia parcialmente el tema de Recuperación ante desastres de TI en la Continuidad del Negocio.

Fuente: Elaboración propia.

En conclusión, de ITIL por ser una biblioteca reconocida en los servicios de información, puede apoyar la parte de servicios de IT para la propuesta ya que tiene varios apartados donde se contemplan la mayoría de los procesos relacionados con la garantía de la continuidad del servicio, pero no tiene un enfoque integrado de todo el proceso. El EOC definitivamente toca un punto relevante en la Administración de Continuidad de Negocio, es decir, el centro de operación. La norma BS 25777, contiene una guía que establece cómo abordar la gestión de la continuidad de servicios de una organización, siguiendo el marco de referencia de la norma BS 25999, sistema de gestión de continuidad del negocio.

4.2 Actividades necesarias para diseñar, implementar y mantener un Plan de Continuidad de Negocio (BCP) en Chile.

4.2.1 Planificación y Política de Continuidad de Negocios

En esta fase, y tras haber obtenido el soporte y las inversiones necesarias, la empresa que decide abordar un plan de continuidad de negocio lo primero que debe hacer es averiguar qué se va a hacer y por qué. A continuación se presentaran las actividades a realizar para comenzar con la implementación de un Plan de Continuidad de Negocio.

- **Compromiso de la Dirección**

El Compromiso de la Dirección se refiere a las obligaciones y responsabilidades que adquiere la alta dirección en el desarrollo y la implementación del Plan de Continuidad de Negocio.

Obligaciones o compromisos mínimos que debe adoptar la Dirección:

- Asegurarse que las políticas y objetivos son establecidos.
- Asegurar la integración del BCP con los procesos de negocio.
- Asegurar que los recursos necesarios para el BCM estén disponibles.
- Comunicar la importancia del BCP.
- Asegurar que se logre el resultado esperado.
- Nombrar las personas competentes para ser responsables de la implementación del BCP y dotarlas de la autoridad apropiada.
- Direccionar y dar soporte a las personas que contribuyen a la efectividad del BCP.
- Promover la mejora continua.
- Definir los criterios de aceptación del riesgo y los niveles aceptables de riesgo.
- Participar activamente en los ejercicios y pruebas.
- Asegurar que las auditorías internas del BCP son realizadas.
- Conducir las revisiones administrativas del BCP.

- **Designar un Coordinador de Continuidad de Negocio**

El coordinador o el equipo deben trabajar con la dirección para identificar el alcance y los objetivos que persigue el plan, así como las actividades de negocio que son críticas en la organización.

Adicionalmente, el perfil o perfiles de las figuras encargadas de la gestión de la continuidad de negocio no tiene que estar forzosamente localizado en las áreas de tecnología y sistemas (derivado de la idea generalizada de que los procesos de continuidad de negocio están constituidos principalmente por componentes tecnológicos), lo más importante es que posea una visión integral de la organización.

El coordinador de Continuidad de Negocio debe poseer:

- Habilidades de Liderazgo, para desarrollar un ambiente participativo y cooperativo.
- Buenas relaciones interpersonales.
- Capacidad analítica.
- Buena comunicación verbal y escrita.
- Orientación al logro.
- Trabajo en equipo.
- Capacidad de delegar autoridad y toma de decisiones.
- Capacidad de autogestión.

Además se presenta a modo de recomendación utilizar el modelo elaborado por James Kouzes y Barry Posner (2007), para evaluar el comportamiento del liderazgo en las organizaciones y así identificar al miembro del equipo que posea más capacidades de liderazgo frente al grupo para ser designado luego como Coordinador del Plan de Continuidad de Negocio. El análisis del liderazgo se lleva a cabo por medio de la evaluación de cinco comportamientos:

- **Desafiar los procesos:** El líder se hace responsable de los riesgos que conllevan los procesos administrativos y operativos, además de la dinámica interna y externa que juegan los procesos.
- **Inspirar una visión compartida:** Se refiere a la imaginación apasionante del líder sobre escenarios futuros.
- **Habilitar a los demás a que actúen:** Esta característica se refiere a la facultad del líder para desarrollar un ambiente participativo y cooperativo, haciendo del equipo de trabajo, compañeros pro-activos.
- **Modelar el camino:** Se refiere a una alta jerarquía de valores y de igual forma una alta moralidad. Coloquialmente podría decirse: “El líder predica con el ejemplo”.
- **Dar aliento con el corazón:** Es un comportamiento transaccional integrado en el Inventario de las prácticas de liderazgo. Este comportamiento se refiere a la retroalimentación positiva que el líder da a los seguidores, reconociendo públicamente las contribuciones individuales y celebrando los logros del equipo.

Sumado a lo anterior, se propone que para aquellas organizaciones que constituyen un equipo de continuidad de negocio, se conforme principalmente por personal que pertenezca o conozca las diferentes actividades del negocio (tecnología y sistemas, financiero, comercial, recursos humanos, etc.), ya que los riesgos y amenazas varían en función de dicha actividad y deben ser absolutamente identificados y priorizados.

- **Documentación del BCP**

Documentos que debe considerarse como evidencia según lo establecido por el estándar BS 25999 y el estándar ISO 22301:

- Política de Continuidad de Negocio.
- Material que contenga los términos de referencia para que el personal identifique los términos claves.
- Análisis de riesgos de la organización.
- Análisis de Impacto al Negocio (BIA) de cada una de las áreas consideradas como área clave.
- Identificación de los recursos con los que cuenta la organización para el programa de BCP.
- Programa de Capacitación para que cada persona tenga perfectamente definidas las tareas que debe realizar una vez declarada la contingencia..
- Programa de concientización. Al inicio del año se define un plan de concientización para los empleados referente al BCP. Con ello se busca que los colaboradores tengan conocimiento de las acciones que la organización lleva a cabo para estar preparado y reaccionar en caso de una contingencia, así como las acciones en las que se necesita de su participación y que se tenga claramente definida la importancia de las tareas de cada colaborador.
- Plan de Administración de Incidentes. El Plan debe tener los detalles sobre la forma en que los equipos deben trasladarse al sitio alterno. Los números de contacto de las instituciones que se necesite contactar en un escenario de contingencia.
- Contratos con terceras partes. Es necesario tener un Acuerdo de Nivel de Servicios (SLA) con cada una de las empresas que brindan algún servicio, para así asegurar que en caso de contingencia, sigan proporcionando el servicio.
- Plan de Recuperación de Tecnología en caso de Desastre (DRP por sus siglas en inglés). Para la Continuidad de Negocio es importante contar con un Plan para la recuperación de tecnología actualizado al día, pues es el soporte principal del BCP.

Según el alcance del Plan de Continuidad de Negocio en cada empresa, dependerá el número de documentos del listado anterior que apliquen a cada caso, de cualquier forma es indispensable elaborar todos los que convengan a la eficiencia del BCP, en los siguientes puntos se describe y se explica cómo se deben realizar las tareas anteriormente mencionadas.

- **Elaborar la Política de Continuidad de Negocio**

La política de continuidad de negocio debe ser apropiada para los propósitos de la organización además debe estar documentada, comunicada, disponible y se deben definir los tiempos para su revisión. Esta política tiene que establecer las directrices generales del Plan de continuidad de negocio, como su alcance, lineamientos y objetivos de la gestión, principales roles y responsabilidades.

A continuación se muestran los puntos que debe contener una Política de Continuidad de Negocio, para que permita conocer con más exactitud el enfoque que con frecuencia es aplicado a la elaboración de la misma:

- **Introducción:** En la que se detalle de forma resumida la materia tratada (Plan de Continuidad de Negocio), la estructura del documento y lo que se persigue a través del mismo.
- **Objetivos:** En este apartado se detallan los objetivos que serán satisfechos mediante la aplicación de la propia política, como garantizar la continuidad de las actividades y de los servicios, aplicar los procedimientos de contingencia y planes de respuesta necesarios, etc.
- **Alcance:** Indica los procesos u operaciones de negocio que son cubiertos por la política, así como los recursos que soportan los citados procesos. Si aplica, también puede llegar a considerarse la zona geográfica sujeta a las instrucciones marcadas por la política.
- **Responsabilidades:** Relación de los diferentes responsables implicados de una forma u otra en la gestión de la continuidad de negocio (gerencia, coordinador, equipo, áreas de negocio, proveedores de servicio, etc.) junto con una descripción detallada de sus funciones y obligaciones (gestión de riesgos, asignación y distribución de los recursos, desarrollo de procedimientos de respuesta, realización de pruebas periódicas, formación, etc.).

- **Establecer la planificación del BCP**

La organización debe planificar, implementar y controlar el proceso necesario para alcanzar los requerimientos. Finalmente el coordinador o equipo de continuidad, debe aplicar sus habilidades en gestión de proyectos, para programar y desarrollar los siguientes componentes del plan de trabajo: tareas a llevar a cabo para satisfacer los objetivos descritos en la política de continuidad, responsables de ejecutar tales tareas, tiempos de ejecución, hitos, presupuestos, plazos e indicadores de éxito.

4.2.2 Comprensión de la Organización y Análisis de Riesgos

- **Comprensión de la Organización**

Esta fase tiene el propósito de identificar los servicios y productos que la organización tiene comprometido entregar a sus clientes, en esta fase, se definen también las actividades necesarias para

llevar a cabo ese objetivo. Los recursos necesarios disponibles en la organización que permitan entregar los servicios y productos a los clientes correspondientes en tiempo y forma.

Como primer paso para llevar a cabo la implantación del proceso de Continuidad de Negocio es necesario realizar un estudio detallado de la organización, que muestre la situación en la que se encuentra en el momento anterior a la implantación del BCP. El estudio debe mostrar:

- Tamaño de la organización.
- Sector en el que se llevan a cabo las negociaciones.
- Estructura funcional de la compañía.
- Objetivos de la organización.
- Procesos realizados en cada una de las áreas que forman la organización.
- Personal que trabaja en la organización y los que participarían en el BCP.
- Activos y recursos con los que cuenta la organización para el cumplimiento de los objetivos.
- Interdependencias con otras compañías, entre áreas, procesos y actividades.

Después del análisis de la organización, en el cual se tengan plenos conocimientos de los puntos listados anteriormente, se puede proceder a llevar a cabo el Análisis de Impacto al Negocio, que se detalla en el punto siguiente.

- **Análisis de Impacto al Negocio (BIA por sus siglas en inglés)**

El BIA identifica en cada área, los procesos críticos que se realizan, así como los recursos técnicos, financieros y tecnológicos necesarios para poder realizarlos y número de empleados que apoyan a cada proceso. En el BIA se debe identificar el impacto que ocasionaría, no realizar el proceso en “x” números de días o de horas.

Para la elaboración del Análisis de Impacto al Negocio puede utilizarse la herramienta o formato que más se adapte a las necesidades de la organización, a continuación se muestra la propuesta de este documento:

a) **Identificación de las actividades críticas**

Luego de conocer en plenitud la organización y posterior a su análisis se procede a la identificación de las actividades críticas, para ello es necesario que las empresas realicen el esfuerzo de identificar y valorar el impacto que podría tener en la organización si una actividad se paralizase, así como el tiempo de interrupción que puede ser soportado por la organización hasta que las pérdidas no sean asumibles (tiempo máximo permitido de interrupción o MTD por sus siglas en inglés).

Para definir el impacto que tendría la no ejecución de cierta actividad, se puede asignar una escala de valores a los siguientes factores:

- Impacto en el bienestar de los empleados.
- Daño o pérdida de la información.
- Incumplimiento de las normas legales.
- Daño de la reputación.
- Daños a la viabilidad financiera.
- Deterioro de la calidad del servicio o producto.
- Daño ambiental.

Otorgándole valores más altos a los factores que la organización considere más importantes de salvaguardar y viceversa. Para luego sumar los valores y poder así obtener información cuantitativa, que resultará ser de más fácil observación y comparación.

Una vez identificadas todas las actividades críticas se sugiere utilizar una Tabla como la del Anexo A, que permita visualizar todas las actividades críticas de una forma rápida.

b) **Tiempos de recuperación**

Ya identificadas las actividades críticas de la organización, debe elaborarse una priorización de las mismas con la finalidad de identificar las que deben recuperarse primero en caso de una contingencia, para lo cual es necesario estimar dos parámetros muy específicos que están estrechamente relacionados con la recuperación: Tiempo de Recuperación Objetivo (RTO) y Punto de Recuperación Objetivo (RPO).

