TESIS PUCP

# PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

## FACULTAD DE CIENCIAS E INGENIERÍA

# Análisis y diseño de un Sistema de Gestión de Continuidad de Negocio en caso de ocurrencia de sismos para una empresa aseguradora local basado en la ISO/IEC 22301:2012

Tesis para optar el Título de **Ingeniero Informático**, que presenta el bachiller:

**Stephany Candy Canchari Pastor**

**ASESOR: Moisés Antonio Villena Aguilar**

Lima, abril de 2014

Tesis publicada con autorización del autor
No olvide citar esta tesis

## Tabla de contenido

RESUMEN 9

CAPÍTULO 1 10

1 INTRODUCCIÓN 10

2 PROBLEMÁTICA 10

3 MARCO TEÓRICO 12

3.1 MARCO CONCEPTUAL 12
3.1.1 CONCEPTOS RELACIONADOS AL PROBLEMA 12
3.1.2 CONCEPTOS RELACIONADOS A LA PROPUESTA DE SOLUCIÓN 16
3.1.3 OTROS CONCEPTOS 23
3.2 MARCO REGULATORIO / LEGAL 24
3.2.1 SUPERINTENDENCIA DE BANCA, SEGUROS Y AFP (SBS) 24
3.2.2 LEY GENERAL DEL SISTEMA FINANCIERO – LEY N° 26702 24
3.2.3 CIRCULAR N° G - 139 – 2009 24
3.2.4 RESOLUCIÓN SBS N° 2115 24
3.2.5 RESOLUCIÓN SBS N° 2116 25
3.3 NORMAS APLICABLES A LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO NACIONALES E INTERNACIONALES 25
3.3.1 NFPA 1600 – STANDARD ON DISASTER/EMERGENCY MANAGEMENT AND BUSINESS CONTINUITY PROGRAMS 25
3.3.2 HB 221:2004 BUSINESS CONTINUITY MANAGEMENT (BCM) 26
3.3.3 BASILEA II EN EL PERÚ 26

4 ESTADO DEL ARTE 26

4.1 FORMAS EXACTAS DE RESOLVER EL PROBLEMA 27
4.1.1 BANCO INTERNACIONAL ESPAÑOL - BANKINTER 27
4.2 FORMAS APROXIMADAS DE RESOLVER EL PROBLEMA 27
4.3 PRODUCTOS COMERCIALES PARA RESOLVER EL PROBLEMA 27
4.4 CONCLUSIONES SOBRE EL ESTADO DEL ARTE 28

Tesis publicada con autorización del autor
No olvide citar esta tesis

CAPÍTULO 2 29

1 OBJETIVO GENERAL 29

2 OBJETIVOS ESPECÍFICOS 29

3 RESULTADOS ESPERADOS 29

4 HERRAMIENTAS, MÉTODOS Y PROCEDIMIENTOS 30

4.1 MAPEO 30
4.2 HERRAMIENTAS Y METODOLOGÍAS 30
4.2.1 ISO/IEC 22301:2012 31
4.2.2 ISO 31000: 2009 32
4.2.3 NFPA 1600 33
4.2.4 BUSINESS PROCESS MANAGEMENT AND NOTATION BPMN 2.0 34

5 ALCANCE 35

5.1 LIMITACIONES 35
5.2 RIESGOS 37

6 JUSTIFICACIÓN Y VIABILIDAD 37

6.1 JUSTIFICATIVA DEL PROYECTO DE TESIS 37
6.2 ANÁLISIS DE VIABILIDAD DEL PROYECTO DE TESIS 38

7 PLAN DE ACTIVIDADES 38

CAPÍTULOS 3 – LA EMPRESA 39

1 INTRODUCCIÓN 39

2 METODOLOGÍA PARA LA IDENTIFICACIÓN DE PROCESOS CRÍTICOS DE CONTINUIDAD 39

2.1 OBJETIVO