El RTO establece la urgencia que las diferentes unidades de negocio precisan para volver a su funcionamiento habitual. Por tanto, determina los plazos en los que deben volver a funcionar con normalidad. Estos pueden establecerse en períodos de tiempo en función de la criticidad de los procesos y pueden ser cuestión de horas o semanas en aquellos procesos prescindibles. Por tanto, se trata de identificar el orden en que hay que tratar de reconstruir la actividad, recuperando antes aquellos procesos cuya paralización suponen un mayor impacto para la organización. En una situación de crisis siempre hay recursos limitados y es necesario elegir qué hacer primero atendiendo a un criterio de negocio.

El RPO se refiere al punto más reciente en el tiempo en el que los sistemas pueden ser recuperados, reflejando por tanto cuánta es la cantidad de información que una organización puede permitirse perder sin que le afecte negativamente. Por tanto, el RPO determina la periodicidad con la que deben salvaguardarse los datos para todos aquellos procesos de negocio.

c) **Costo de Downtime**

Para calcular el costo de Downtime de cada actividad crítica que aporta como indicador en la priorización de las mismas, se sugiere utilizar el modelo de análisis financiero de ORACLE, que se presenta a continuación:

Costo de pérdida de productividad (P)

A= Costo anual de empleados.

B= Número de empleados.

C = Promedio de días trabajados por año.

D = Promedio de horas trabajadas por persona por día.

E = Número de horas de Downtime.

F = Número de empleados afectados.

$$\boxed{(\boldsymbol{P}) = \frac{(\boldsymbol{A}*\boldsymbol{E}*\boldsymbol{F})}{(\boldsymbol{B}*\boldsymbol{C}*\boldsymbol{D})}} \qquad (4.1)$$

Valor de pérdida por ventas (S)

G = Ingreso por ventas anuales.

H = Número total de ventas por año.

I = Número estimado de pérdidas de ventas por año.

$$\boxed{(\boldsymbol{S}) = \frac{(\boldsymbol{G}*\boldsymbol{I})}{(\boldsymbol{H})}} \qquad (4.2)$$

Costo de Recuperación de Servicio (R)

J = Trabajo de horas de soporte de TI.

k = Costo hora de personal de soporte.

$$\boxed{(\boldsymbol{R}) = (\boldsymbol{J} * \boldsymbol{K})} \qquad (4.3)$$

Costo Estimado de Downtime (T)

$$\boxed{(\boldsymbol{T}) = (\boldsymbol{P} + \boldsymbol{S} + \boldsymbol{R})} \qquad (4.4)$$

El número resultante indica la pérdida financiera por materializarse el incidente analizado. Tomando en cuenta el resultado, la organización determina si el impacto es tan alto como para implementar medidas para evitarlo e integrarlo así al BCP.

d) **Criticidad**

En cuanto a la criticidad se puede clasificar de la siguiente manera:

- **Críticos:**
  - Funciones que pueden realizarse sólo si las capacidades se reemplazan por otras idénticas.
  - No pueden reemplazarse por métodos manuales.
  - Muy baja tolerancia a interrupciones.
- **Vitales:**
  - Pueden realizarse manualmente por un periodo breve.
  - Costo de interrupción un poco más bajos, sólo si son restaurados dentro de un tiempo determinado (5 o menos días, por ejemplo).
- **Sensitivos:**
  - Funciones que pueden realizarse manualmente por un periodo prolongado a un costo tolerable.
  - El proceso manual puede ser complicado y requeriría de personal adicional.
- **No críticos:**
  - Funciones que pueden interrumpirse por tiempos prolongados a un costo pequeño o nulo.

Finalmente se presenta una Tabla Nº 4.3, en cual se puede observar un ejemplo de cómo pueden ser registradas las actividades de la organización en base a los parámetros anteriormente descritos.

Tabla Nº 4.3: Registros de las actividades.

Nº	Nombre de la Actividad	Descripción	MDT	RTO	RPO	Costo de Downtime	Impacto	Criticidad
1								
2								
3								
4								

Fuente: Elaboración propia.

- **Evaluación de Riesgos**

Se ha de elaborar un análisis detallado de las situaciones que pueden ocasionar una interrupción a las operaciones del negocio, se estudia las amenazas a la organización, así como la evaluación de los impactos que pudiera provocar cada actividad y la probabilidad de que ocurra una situación de este tipo. Se sugiere utilizar un mapa como el que se muestra a continuación en la Figura Nº 4.1, dónde se ubiquen los riesgos encontrados con la finalidad de identificar visualmente la situación de la organización.

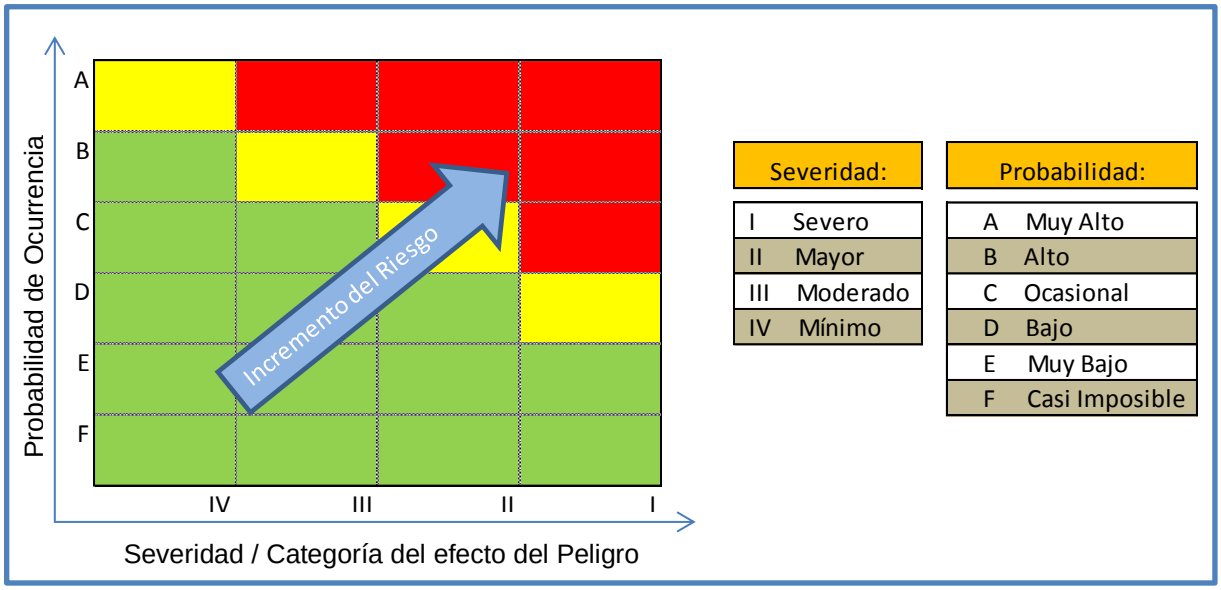

Figura Nº 4.1: Mapa para análisis de riesgos y categorías para evaluar.

Fuente: Elaboración propia.

El mapa para análisis de riesgos representa la ubicación en la que se encuentran los escenarios propios de la organización que se está evaluando para la implantación de un Plan de Continuidad de Negocio. La evaluación de los escenarios va relacionada a la severidad y probabilidad que se tenga sobre la contingencia estudiada. Para el análisis se debe realizar una categorización de los riesgos, para ello es necesario estudiar las vulnerabilidades de que ocurran riesgos naturales, tecnológicos y/o humanos. A continuación se presenta una Tabla Nº 4.4 con la categorización de los riesgos.

Tabla Nº 4.4: Categorización de los Riesgos

Categoría de Riesgo	Descripción	Subcategoría de Riesgo
Riesgo Externo.	Los riesgos resultan de eventos externos a la empresa, directa o indirectamente a la compañía.	• Proveedor, desastre natural., legislación y regulación, fraude externo, actividad criminal.
Riesgo por empleados.	El riesgo resulta de los errores de empleados.	• Personal clave, habilidades, capacidades, relaciones entre empleados, discriminación.
Riesgos por sistemas.	Los riesgos resultan del inadecuado o falla de la infraestructura de sistemas de la compañía.	• Hardware, software, interfaces, redes, comunicaciones, seguridad.
Riesgo por procesos.	Los riesgos que resultan de los inadecuados procesos internos.	• Transacciones, diseño de procesos, procesos, datos internos, datos externos, cambio de proyectos, productos defectuosos, servicio al cliente.

Fuente: Elaboración Propia.

En Tabla anterior Nº 4.4, se identifican las categorías de riesgos que pueden aparecer en el análisis de riesgos, el cual llevará a tomar medidas para prevenir los riesgos que así lo permitan y tomar medidas correctivas para aquellos que no es posible evitar.

Con los resultados del Análisis de Riesgos, se busca identificar medidas para implementar que:

- Disminuyan la probabilidad de ocurrencia del incidente.
- Acorten el período del incidente.
- Limiten el impacto en caso de no poder evitar que ocurra el incidente.

Para llevar a cabo el Análisis de Riesgos puede servir de apoyo una Tabla que permita depositar los datos sobre las vulnerabilidades de la organización, cómo la Tabla Nº 4.5 que se muestra a continuación.

Tabla Nº 4.5: Análisis de Riesgos.

ID	Amenaza	Riesgo	Severidad	Probabilidad	Categoría	Impacto	Escenario
Nº Consecutivo							

Fuente: Elaboración propia.

La tabal anterior Nº 4.5, sirve para mostrar los datos que deben registrarse en el análisis de riesgos, estos son: la amenaza que identifica la organización, los riesgos de que ocurra, la severidad que tendría en la organización, probabilidad de que el evento suceda, categorías, impacto que tendría sobre la operación y/o seguridad de la información y el escenario que se desataría.

A continuación se presenta una Tabla Nº 4.6 con la descripción de los campos mencionados.

Tabla Nº 4.6: Descripción de los Campos.

Campo	Descripción
ID	Nº de la vulnerabilidad
Amenaza	Vulnerabilidad o situación que afecta a una aplicación, servicio o servidor que se está evaluando.
Riesgo	Descripción del riesgo detectado en el análisis. Todo evento, falla o bien que ponga en peligro la integridad. Confidencialidad o disponibilidad de la información o los recursos activos.
Severidad	Medida de severidad del Riesgo I- Severo II- Mayor III- Moderado IV- Mínimo

Probabilidad	Es la probabilidad de ocurrencia del evento que se está tomando en cuenta para las amenazas y vulnerabilidades predominantes. Se utiliza la siguiente escala: A: Muy Alto La situación se presenta 1 vez o más al año. B: Alto La situación se presenta 1 vez entre 1 y 3 años. C: Ocasional La situación se presenta 1 vez entre 3 y 5 años. D: Bajo La situación se presenta 1 vez entre 5 y 10 años. E: Muy Bajo La situación se presenta 1 vez entre 10 y 30 años. F: Casi imposible , la situación se presenta 1 vez en más de 30 años.
Categoría	Riesgo Externo. Riesgo por empleados. Riesgo de sistemas. Riesgo por procesos.
Impacto	Efecto potencial de una falla de seguridad, teniendo en cuanta sus consecuencias en el negocio.

Fuente: Elaboración propia.

Para completar la Tabla es recomendable lo siguiente:

Jerarquizar la probabilidad basada en las situaciones ocurridas en los años pasados, para la severidad e impacto, es necesario tomar en cuenta el daño a la marca, impacto por incumplimiento, además de la cantidad de pérdida de ingresos.

Con la información almacenada en la Tabla 4.5, se procede a graficar y queda un mapa dónde se visualiza la probabilidad que tiene la organización de sufrir algún riesgo, a modo de ejemplo este se puede observar en la Figura Nº 4.2:

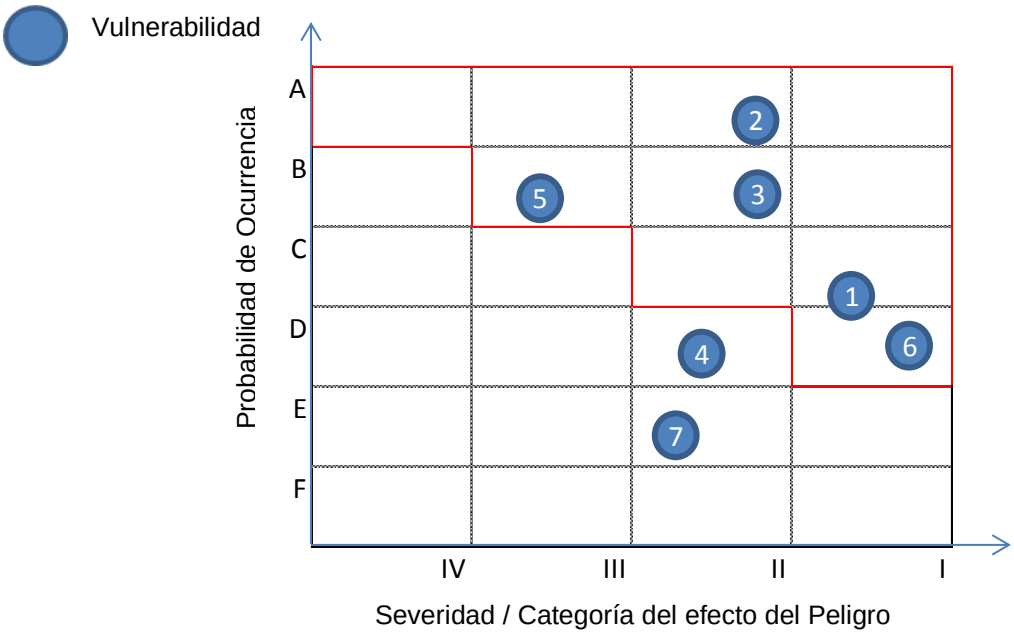

Figura Nº 4.2: Ejemplo de visualización de riesgos en la Organización.

Fuente: Elaboración propia.

Finalmente lo que se debe obtener en esta fase una vez realizado todas las actividades anteriores es:

- Entender la organización mediante la identificación de productos y servicios claves, así como las actividades y recursos críticos que los soportan.
- Estimar el impacto y las consecuencias de los posibles fallos en esas actividades y recursos críticos.
- Y por último, identificar y valorar los riesgos que podrían interrumpir la entrega de los productos y servicios de la empresa, así como de los recursos sobre los que están soportados.

4.2.3 Medidas Preventivas

El propósito de esta fase consiste en aplicar medidas de seguridad que eviten en la medida de lo posible que se produzcan incidentes que, al no ser gestionados adecuadamente, hagan necesaria la activación del Plan de Continuidad de Negocio.

Tomando como base los resultados del BIA y del análisis de riesgos, la organización debe identificar y aplicar controles o medidas de seguridad que:

- Reduzcan la probabilidad de que las actividades críticas sufran interrupciones.
- Disminuyan el tiempo de una eventual interrupción.
- Limiten el impacto que una paralización de las actividades críticas pueda provocar en la organización.
- Incrementen la fortaleza del negocio mediante la eliminación de puntos de fallo únicos (accesos, procesos, clientes, etc.)

De esta forma se elabora un plan de acción que contempla las tareas que la compañía pretende adoptar para prevenir y evitar en la medida de lo posible los riesgos que impactan en la disponibilidad de las operaciones. Finalmente el proceso de identificar e implantar medidas de seguridad debe estar basado en un equilibrio entre los siguientes factores:

- Riesgo que está siendo mitigado o impacto que estaría siendo reducido.
- Costo de implementar la/s medida/s de seguridad (económico y humano).
- Beneficios que la implementación de la/s medida/s de seguridad que aporta a la empresa.

Por lo tanto, en vez de esperar a que un desastre golpee a la organización para ver cómo esta se recupera, las medidas preventivas (en ocasiones denominadas contramedidas) deben ser aplicadas con el objetivo de incrementar la fortaleza de sus actividades frente a posibles impactos previamente identificados en el BIA. Algunos ejemplos de medidas preventivas más comunes son:

- Empleo de materiales de construcción robustos.
- Redundancia de sistemas informáticos y líneas de comunicación.
- Adquisición de seguros con diferentes grados de cobertura.
- Copias de seguridad de información que soporta una actividad crítica de la organización.
- Sistemas de detección y extinción de incendios.
- Sistemas de prevención de intrusiones, control de accesos, alarma y vigilancia.

A continuación se presenta una Tabla Nº 4.7 con algunos ejemplos de medidas preventivas, que proporcionan una protección ante los riesgos que puede sufrir una organización, y que cuya ocurrencia se puede atenuar instrumentando controles adecuados.

Tabla Nº 4.7: Ejemplos de medidas preventivas.

Riesgo	Medidas Preventivas
Interrupción eléctrica.	• Fuentes alternas de generación eléctrica: UPS y plantas eléctricas. • Mantenimiento de las fuentes alternas de generación eléctrica. • Estado de la instalación eléctrica y capacidad eléctrica instalada. • Lámparas de emergencia.
Fallos en Hardware.	• Equipo de cómputo utilizado y obsolescencia. • Capacidad de redundancia entre servidores. • Monitoreo de problemas en los servidores. • Contratos de mantenimiento preventivo y correctivo. • Condiciones físicas y ambientales (limpieza, humedad, temperatura).
Fallas en Software.	• Desarrollo local de aplicaciones (metodologías/ estándares). • Cambios y configuración en aplicaciones. • Trascendencia de los sistemas incluidos en el estudio.
Fallas en Comunicaciones.	• Soporte técnico de los equipos utilizados. • Mantenimiento preventivo y correctivo de los equipos de comunicación.
Desastres naturales.	• Pólizas de seguro vigentes. • Brigadas de atención ante situaciones de emergencia. • Capacitación al personal. • Rutas de evacuación. • Iluminación de pasillos, puertas y salidas de emergencia.
Incendio.	• Pólizas vigentes de seguro. • Sistemas automáticos y manuales contra incendio (gabinetes, extintores, aspersores). • Uso de materiales retardantes del fuego. • Almacenamiento de material combustible. • Detectores de humo revisados regularmente.
Fallas en Respaldos.	• Procedimientos para respaldo y recuperación de información, fuentes, objetos, documentación, y configuración de los sistemas. • Periodicidad de los respaldos. • Facilidades y protección para el almacenamiento dentro y fuera de sitio. • Configuración de los discos duros de los servidores. • Documentación actualizada sobre procedimientos de respaldo y recuperación.
Virus	• Programa antivirus instalado en computadoras y servidores. • Configuración y actualización del software antivirus. • Consultas regulares de fuentes de información para actualizaciones sobre virus. • Capacitación al personal para identificar potenciales fuentes de ataque de virus. • Políticas para el ataque de virus.

Violaciones a la Seguridad física.	• Seguridad física para el ingreso al edificio, oficinas y cuartos de servidores y equipos de comunicación. • Capacitación al personal para detectar situaciones que puedan representar riesgo o cuestionar la presencia de personas desconocidas o sin identificación. • Sistemas de seguridad: circuitos cerrados de televisión, sensores de movimiento, alarmas. • Revisión y control de salida e ingreso de equipo de cómputo. • Utilización de bitácoras para el registro de ingresos.
Intrusión (Hackeo).	• Procedimientos establecidos para otorgamiento de acceso a las aplicaciones y políticas de acceso lógico. • Procedimientos establecidos para el acceso a los recursos tecnológicos (redes y aplicaciones). • Administración y configuración de “firewalls”. • Monitoreo de los accesos tanto legítimos como ilegítimos. • Disponibilidad de herramientas para el monitoreo de la seguridad.
Recurso Humano.	• Dependencia en el personal. • Capacitación. • Documentación de las funciones del personal.

Fuente: Elaboración Propia.

4.2.4 Estrategias de Recuperación

Derivado de los resultados del BIA, el objetivo perseguido en esta fase consiste en identificar las alternativas de recuperación de las actividades críticas de la organización en los marcos de tiempo definidos y aceptados. La organización debe tener en cuenta los posibles daños potenciales a la hora de revisar y seleccionar las diferentes soluciones o alternativas de recuperación de sus actividades críticas, considerando adicionalmente los siguientes factores:

- El costo asociado al establecimiento de la estrategia, la cual suele constituir uno de los mayores inconvenientes a la hora de adquirir una solución de recuperación.
- Los beneficios que proporciona la citada estrategia.
- El Tiempo Máximo Permitido de Interrupción (MTD) de la actividad crítica.
- El Tiempo de Recuperación Objetivo (RTO).
- La pérdida máxima de información que una empresa se puede permitir (RPO).

A continuación se presenta la Tabla Nº 4.8, en la cual se pueden observar ejemplos de estrategias de recuperación.

Tabla Nº 4.8: Ejemplos de estrategias de recuperación.

Recurso crítico	Objetivo	Estrategias de recuperación
Personas que participan en las actividades de negocio.	Mantener el conocimiento y las capacidades del personal con funciones y responsabilidades en actividades críticas.	• Documentar actividades críticas. • Formación. • Conocimiento compartido y multidisciplinario. • Separación de tareas claves.
Instalaciones y Puestos de trabajo.	Reducir el impacto que genera la falta de disponibilidad de las instalaciones de trabajo.	• Instalaciones alternativas. • Acuerdos recíprocos. • Teletrabajo.

Tecnología.	Entender el entorno tecnológico que soporta las actividades críticas y mantener la capacidad para replicarlo en caso de desastre.	• Redundancia de equipos y comunicaciones. • Mantenimiento de la misma tecnología en diferentes ubicaciones. • Copias de software crítico.
Información y Documentación.	Garantizar la protección y recuperación de la información vital para la organización.	• Copias de seguridad. • Procedimientos de recuperación. • Documentación de activación del Plan de Continuidad.
Proveedores.	Identificar y mantener un inventario de proveedores de servicios claves que soportan las actividades críticas.	• Contacto con proveedores alternativos. • Acuerdos con terceros. • Envío y almacenamiento de recursos críticos en ubicaciones alternativas.
Accionistas y Socios.	Proteger los intereses de socios y accionistas afectados por un desastre.	• Acuerdos que garantizan el bienestar de los colectivos involucrados en el desastre.
Servicios civiles de emergencia (tráfico, bomberos).	Garantizar que la organización conoce los procedimientos de los servicios de emergencia.	• Recomendaciones de rutas de evacuación y puntos de reunión. • Participación en simulacros.

Fuente: Elaboración propia.

En este sentido, es importante destacar los siguientes aspectos con respecto a la selección de las estrategias de recuperación:

- La elección de las diferentes alternativas de recuperación depende de las necesidades de la organización: tiempos de recuperación objetivo (RTO), costos, recursos humanos, recursos técnicos, etc.
- Lo más común y recomendable es adoptar una combinación de las estrategias de recuperación para los distintos recursos críticos.
- El tiempo de recuperación objetivo (RTO) definido por la organización para sus actividades críticas siempre debe ser menor al tiempo máximo permitido de interrupción (MTD).
- El costo de las estrategias de recuperación será generalmente mayor cuanto menor sea el tiempo de recuperación objetivo (RTO).

Según los criterios previamente detallados, y teniendo en cuenta la formalidad de los resultados del proceso BIA, se recomienda una selección de las estrategias de continuidad debidamente documentada para cada actividad crítica. Dicha selección debe ser acordada y ratificada con el director o el nivel directivo de la empresa. Además, es necesario destacar que las estrategias de recuperación seleccionadas para cada actividad deben ser acordes a los Tiempos de Recuperación Objetivo (RTO) previamente definidos y aprobados .En paralelo, es aconsejable diseñar una planificación para la puesta en marcha de la estrategia acordada para determinar el aprovisionamiento de los recursos.

Recomendaciones para la elaboración de las estrategias de recuperación

Las estrategias de recuperación deben considerar los siguientes recursos:

- **Personal:** Es necesario definir la mejor estrategia para mantener las principales habilidades y conocimiento necesario para dar continuidad a las operaciones del negocio, información para proveedores, administración y retención de conocimiento. Se sugiere tener un Plan de capacitación para el personal, el cual permite identificar visualmente cuales son las tareas que la organización llevará a cabo con el personal a lo largo de un tiempo determinado. El Plan de Capacitación debe identificar capacitación para empleados de nuevo ingreso, para las áreas técnicas y para las áreas comerciales.

- **Instalaciones:** En esta sección se debe verificar que las instalaciones alternas permitan llevar a cabo las actividades que apoyen a las operaciones de la organización, estas instalaciones alternas deben contar con la infraestructura necesaria que permita continuar con la operación a un nivel aceptable. Para otro tipo de escenario puede tomarse la medida para trabajar desde casa o vía remota. Las instalaciones alternas con las que cuente la organización van a depender directamente del presupuesto que posea la organización para el Plan de Continuidad de Negocio. Si se ha de contar con un proveedor para dar el servicio de Instalaciones de trabajo alterno este debe cumplir al menos con los siguientes puntos:
  - ✓ Estar ubicado a 50 km de las instalaciones principales.
  - ✓ Ubicarse en una zona segura, de preferencia evitar que se encuentre cerca de fábricas o industrializadoras.
  - ✓ Tener experiencia en el tema de Continuidad del Negocio.

  Para elegir el proveedor que más se acerque a los requerimientos de la organización es conveniente llevar a cabo un concurso, en el que se entrevisten las diferentes opciones y se compare la oferta de cada uno con la finalidad de elegir la propuesta que mejor se adecue a las necesidades de la organización.

- **Información:** Se debe verificar que se posea la información necesaria para dar continuidad a las operaciones del negocio, esta información debe cumplir con las características de seguridad indispensables, integridad, disponibilidad y confidencialidad aunque se esté en las instalaciones alternas. Como parte de las estrategias de información, y siendo este tema muy sensible, es necesario tomar elaborar respaldos de la información. También como medida se seguridad adicional, los respaldos pueden resguardarse en una bóveda especial para resguardo de respaldos, actualmente existen proveedores que brindan este servicio, por lo que es recomendable realizar un exhaustivo análisis de los proveedores existentes para elegir el que más convenga a las necesidades de la organización.

- **Tecnología:** La tecnología va a depender del tipo de operación que realice normalmente la organización, lo que se debe verificar es que la tecnología que se tenga, sea suficiente para poder llevar a cabo la operación a un nivel aceptable en un escenario de contingencia. Para esta

estrategia se debe elegir la infraestructura según las necesidades y el presupuesto de la organización. Para una mejor implementación de la estrategia de Tecnología se sugiere elaborar Inventarios de todo lo que tenga que ver con Tecnología, en el inventario es necesario indicar la criticidad que cada elemento represente para la operación de la organización, Los inventarios que se sugieren son sobre: Sistemas de Información Críticos, Hardware de Redes, servidores, usuarios y comunicaciones, Software y relaciones entre cada uno de estos elementos, con la finalidad de tener una visión de lo que se tiene en la organización como lo sugiere ITIL. Adicionalmente se recomienda tener un inventario de lo mínimo necesario en materia de tecnología para Restaurar la Operación a un nivel aceptable en un escenario de contingencia. Este inventario debe estar contemplado en el análisis financiero para el Programa de Continuidad del Negocio.

- **Registros Vitales:** Además de la tecnología, de la información y del personal que apoyará en la continuidad de la operación, es necesario tomar en cuenta algunos recursos necesarios para que las tareas puedan realizarse, como:
  - ✓ Hojas membretadas.
  - ✓ Formatos necesarios para llevar a cabo alguna tarea.
  - ✓ Documentos que fueron entregados algún día y que se necesiten para el trabajo diario.
  - ✓ Documentos legales como contratos de los proveedores.

  Todos estos ejemplos son identificados como registros vitales. Para contar con ellos en un escenario de contingencia, dónde lo más factible es continuar con la operación en un sitio alterno, se debe asegurar que los registros vitales estén disponibles. Algunas de las recomendaciones para solucionar este requerimiento son:
  - ✓ Contratar los servicios de un proveedor especializado en este tema.
  - ✓ Tener instalaciones alternas que sirvan como bóveda para el resguardo de este tipo de recursos, actualmente existen en el mercado proveedores encargados de este tema.

- **Protección Civil:** Esta estrategia presenta afinidad con la NFPA 1600. La organización debe tener la capacidad de dar la seguridad necesaria a sus empleados aún, en caso de contingencia, para ello es necesario contar con capacitación en tema de protección civil. Actualmente existen organizaciones especializadas en preparar equipos de trabajo para protección civil dentro de las organizaciones. Para este punto, se sugiere organizar un equipo que este encargado de esta tarea dentro de la organización y que reciba capacitaciones de un proveedor especialista en el tema.

4.2.5 Definición de responsabilidades y desarrollo de los Planes de Contingencia

En esta fase, es necesario situar todas las soluciones, estrategias y pasos en un solo plan. Es decir, una vez que las estrategias han sido definidas, deben ser documentadas y puestas en marcha por los encargados de la continuidad de negocio de la organización. Así los esfuerzos pasan de una fase de planificación a una fase de acción e implementación en la que se pretende gestionar la respuesta a incidentes y asegurar la continuidad de las actividades críticas.

- **Definir los cargos o los equipos necesarios para la activación del Plan de Contingencia**

La composición y el número de cargos o equipos que intervienen en la ejecución del plan pueden variar en función del tamaño de la organización y de su estrategia de recuperación. Es posible destacar funciones claves que serán llevadas a cabo por los responsables (personas o equipos, dependiendo del tamaño y de los recursos de la empresa) de la activación y ejecución del Plan de Continuidad de Negocio:

- **Respuesta a incidentes:** Responsables de analizar y acotar el impacto que una incidencia puede provocar en la organización de forma que no se tenga que recurrir a la activación del Plan de Continuidad de Negocio.
- **Comité de crisis:** Encargado de activar el Plan de Continuidad de Negocio y dirigir las acciones durante la contingencia.
- **Equipo de alerta:** Comunicación rápida y efectiva con los servicios civiles de emergencia necesariamente localizables en caso de catástrofe (como por ejemplo los bomberos) que generalmente constituyen la primera figura de respuesta.
- **Logística:** Responsable de reunir todos los medios (lugar alternativo de trabajo, material, herramientas, etc.) necesarios para contribuir a la reactivación de la actividad.
- **Recuperación:** Asume la recuperación en servicio de la infraestructura tecnológica (sistemas, aplicaciones y líneas de comunicación).
- **Relaciones públicas:** Responsable de las comunicaciones con clientes, accionistas, medios de comunicación, etc.

Esta designación de funciones es semejante a las que se establecen en los planes de emergencia encuadrados en la Ley de Prevención de Riesgos Laborales (y sus correspondientes desarrollos reglamentarios), en las que intervienen personas encargadas de poner en práctica diferentes medidas como: gestionar las alertas para la acción de los equipos de primera intervención, dar la alarma para facilitar la evacuación de los empleados, gestionar la coordinación y la cooperación entre los integrantes de los diferentes equipos de emergencia, etc. Una vez que se han definido los cargos o equipos, así como las funciones a desempeñar por los mismos, se deben desarrollar los planes o procedimientos de contingencia a seguir.

- **Desarrollar los Planes de Contingencias Tecnológicos**

En el caso de que la contingencia tenga que ver tecnologías de información, se ha de diseñar un Plan de Contingencias Tecnológico o Disaster Recovery Plan (DRP), que contemple las definiciones, responsabilidades y actividades que debe ejecutar el Área de Tecnología para recuperar las aplicaciones o servicios críticos ante escenarios de fallas tecnológicos, permitiendo así la continuidad de las operaciones. A continuación se explica cómo desarrollar un plan de estas características:

Definición de roles y responsabilidades del DRP:

Director del DRP:

- Responsable por la vigencia y mantención del DRP, respecto de los alcances, estrategia y actualización de los procedimientos relacionados con la recuperación de los servicios y continuidad de los procesos.
- Debe proveer los recursos para la capacitación del personal involucrado, con el fin de contar con personal entrenado adecuadamente para el cumplimiento de cada rol asignado en el procedimiento.

Coordinador Técnico DRP:

- Encargado de coordinar las actividades técnicas de recuperación tecnológica.
- Debe actuar como observador durante la realización de pruebas, con el fin de detectar y corregir deficiencias del DRP y como supervisor en el caso de activarse.
- Debe velar porque los integrantes del DRP, cuenten con el entrenamiento y especialización técnica necesarios para llevar a cabo correctamente las tareas de recuperación de los servicios.
- Debe detectar las necesidades de capacitación y solicitar el entrenamiento respectivo.
- Debe velar por la actualización y vigencia de los procedimientos técnicos asociados al DRP exigiendo a cada encargado el cumplimiento de esta obligación.
- Es responsable de mantener actualizados los procedimientos, el hardware y el software requeridos para la recuperación de los sistemas.
- En caso de emergencia es responsable de activar la recuperación de los sistemas habilitando tanto el hardware como el software asociado.

Coordinador de Comunicaciones externas, internas y con proveedores:

- Asume su rol durante la contingencia y es el encargado de la relación con la contraparte técnica. Es el encargado de recoger y canalizar las inquietudes, liberando al grupo de coordinación técnica de la obligación de atender consultas o requerimientos, de tal manera de orientar sus esfuerzos a dar cumplimiento cabal a las actividades descritas en el plan.

- **Desarrollar los Planes de Contingencias Operacionales**

Los Planes de Contingencias Operacionales deben ser concisos, factibles y accesibles a todos aquellos miembros que tienen algún tipo de responsabilidad dentro del plan. Los objetivos y el alcance de cada uno de ellos deben ser documentados, fáciles de leer y entender por todos los miembros implicados, considerando:

- Las actividades y recursos críticos que deben ser recuperados.
- Los tiempos de recuperación de dichas actividades y recursos.
- En qué situación o situaciones debe ser utilizado cada plan.
- Información útil para la gestión de la contingencia (teléfonos, inventarios de proveedores, servicios, direcciones, check list, etc.).

Adicionalmente, se deben detallar claramente las funciones y responsabilidades de los miembros que forman parte activa del Plan de Continuidad de Negocio, así como el método para activar o invocar el mismo (¿bajo qué circunstancias?; ¿quiénes activan el plan?; ¿cómo es activado el plan?).

Además de esto, en el Anexo B, se puede observar a modo de ejemplo un Plan de Contingencia Operacional para una actividad crítica de una Institución Financiera.

Recomendaciones

Para evitar pérdidas de los planes de contingencias deben mantenerse copias de los mismos en diferentes locaciones. Al menos una de estas locaciones debe estar alejada del lugar físico en el que principalmente se desarrollan las actividades críticas de la organización (oficinas o domicilios particulares). También es importante que el BCP esté disponible para las personas que participan en el Plan de Contingencias en diferentes formatos (incluyendo el electrónico y el soporte en papel).

4.2.6 Pruebas, revisión y mantenimiento del BCP

En esta fase se especifican los ejercicios que más a ayuden a verificar la efectividad del Plan de Continuidad de Negocio. Por tal motivo se debe diseñar un Plan de Prueba para cada actividad crítica del BCP, un ejemplo de esto se puede observar en el Anexo C.

Sin importar el tipo de prueba, la repetición y conjunto de actividades que la fundamentan, estas permiten identificar detalles o situaciones que requieren atención.

Es necesario demostrar la efectividad del BCP probando mediante ejercicios: los roles del personal clave, capacidad de recuperación, conocimiento y toma de decisiones en situaciones de crisis.

Las Pruebas y ejercicios se llevan a cabo con la finalidad de cumplir los siguientes objetivos:

- Garantizar que la documentación prevista para ser usada durante eventos o situaciones de crisis, sea validada por la práctica y la evaluación.
- Mantener vigente la documentación de Administración de la Continuidad de Negocio creada en las etapas del ciclo de vida del proceso de BCP.
- Asegurar que los planes se ajusten a los objetivos del negocio, mediante prácticas, auditorías y procesos de auto-evaluación.
- Cumplir con los requerimientos de los procesos clave del negocio (RTO y RPO).
- Familiarizar a los equipos con el proceso de Pruebas de BCP.
- Satisfacer los requerimientos legales y de auditoria interna.

En las diferentes Pruebas que se pueden realizar, se tienen las siguientes:

- **Prueba de escritorio:** Esta prueba permite evaluar un plan sin necesidad de realizar la prueba fuera del edificio, la cual debe realizarse de manera de verificar la consistencia del plan con respecto a algún escenario de interrupción. Además permite validar los datos de los planes.
- **Prueba funcional:** En esta prueba se evalúa la efectividad de los planes que integran el BCP, recreando los procesos de negocio y la participación de los usuarios desde un sitio alterno.
- **Ejercicio Completo:** Permite evaluar la continuidad de las operaciones para un escenario de desastre mayor en el cual se simularía un procesamiento desde el sitio alterno definido en la estrategia de recuperación. Este tipo de prueba permite validar todos los planes de contingencia de manera integrada.

Una vez realizado el ejercicio o prueba, se deben documentar los resultados basados en los cuestionarios de revisión y bitácoras de los participantes. Para este proceso es necesario ordenar todas las evidencias recolectadas después de la prueba o ejercicio y definir planes de acción para administrar los problemas surgidos durante la prueba o ejercicio.

Se sugiere elaborar una reunión con los participantes de la prueba, en la que sea de fácil visualización a través de gráficas comparativas entre resultados anteriores contra los actuales, o un análisis entre los requerimientos y los resultados de la prueba. Estos servirán para identificar áreas de oportunidad.

- **Documentos que deben ser actualizados constantemente**

El BCP contiene puntos importantes que deben ser actualizados constantemente, debido a la innovación que la organización va experimentando, ellos son:

- **Alcance del Plan:** Con el transcurso de los años, el alcance del BCP puede ampliarse, según el crecimiento de la organización.

- **Puntos del BCP alineados a las buenas prácticas:** El programa de Continuidad de Negocio puede modificarse, dependiendo del código de buenas prácticas al cual está alineado, ya sea por cambio de versión o por cambio de un código a otro.
- **Plan de Pruebas:** Al inicio del año, se elabora el plan de pruebas anual del BCP, en el que se definen los ejercicios que se pretenden realizar, con el pasar de los meses es necesario verificar si será posible llevar a cabo dichos ejercicios, en caso contrario, se debe actualizar el Plan de Pruebas que se elaboró al inicio del año.
- **Roles y responsabilidades:** Para el BCP se tiene identificada cierta parte del personal de la organización que participa en éste, dependiendo del cambio de rol de las personas en la operación normal, debe actualizarse el BCP.

Cada uno de los documentos que han sido mencionados, deben ser actualizados cada vez que se identifique un cambio, para que el Plan de Continuidad de Negocio sea eficiente, debe estar al día.

- **Actualización (ciclo de mejora continua)**

Los planes de continuidad de negocio deben ser mantenidos a través de un ciclo de mejora continua. Cualquier cambio a nivel estratégico, operacional o técnico puede impactar en el negocio y por tanto en el plan de continuidad. Consecuentemente, la empresa debe emprender un proceso para mantener al día la capacidad, eficacia e idoneidad del Plan de Continuidad de Negocio. Algunas propuestas en ese sentido son:

- Revisión periódica en busca de cambios en la estructura de la organización, en los productos/servicios que se desarrollan, en la plantilla, etc., los cuales pueden tener consecuencias en el Plan de Continuidad de Negocio (política, BIA, procedimientos de recuperación, etc.).
- Confirmación de que el Plan de Continuidad de Negocio es acorde y contempla los citados cambios en los diversos componentes de la organización.
- Adecuación de los planes de continuidad de negocio a requerimientos de socios, clientes, accionistas u otro tipo de requerimientos regulatorios.
- Revisión de los resultados de las pruebas realizadas y de que las mejoras identificadas en las mismas han sido aplicadas.
- Auditorías internas o externas de todos y cada uno de los componentes del Plan de Continuidad de Negocio.

En el caso de que se evidencien cambios que afecten a la organización y que tengan impacto en los procesos de negocio, puede ser necesario revisar los Análisis de Impacto en el Negocio (BIA) y Análisis de Riesgos para ver en qué medida dichos cambios pueden provocar desajustes en las estrategias y los

procedimientos. De esta forma, la organización puede disponer de ciertas garantías sobre la efectividad de su plan de continuidad de negocio.

Finalmente para asegurar el mantenimiento del Plan de Continuidad de Negocio es recomendable el desarrollo de programas educativos que mezclen diferentes formas de comunicación y aprendizaje de forma que sea fácilmente asimilable por toda la organización. Por otro lado, y como medida general, se recomienda que los planes de continuidad de negocio, aparte de ser flexibles, sean testados al menos una vez al año a través de la realización periódica de simulacros que reproduzcan de forma ficticia situaciones de emergencia o contingencia. Dicha periodicidad depende de las necesidades que determine la organización y el entorno en el que opera.

4.3 Análisis de la cultura organizacional chilena y la incorporación de la cultura de BCP a ésta.

En esta fase se desea obtener en el personal una concientización sobre los beneficios que se obtienen, cuando se cuenta con una cultura de prevención, además de proporcionarles seguridad ante una situación que requiera el uso del BCP, para esto y de acuerdo con el análisis de la información recopilada en cuanto a la cultura organizacional chilena, la forma en la que se debe entregar las tareas y obligaciones a los demás, deben ser de una forma impersonal y formal, también la gran importancia de la delegación de autoridad y toma de decisiones que han de tener los colaboradores debe ser significativa, con lo cual se busca obtener que los colaboradores se sientan parte de la empresa y como un recurso valioso para la misma.

Antes de impartir cualquier acción de formación o concientización, es necesario que la organización determine los colectivos y grupos objetivos, qué tipo de necesidades formativas son requeridas y qué estrategia de comunicación es la más adecuada, un ejemplo de esto puede ser observado en el Anexo D, para lograr la incorporación del BCP a la organización, se pueden utilizar diversos medios en la difusión efectiva de los paquetes formativos, como por ejemplo: la inclusión de mensajes y contenidos relacionados con la continuidad de negocio en la Intranet de la organización, las plataformas online y/o soportes semejantes, etc.

Los responsables deben ser adecuadamente formados y concientizados acerca de los diferentes conceptos que contempla la continuidad de negocio (riesgos, medidas preventivas, detección temprana de incidencias, etc.). Incluso cabe la posibilidad de extender estos programas de formación a proveedores o en general a terceros con los que la organización mantiene relaciones comerciales.

En esta fase se sugiere desarrollar un programa de cultura para el BCP que contenga los siguientes puntos:

- Definición de responsabilidades.

- Actividades que fortalezcan las habilidades del personal.
- Organización de talleres para la concientización del personal.
- Capacitación para el desarrollo de habilidades necesarias para trabajar en una situación de crisis.
- Planes de ejercicios.
- Involucrar al personal en la solución de incidentes resultantes de la prueba.

Finalmente cabe destacar, que entre más incorporada esté la cultura de BCP en la operación normal, mayor capacidad de continuidad de negocio tendrá la organización, ya que una cultura positiva lograda con el desarrollo de un programa de cultura eficiente, puede ayudar a infundir confianza en los trabajadores, socios del negocio y clientes de la organización.

A continuación se presenta una Figura Nº 4.3 con las principales características de la cultura organizacional chilena y la implicancia que esta tendría sobre el plan de continuidad de negocio.

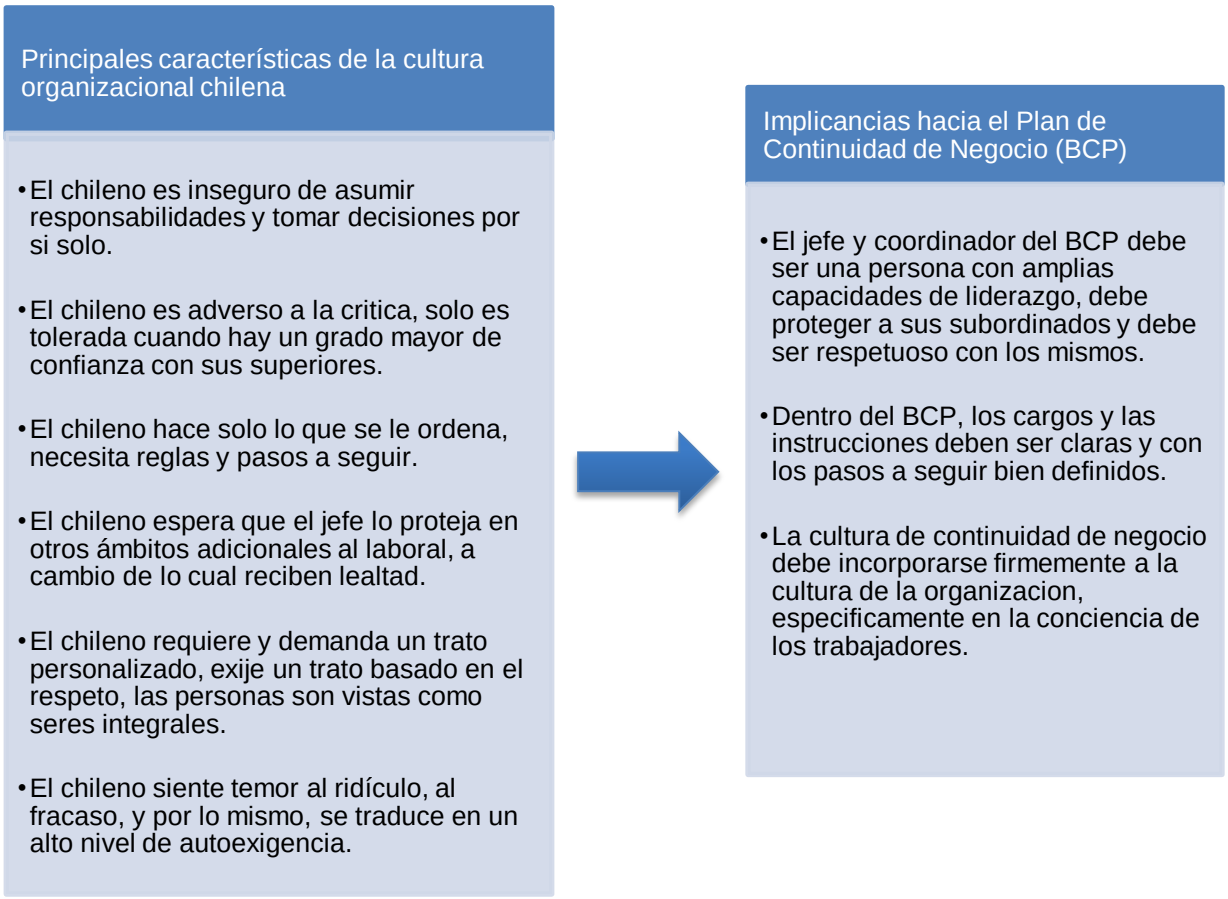

Figura Nº 4.3: Relación de la cultura organizacional chilena con el Plan de Continuidad de Negocio.

Fuente: Elaboración propia.

4.4 Propuesta metodológica para la implementación de un Plan de Continuad de Negocio en Chile.

A continuación a modo de resumen, se puede apreciar en la Figura Nº 4.4, los principales elementos de cada fase, pertenecientes al modelo propuesto en este trabajo de grado.

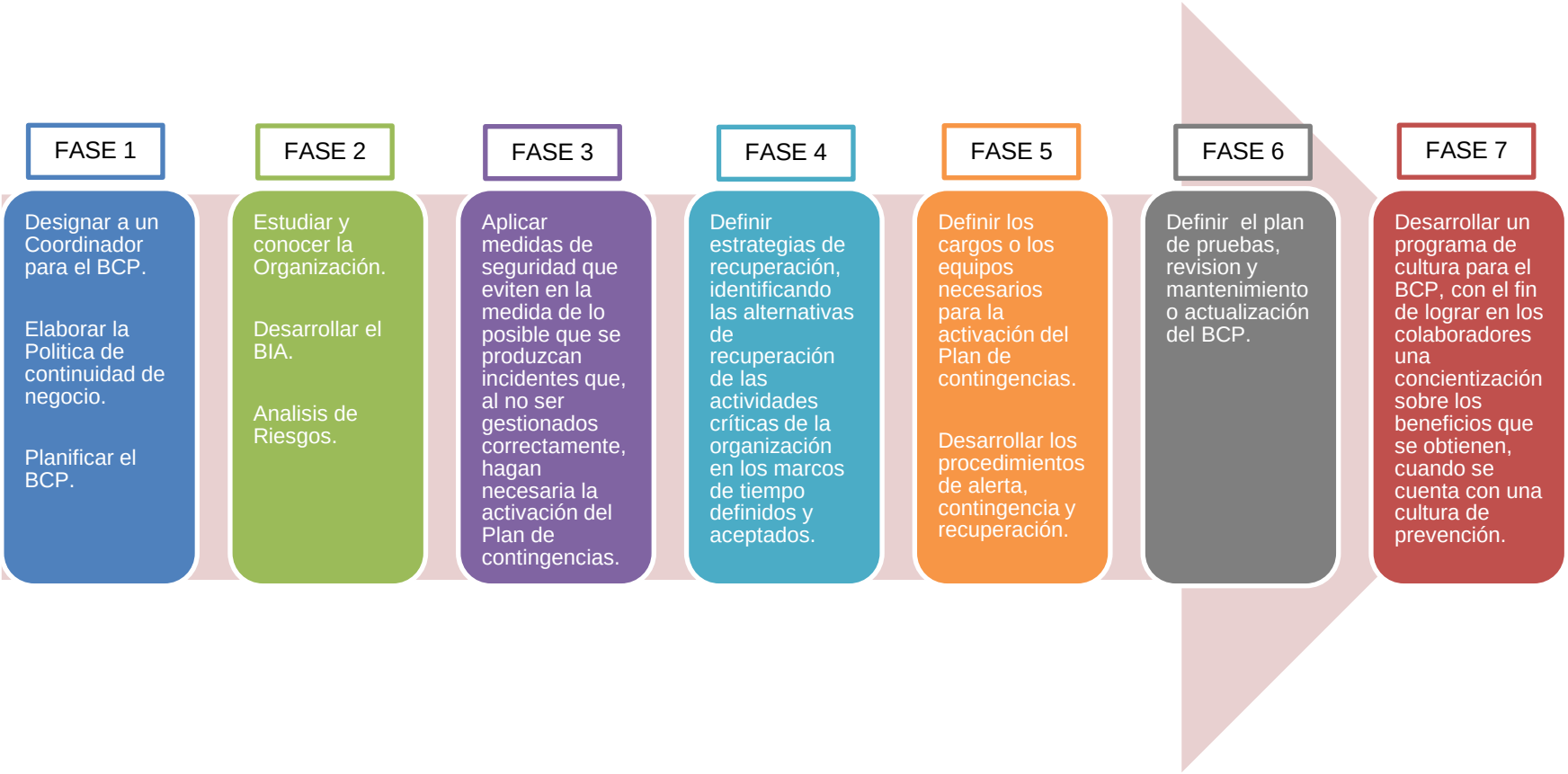

Figura Nº 4.4: Resumen del Modelo propuesto para el BCP.

Fuente: Elaboración propia.

4.5 Análisis de Resultados

Los resultados obtenidos se pueden medir de acuerdo al cumplimiento de los objetivos.

4.5.1 Acerca del Objetivo General de la Investigación

- **Crear una propuesta metodológica para la implementación de un Plan de Continuad de Negocio en Chile:** se logró realizar una metodología para la implementación de un Plan de Continuidad de Negocio expresada en el punto 4.1 de este trabajo de grado, todo gracias a un extenso análisis de la metodologías existentes a nivel mundial, para tomar los puntos más fuertes de cada uno.

4.5.2 Acerca de los Objetivos específicos de la investigación

- **Analizar las metodologías existentes y estándares internacionales para la implementación de un Plan de Continuidad de Negocio y extraer sus principales fortalezas:** esto se realizó en los puntos 2.3 y 2.4, en donde se describen las principales metodologías existentes para la elaboración de un BCP y en el punto 4.1 se realizó un análisis de estas para identificar sus fortalezas y así aprovecharlas al máximo.

- **Identificar las actividades necesarias para diseñar, implementar y mantener un Plan de Continuidad de Negocio (BCP) en Chile:** se identificaron las actividades necesarias para diseñar, implementar y mantener un BCP, principalmente a través de los estándares internacionales como la norma ISO 22301 y el BS 25999.

- **Analizar la cultura organizacional de las empresas chilenas, con el fin de detectar las características más importantes, para así aprovecharlas al momento de la implementación y gestión del BCP:** esto se realizó en el punto 2.2.5, en donde se recopiló información de varios autores, además de un estudio basado en una encuesta, todo esto con el fin de obtener una percepción clara de la cultura organizacional que está viviendo Chile, en donde se pudo apreciar que esta ha ido cambiando bastante en estos últimos años, en la cual se acentúa más el individualismo que el trabajo en grupo.

CONCLUSIONES Y RECOMENDACIONES

En conclusión se ha logrado concretar los objetivos, creando una propuesta metodológica para la implementación de un Plan de Continuad de Negocio en Chile, en donde se analizaron y se evaluaron las características principales de la cultura organizacional chilena con el fin de identificar y aprovechar aquellas positivas y tratar de evitar las negativas, de acuerdo con esto se pudo apreciar que esta ha ido cambiando bastante en estos últimos años, en la cual se acentúa más el individualismo que el trabajo en grupo. Se analizaron también las metodologías utilizadas a nivel mundial en la actualidad para implementar un BCP, con el objetivo de extraer lo mejor de cada una, en donde se pudo establecer como base para este trabajo de grado el ciclo de vida del BCP expuesto por el estándar internacional BS 25999 y la norma ISO 22301. Además la metodología de este trabajo de grado comprendió un análisis teórico sobre: administración de proyectos, administración de riesgos, comportamiento organizacional, cultura corporativa, y liderazgo, ya que estos apoyan de forma directa los proyectos empresariales, ligados a la influencia que tiene la cultura en la administración, además es importante mencionar que para realizar el BCP, es importante analizar al negocio como un todo mas no como procesos, actividades o funciones individuales, ya que éste es un sistema dinámico, constantemente en cambio y en adaptación a las presiones internas y externas, y está en un proceso continuo de evolución.

La historia y el presente evidencian problemas de continuidad de negocios en las empresas chilenas; las amenazas están presentes en el país. En este punto se detecta la oportunidad de desarrollar este tema, incorporándolo en los planes de estudio de carreras relacionadas con esta área, creación de consultorías, o la creación de un organismo a nivel nacional para difundir, capacitar y certificar los estándares relacionados con el BCP.

Así como no hay dos organizaciones iguales, no hay dos planes de continuidad de negocio iguales. Es decir, un mismo plan, desarrollado por dos equipos diferentes o en dos momentos diferentes, no tiene por qué coincidir. Con ello se advierte que, si bien la propuesta metodológica proporciona unas pautas a seguir, el contenido que se dé a cada fase, será función no solamente de la organización en cuestión, sino de una serie de parámetros que probablemente variarán de acuerdo con los objetivos individuales de la organización en particular y de las premisas que se establezcan en los pasos iniciales.

Para comenzar con la implementación de un Plan de Continuidad de Negocios es fundamental contar con el apoyo de la alta dirección, a través del convencimiento de la importancia del tema, las ventajas que se obtendrán y el valor agregado que traerá consigo su puesta en marcha. Luego, es importante avanzar apoyándose en los marcos normativos existentes, comenzar por las áreas más críticas de la compañía y certificar en función de los intereses de la organización.

Además en la elaboración del BCP las etapas iniciales de “evaluación de amenazas y riesgos” y “análisis de impacto en el negocio” BIA, forman la base del Plan .Estas entregan la información con la cual se

trabaja en el Plan, si se realiza una deficiente evaluación de riegos, el BIA así como los planes derivados serán deficientes. Se debe tener presente que es imposible detectar todas las amenazas, así como que tampoco van a desaparecer por el solo hecho de tener un BCP, si no que se debe convivir con ellas en todos los procesos de la organización, con la diferencia de que el BCP permite mitigar su impacto cuando ellas aparezcan.

Finalmente queda señalar que en la propuesta se han agregado puntos específicos en cada fase, sugeridos sobre cómo aplicar el Plan de Continuidad de Negocio, reforzándolo con puntos que, por investigaciones, van a funcionar de forma muy eficiente y eficaz. Con lo anterior se tiene como resultado una Metodología para la implementación y desarrollo de un Plan de Continuidad de Negocio.

BIBLIOGRAFÍA

- ABARCA N., MAJLUF N. y RODRÍGUEZ D., 1998. Identifying Management in Chile: A Behavioral Approach. USA, M.E. Sharpe. pp. 18 - 37.

- BASS B., 1997. Personal Selling and Transactional/ Transformational Leadership, Journal of Personal Selling & Sales Management 17(3): 19-28.

- BASSI E., 1999. Globalización de negocios: construyendo estrategias competitivas. México, Editorial Limusa. 175p.

- BCI, 2010. Good Practice Guidelines. 108p.

- BRETONES F. y GONZÁLEZ M., 2009. Well-being, values and responsibility among a sample of Mexican workers. México.

- BSI GROUP, 2006. Business continuity management. Code of practice (BS 25999-1: 2006). Londres, BSI. 50p.

- BSI GROUP, 2007. Business Continuity Management. Specification (BS 25999-2: 2007). Londres, BSI. 50p.

- BSI GROUP, 2008. Information and communications technology continuity management. Code of practice (BS 25777: 2008). Londres, BSI. 40p.

- HOJMAN D. y PÉREZ G., 2005. Cultura nacional y cultura organizacional en tiempos de cambio: la experiencia chilena. Revista latinoamericana de administración (35): 87 – 105.

- DAFT R., 2006. La experiencia del liderazgo. 3ª ed. México, Cengage Learning, 720p.

- DÁVILA A. y ELVIRA M., 2005. Cultura y Administración de Recursos Humanos en América Latina. Universia Business Review (5): 28 - 45.

- DE LARA A., 2005. Medición y control de riesgos financieros. 3ª ed. México, Limusa. 219p.

- DRII y DRJ, 2007. Generally Accepted Practices. 163p.

- DRJ, 2012. Emergency Operations Center (EOC). 23p.

- FORSBERG K., MOOZ H. y COTTERMAN H., 2000. Visualizing Project Management: A Model for Business and Technical Success. 2ª ed. USA, John Wiley & Sons. 354p.

- GALINDO L. 2008. Metodología para la Creación de la Tabla Metodológica o Solución Integral. En: 3er CONGRESO INTERNACIONAL de Metodología de la Ciencia y la Investigación para la Educación junio de 2008. México, Asociación Mexicana de Metodología de la Ciencia y de la Investigación, A.C. y CFIE del IPN.

- GASPAR J., 2004. Planes de contingencia: la continuidad del negocio en las organizaciones. España, Ediciones Díaz de Santos. 220p.

- GIL F., 1990. Liderazgo. México, Instituto de Capacitación Política.

- GONZÁLEZ J., MONROY A. y KUPFERMAN E., 1994. Dinámica de Grupos: Técnicas y Tácticas. México, Editorial Pax México. 134p.

- HILL C. y GARETH J. 2011. Administración Estratégica, Un Enfoque Integrado. 9ª ed. México, Cengage Learning. 250p.

- HOFSTEDE G., HOFSTEDE G. y MINKOV M., 2010. Cultures and Organizations: Software of the Mind, Third Edition. 3ª ed. USA, McGraw Hill. 576p.

- HUSE E. y BOWDITCH J. 1980. El comportamiento humano en la organización. México, Fondo Educativo Interamericano. 439p.

- ISO, 2005. ISO 27002: 2005 Information technology - Security technique - Code of practice for information security management. 115p.

- ISO, 2012. ISO 22301:2012 Societal security - Business continuity management systems - Requirements. 24p.

- KOUZES J. y POSNER B. 2007. Inventario de Prácticas de Liderazgo. 3ª ed. USA John Wiley & Sons. 104p.

- MARTÍNEZ J., 2001. Introducción al análisis de riesgos. México, Editorial Limusa. 218p.

- MOSTERÍN J., 2009. La Cultura Humana. Madrid, Espasa. 404p.

- MUR A., 2013. El incendio del Edificio Windsor un caso real. En: CONFERENCIA UPM TASSI: Planes de Contingencia, 20 de febrero 2013. Madrid, Universidad Politécnica de Madrid.

- NFPA, 2013. NFPA-1600 Standard on Disaster/Emergency Management and Business Continuity Programs. USA, NFPA. 58p.

- OPS, Organización Panamericana de la Salud, 2010. El terremoto y tsunami del 27 de febrero en Chile: Crónica y lecciones aprendidas en el sector salud. Santiago, 109p.

- ROBBINS S., 2004. Comportamiento organizacional. 10ª ed. Madrid, Pearson Educación. 675p.

- RODRÍGUEZ D. 2008. Gestión Organizacional: Elementos para su estudio. 4ª ed. Chile, Ediciones Universidad Católica de Chile. 295p.

- RODRÍGUEZ J. y GÓMEZ C. 2009. HRM in Chile: the impact of organizational culture. Employee Relations 31 (3): 276 - 294.

- WOODMAN P., 2007. Business continuity Management. Reino Unido, Chartered Management Institute. 20p.

- XXII CONGRESO Y FERIA IBEROAMERICANA de seguridad de la información: 22 de agosto de 2012. W Santiago Hotel, Chile. USUARIA.

LINKOGRAFÍA

- BANCO CENTRAL DE CHILE [en línea] <http://www.bcentral.cl/licitaciones/pdf/2008/L09002bases.pdf> [consulta: 16 mayo 2013].

- BSI GROUP, 2012. Bankinter recibe el primer certificado ISO 22301 emitido por BSI [en línea] <http://www.bsigroup.es/es/certificacion-y-auditoria/Sistemas-de-gestion/Novedades/Noticias-2012/LD-News-Source-/Bankinter-recibe-el-primer-certificado-ISO-22301-emitido-por-BSI/> [consulta: 20 junio 2013].

- BSI GROUP, 2013. Continuidad de Negocio ISO 22301 [en línea] <http://www.bsigroup.es/certificacion-y-auditoria/Sistemas-de-gestion/estandares-esquemas/Continuidad-de-Negocio-BS25999/> [consulta: 24 febrero 2013].

- CASO FARMACIAS: $ 255 millones a organizaciones benéficas cierran arista penal. [en línea] Diario Financiero en Internet. 09 de julio 2013. <http://www.df.cl/caso-farmacias-255-millones-a-organizaciones-beneficas-cierran-arista-penal/prontus_df/2013-07-08/211847.html> [consulta: 09 julio 2013].

- CHILE POTENCIA ALIMENTARIA, 2008. Japón y Corea del Sur reactivan importaciones de carnes de cerdo. [en línea]. <http://www.chilepotenciaalimentaria.cl/content/view/397156/Japon-y-Corea-del-Sur-reactivan-importaciones-de-carnes-de-cerdo.html> [consulta: 05 junio 2013].

- DACCACH JOSÉ, 2007. Administración de Proyectos. [en línea] artículo en Delta Asesores <http://www.deltaasesores.com/articulos/gestion-de-proyectos/349-administracion-de-proyectos-i-> [consulta: 20 octubre 2012].

- DIRECTORIO ISO 27000, sección ISO 27002 [en línea] <http://www.27000.org/iso-27002.htm> [consulta: 9 mayo 2013].

- ESCALERA JORGE, 2011. ¿Qué es Administración de Riesgos Empresarial (ERM) y Administración de la Continuidad del Negocio (BCM)? [en línea] artículo en Risk México <http://www.riskmexico.com/articulos/administracion-de-riesgos-empresarial/> [consulta: 15 abril 2013].

- ITEAM consultora especializada en Planes de Continuidad de Negocio, Plan de Manejo de Crisis y Riesgo Empresarial [en línea] <http://www.iteam.com.co/index.php?option=com_content&view=article&id=10%3Ariesgos-que-pueden-impactar-negativamente-las-operaciones-normales-de-una-empresa&catid=1%3Aiteam&Itemid=8> [consulta: 20 abril 2013].

- ITEAM consultora especializada en Planes de Continuidad de Negocio, Plan de Manejo de Crisis y Riesgo Empresarial [en línea] <http://www.iteam.com.co/index.php?option=com_content&view=article&id=12%3Aique-es-un-plan-de-continuidad-de-negocio&catid=1%3Aiteam&Itemid=8> [consulta: 20 abril 2013].

- LONG GIDEON, 2009. El Golpe de la Tormenta Perfecta. [en línea] Revista Business Chile en Internet. 01 de mayo, 2009. <http://www.businesschile.cl/es/noticia/salmon/el-golpe-de-la-tormenta-perfecta> [consulta: 18 mayo 2013].

- OSIATIS, ITIL V3 Gestión de la Continuidad de Servicios TI [en línea] <http://itilv3.osiatis.es/diseno_servicios_TI/gestion_continuidad_servicios_ti.php> [consulta: 02 mayo 2013].

- PALACIOS MIGUEL, 2009. Arquitectura de Máxima Disponibilidad (MAA): Continuidad de Negocios (CN) [en línea]. Perú. <http://www.peoug.org/docs/18-03-2009/EventoGB_Marriot_18Marzo2009_Continuidad_de_Negocio_withROI.pdf> [consulta: 15 abril 2013].

- PJR, Perry Johnson Registrars [en línea] <http://www.pjr.com/spanish/bs25999.htm> [consulta: 08 mayo 2013].

- RAGA FERNANDO, 2009. El Sector Forestal Chileno y sus riesgos. [en línea] Revista Trébol de Mapfre en Internet. 07 de diciembre, 2009. <http://www.mapfre.com/mapfrere/docs/html/revistas/trebol/n51/docs/Articulo2.pdf> [consulta: 19 junio 2013].

- ROMERO ARTURO, 2008. La cultura, los valores empresariales y el cambio [en línea] artículo en Gestiópolis <http://www.gestiopolis.com/administracion-estrategia/cultura-valores-empresariales-y-el-cambio.htm> [consulta: 18 marzo 2013].

- SQUIEBRAS, Superintendencia de Quiebras Chile [en línea] <http://www.squiebras.gob.cl/images/stories/documentos/informacion_estadisticas/generales/Cifras_31.12.2012.pdf> [consulta: 16 mayo 2013].

- ZIMMERMAN ANN y BAUERLEIN VALERIE, 2005. Wal-Mart respondió a Katrina mejor que el gobierno de USA. [en línea] Foro de Seguridad en Internet. <http://www.forodeseguridad.com/artic/admin/5228.htm> [consulta: 20 junio 2013].

ANEXOS

Anexo A: Ejemplo de registro de las actividades críticas.

Sucursal	Sub-Proceso	Nº	Actividad crítica
El Bosque	Liquidación Banco	1	Realizar Factibilidad Liquidez Intradía (FLI)
	Pago de Obligaciones a la vista y a Plazo	2	Pagar por MDP
	Formalizar el Negocio Colocaciones y Captaciones	3	Visado comercial
		4	Curse comercial
		5	Visado Consumo
		6	Curse Consumo
		7	Visado Hipotecario
		8	Curse Hipotecario (Desembolso)
Mac Iver	Administrar y dar Seguimiento Productos Financieros	9	Vencimiento cupones
		10	Vencimiento derivados
		11	Cuadratura carteras
	Recaudar Colocaciones Comerciales y de Personas	12	Apertura Contable
		13	Envío diario cartera para recaudación (automático)
		14	Subir nómina de recaudación hipotecario (Fisa)

Anexo B: Ejemplo de Plan de Contingencia Operacional para una actividad crítica.

Nombre Actividad Crítica	**Curse Hipotecario (Desembolso)**				
Nombre del Sub-Proceso	**Formalizar el Negocio Colocaciones y Captaciones**				
Vigencia				**Fecha de Inicio**	07-2013
	Versión	1.0		**Fecha Última Actualización**	07-2013
Frecuencia Prueba Procedimiento	Anual				
Redactado por			**Fecha**		
Aprobado por			**Fecha**		
Tiempo Máximo de Espera para Activación de Proceso en Contingencia	1 Día		**Tiempo Requerido de ejecución Proceso en contingencia**	Depende de la carga de trabajo	
Responsable de Activación	Supervisor emisión hipotecario		**Back up**	Subgerente de Operaciones	
Coordinador del procedimiento	Supervisor emisión hipotecario		**Back up**	Subgerente de Operaciones	
Usuario Crítico	Ejecutivo Revisor	**Back up 1**	Administrativo de Operaciones	**Back up 2**	Asistente Administrativo
Áreas a ser Notificadas	• Tesorería • Gerencia de Operaciones y Control Financiero • Gerencia Comercial				

Escenario 1: Indisponibilidad de Usuario Crítico.

Estrategia de Recuperación

Se asigna la labor al Back Up 1, Administrativo de Operaciones, el cual posee las capacidades para realizar la actividad crítica.

Condiciones Previas	**Responsable**
Disponer de los siguientes recursos: • SINACOFI • Microsoft Office • Office Banking • FISA • Motor de pago • Work-Flow Cibergestión • Planillas de mutuos por pagar • G.L. • Internet.	Supervisor emisión hipotecario

Procedimiento de Contingencia	**Ejecutor**
1. Busca los documentos: Pago de Mutuos (Detalle).pdf y Pago de Mutuos (Flujo).pdf 2. Sigue las instrucciones contenidas en los documentos.	Administrativo de Operaciones Back up 1

Transición a la Normalidad	**Responsable**
Una vez finalizada la contingencia, el Ejecutivo Revisor Back up 1, hace entrega de las funciones al usuario crítico, Ejecutivo Revisor.	Asistente Administrativo Back up 1

Escenario 2: Indisponibilidad de Instalaciones.	
Escenario 2.1: Usuario Crítico se traslada a lugar de contingencia.	
Estrategia de Recuperación	
El Usuario crítico se traslada al lugar de contingencia para realizar la actividad crítica.	
Condiciones Previas	**Responsable**
El lugar de Contingencia debe disponer de los siguientes recursos: • SINACOFI • Microsoft Office • Office Banking • FISA • Motor de pago • Work-Flow Cibergestón • Planillas de mutuos por pagar • G.L. • Internet.	Supervisor emisión hipotecario
Procedimiento de Contingencia	**Ejecutor**
1. Envía al usuario crítico, Ejecutivo Revisor, al lugar de contingencia. 2. Da a conocer a las áreas interesadas, las que deben ser notificadas por medio de correo electrónico, que se estará en contingencia operacional (envío de documentación al lugar de contingencia).	Supervisor emisión hipotecario
Transición a la Normalidad	**Responsable**
1. Da a conocer a las áreas interesadas, las que deben ser notificadas por medio de correo electrónico, que se vuelve a la normalidad y se termina el proceso de contingencia.	Supervisor emisión hipotecario

Escenario 2.2: Usuario Back Up 2 realiza la operación sin asistencia telefónica.	
Estrategia de Recuperación	
El Back Up 2 ubicado en el lugar de contingencia, realiza la actividad crítica sin la necesidad de la asistencia telefónica.	
Condiciones Previas	**Responsable**
El lugar de trabajo del Usuario Back Up 2 debe disponer de los siguientes recursos: • SINACOFI • Microsoft Office • Office Banking • FISA • Motor de pago • Work-Flow Cibergestón • Planillas de mutuos por pagar • G.L. • Internet	Supervisor emisión hipotecario
Procedimiento de Contingencia	**Ejecutor**
1. Se contacta con el usuario Back Up 2, Asistente Administrativo, para que realice las operaciones. 2. Da a conocer a las áreas interesadas, las que deben ser notificadas por medio de correo electrónico, que se estará en contingencia operacional (envío de documentación al lugar de contingencia).	Supervisor emisión hipotecario
3. Realiza las actividades definidas, en el procedimiento de contingencias del escenario 1.	Asistente Administrativo Back up 2
Transición a la Normalidad	**Responsable**
1. Informa al Back Up 2 cuando las instalaciones están disponibles, para que este finalice sus actividades. 2. Informa al Usuario crítico, la disponibilidad de las instalaciones. 3. Da a conocer a las áreas interesadas, las que deben ser notificadas por medio de correo electrónico, que se vuelve a la normalidad y se termina el proceso de contingencia.	Supervisor emisión hipotecario

Escenario 2.3: Usuario Back Up 2 realiza la operación con asistencia telefónica.	
Estrategia de Recuperación	
El Back Up 2 ubicado en el lugar de contingencia, realiza la actividad crítica con la necesidad de la asistencia telefónica.	
Condiciones Previas	**Responsable**
El lugar de trabajo del Usuario Back Up 2 debe disponer de los siguientes recursos: • SINACOFI • Microsoft Office • Office Banking • FISA • Motor de pago • Work-Flow Cibergestón • Planillas de mutuos por pagar • G.L. • Internet	Supervisor emisión hipotecario
Procedimiento de Contingencia	**Ejecutor**
1. Da a conocer a las áreas interesadas, las que deben ser notificadas por medio de correo electrónico, que se estará en contingencia operacional (envío de documentación al lugar de contingencia).	Supervisor emisión hipotecario
2. Se contacta con el usuario Back Up 2, Asistente Administrativo, para que realice las operaciones y le brinda asistencia telefónica	Ejecutivo Revisor
3. Realiza las actividades definidas, en el procedimiento de contingencias del escenario 1.	Asistente Administrativo Back up 2
Transición a la Normalidad	**Responsable**
1. Informa al Back Up 2 cuando las instalaciones están disponibles, para que este finalice sus actividades. 2. Da a conocer a las áreas interesadas, las que deben ser notificadas por medio de correo electrónico, que se vuelve a la normalidad y se termina el proceso de contingencia.	Supervisor emisión hipotecario

Escenario 3: Indisponibilidad de Sistema.	
Estrategia de Recuperación	
Revisar inventario de Contabilidad para realizar las operaciones.	
Condiciones Previas	**Responsable**
Disponer de los siguientes recursos: • SINACOFI • Microsoft Office • Office Banking • Work-Flow Cibergestón • Planillas de mutuos por pagar • Internet.	Supervisor emisión hipotecario
Procedimiento de Contingencia	**Ejecutor**
1. Da a conocer a las áreas interesadas, las que deben ser notificadas por medio de correo electrónico, que se estará en contingencia operacional.	Supervisor emisión hipotecario
2. Realiza las actividades contenidas en el procedimiento de contingencias del escenario 1 con la información contenida en el inventario de contabilidad.	Ejecutivo Revisor
Transición a la Normalidad	**Responsable**
1. Una vez recuperado el sistema, se vuelve a la trabajar con normalidad y se informa a las áreas interesadas.	Supervisor emisión hipotecario

Escenario 4: Indisponibilidad de Proveedor.	
Estrategia de Recuperación	
Realizar las operaciones que eran realizadas por el proveedor de servicios con personal interno de la empresa capacitado para realizar las labores requeridas.	
Condiciones Previas	**Responsable**
Disponer de los siguientes recursos: • SINACOFI • Microsoft Office • Office Banking • FISA • Motor de pago • Planillas de mutuos por pagar • G.L. • Internet.	Supervisor emisión hipotecario
Procedimiento de Contingencia	**Ejecutor**
1. Da a conocer a las áreas interesadas, las que deben ser notificadas por medio de correo electrónico, que se estará en contingencia operacional.	Supervisor emisión hipotecario
2. Realiza las operaciones que eran ejecutadas por el proveedor de servicios.	Ejecutivo Revisor
Transición a la Normalidad	**Responsable**
1. Una vez recuperado los servicios del proveedor, se vuelve a trabajar con normalidad y se informa a las áreas interesadas.	Ejecutivo Revisor

Anexo C: Ejemplo de un Plan de Pruebas

PLAN DE PRUEBA PARA PLAN DE CONTINUIDAD OPERACIONAL
Curse Hipotecario (Desembolso)

Tamaño de la muestra para realizar la prueba:

La actividad crítica se realizará en cada escenario, bajo el Procedimiento de Contingencia definido en la Ficha de Continuidad Operacional correspondiente a la actividad crítica, y el tamaño de la muestra será una operación.

Descripción:

Quien realiza la prueba debe actualizar planilla de Provisión de Pagos, enviar solicitud de Fondos a Tesorería para provisionar, obtener fichas resumen de firmas de escrituras, verificar y completar planilla de Pago de Mutuos desde el resumen de firmas de escrituras, ingresar datos a planilla de Proveedores, ingresar a sistema Toolkit para importar nómina de proveedores, finalmente cargar nómina de proveedores a sistema Office Banking y validar.

Ante la indisponibilidad de sistema FISA, revisar inventario de Contabilidad para realizar las operaciones.

Ante la indisponibilidad de Proveedor, realizar las operaciones que eran realizadas por el proveedor de servicios con personal interno de la empresa capacitado para realizar las labores requeridas.

Resultado esperado:

Envío de memorándum a Subtesorero para su visación.

Escenarios considerados en la prueba:

-Escenario 1
-Escenario 2.1
-Escenario 2.2
-Escenario 2.3
-Escenario 3
-Escenario 4

Participantes:

-Responsable y coordinador de la activación del PCO:
-Usuario Crítico :
-Back up 1 :
-Back up 2 :

Plan de Comunicación interna

1. Objetivo:

Informar y concientizar a todos los colaboradores del Banco sobre las gestiones llevadas a cabo por el Departamento de Gestión de Calidad y Riesgo Operacional en cuanto al Plan de Continuidad de Negocio que se está implementado, además de apoyar la estrategia de la empresa proporcionando coherencia e integración entre los objetivos, los planes y las acciones de la dirección.

2. Información que deberá ser difundida:

A. Definiciones:

- ✓ **Actividad de negocio:** proceso o conjunto de procesos establecidos por una organización para producir o soportar sus productos o servicios.
- ✓ **Estrategia de recuperación:** conjunto de actividades predefinidas que serán implementadas y llevadas a cabo en respuesta a un desastre.
- ✓ **Análisis de Impacto en el Negocio o *Business Impact Analysis*** (BIA): proceso de análisis de las actividades de negocio y las consecuencias que una interrupción sobre las mismas puede provocar en la organización.
- ✓ **Contingencia:** suceso no deseado que afecta a la continuidad normal de las operaciones de la organización.
- ✓ **Desastre:** problema o evento no planificado, cuya consecuencia es la interrupción de los procesos de negocio durante un periodo de tiempo. Este tiempo de paralización de los procesos es superior a lo que la organización puede soportar sin sufrir perjuicios considerables para el negocio.
- ✓ **Indisponibilidad:** característica, cualidad o condición de un proceso de negocio/activo/recurso de encontrarse indisponible para la organización.

- ✓ **Plan de continuidad de Negocio** (PCN) o *Business Continuity Plan* (BCP por sus siglas en inglés) es un conjunto de directrices, criterios, normas de actuación y herramientas organizativas que, ante la ocurrencia de una contingencia que provocase la interrupción de alguna o todas las áreas de negocio de una organización, permiten la recuperación de la operatividad de las mismas en el menor tiempo posible, de modo que las pérdidas económicas ocasionadas sean mínimas.
- ✓ **Plan de recuperación ante desastres** (PRD) o *Disaster Recovery Plan* (DRP por sus siglas en inglés): constituye una parte del Plan de Continuidad de Negocio en aquellas compañías que dispongan de infraestructura tecnológica para soportar sus operaciones y, de forma análoga al Plan de Continuidad de Negocio, consta de todas las prácticas necesarias que, en caso de desastre, permiten recuperar en el menor tiempo posible el entorno tecnológico (sistemas, aplicaciones e infraestructuras) que soporta las actividades de una organización.
- ✓ **Usuario crítico:** persona designada para realizar la actividad crítica de forma regular.
- ✓ **Back up 1:** persona designada dentro del mismo lugar de trabajo que debe reemplazar al usuario critico en caso de contingencia.
- ✓ **Back up 2:** persona designada que se encuentra en otra sucursal (lugar de contingencia) y que debe realizar las labores del usuario crítico en caso de contingencia.

B. ¿Por qué es importante la Continuidad del Negocio?

La competitividad creciente entre las organizaciones empresariales, las demandas cada vez más exigentes de clientes y stakeholders, o los requerimientos regulatorios cada vez más restrictivos, son factores que hoy en día fuerzan a las empresas a demostrar la resistencia de las actividades de negocio a permanecer activas ante cualquier contingencia grave.

Una caída de la luz, una inundación, un incendio, etc., han de considerarse amenazas reales que deben ser tratadas de forma preventiva para evitar, en caso de que éstas sucedan, que las pérdidas sean tan graves que afecten a la viabilidad del negocio. Son múltiples las organizaciones que, independientemente de su tamaño, fracasan o incluso desaparecen por la falta de procesos, mecanismos y técnicas que mitiguen los riesgos a los que están expuestas y garanticen una alta disponibilidad en las operaciones de su negocio.

De este modo, es necesario que las organizaciones establezcan una serie de medidas técnicas, organizativas y procedimentales que garanticen la continuidad de las actividades o procesos de negocio en caso de tener que afrontar una contingencia grave.

C. Gestiones realizadas y en desarrollo:

- ✓ Identificación y registro de los procesos y actividades críticas a través del BIA, con el fin de identificar los recursos operativos, proveedores, aplicaciones tecnológicas y recursos tecnológicos que soportan esas actividades.
- ✓ Identificación y registro de usuarios críticos, back up 1, back up 2 y responsables de la activación del plan de contingencia, para cada actividad critica definida.
- ✓ Identificación y registro de los escenarios de contingencia operativa y de los escenarios de falla tecnológica.
- ✓ Levantamiento de información a través de reuniones con los usuarios críticos para la creación de fichas con los planes de continuidad operativa y fichas de procedimientos alternativos tecnológicos para cada actividad crítica.
- ✓ Programación y realización de capacitaciones para los planes de continuidad operativa y tecnológicas, en las cuales participan el usuario crítico como capacitador, los back up 1 y 2, como asistentes, además del Encargado de Riesgo Operacional y el Oficial de Seguridad de la Información (para los planes de continuidad tecnológica) como coordinadores de la capacitación.
- ✓ Programación y realización de pruebas de los planes de continuidad operativa y de los procedimientos alternativos tecnológicos, en las cuales participan, el responsable y coordinador de la activación el procedimiento de contingencia, el usuario crítico, los back up 1 y 2, además del Encargado de Riesgo Operacional y el Oficial de Seguridad de la Información (para los planes de continuidad tecnológica) como coordinadores de la prueba.

3. Estrategia de Comunicación:

Información a difundir[1]	Emisor	Receptor	Canal	Periodicidad	Procedimiento
A, B y C.	Depto. Gestión de la Calidad y Riesgo Operacional	Colaboradores del Banco	**Intranet**	Semestral	Subir la información a la página web del Banco, por medio de videos, imágenes o escritos.
B y C.	Depto. Gestión de la Calidad y Riesgo Operacional	Colaboradores del Banco	**Sesiones Informativas**	Anual	Entrega de información a través de una presentación con apoyo visual efectuada por la Jefa de Gestión de Calidad y Riesgo Operacional, el Encargado de Riesgo Operacional y el Oficial de Seguridad de la Información. Serán 7 sesiones distribuidas de acuerdo a la capacidad de la sala o auditórium.
A, B y C.	Depto. Gestión de la Calidad y Riesgo Operacional	Colaboradores del Banco	**Correo electrónico**	Semestral	Enviar correo electrónico a todos los colaboradores con la información.
B y C.	Depto. Gestión de la Calidad y Riesgo Operacional	Colaboradores del Banco	**Revista interna**	Semestral	Dentro de las noticias de “Contigo al día” (revista interna) incluir la información a difundir.
B y C.	Depto. Gestión de la Calidad y Riesgo Operacional	Colaboradores del Banco	**Diario mural o tablero informativo**	Semestral	Incluir dentro del diario mural la información a difundir.

[1] Las letras corresponden a la información definida en el punto 2.

Información a difundir	Emisor	Receptor	Canal	Periodicidad	Procedimiento
C.	Depto. Gestión de la Calidad y Riesgo Operacional	Colaboradores del Banco	**Buzón de sugerencias**	----------	Con el fin de lograr una retroalimentación, se puede habilitar una dirección de correo electrónico, donde se consiga dirigir las sugerencias, en cuanto a las gestiones realizadas que vayan surgiendo por parte de los colaboradores.
A y B.	Depto. Gestión de la Calidad y Riesgo Operacional	Participantes de los PCO	**Capacitaciones**	Anual	Entregar la información dentro de las capacitaciones de definición de roles y responsabilidades, a los participantes del PCO.
A, B y C.	Depto. Gestión de la Calidad y Riesgo Operacional	Colaboradores del Banco	**Intranet**	----------	Habilitar dentro de la Página web del Banco un segmento en donde los colaboradores deban realizar cursos e-learning, con respecto a la información a difundir
A, B y C.	Depto. Gestión de la Calidad y Riesgo Operacional	Nuevos Colaboradores que se integran a la Organización	**Inducciones**	----------	Por medio de las inducciones a los nuevos colaboradores que ingresen al Banco, se entregará la información.

4. Análisis de efectividad de la comunicación:

Actividad	Colaboradores presentes	Total de citados	Periodicidad	Indicador (presentes/cantidad total) x100%
Sesiones informativas			Anual	

Concepto	Colaboradores que conocen el plan de continuidad de negocios	Total de colaboradores	Periodicidad	Indicador (Colaboradores que conocen el plan/total) x100%
Plan de Continuidad de Negocios			Anual	

Actividad	Colaboradores presentes	Total de citados	Periodicidad	Indicador (presentes/cantidad total) x100%
Capacitaciones			Anual	

Actividad	Realizaron el curso e-learning	Total de colaboradores	Periodicidad	Indicador (realizaron el curso e-learning /total) x100%
Intranet			Anual	

Concepto	Colaboradores nuevos en la Organización que recibieron inducción	Total de colaboradores nuevos en la Organización	Periodicidad	Indicador (Colaboradores que conocen el plan/total) x100%
Inducciones			Anual	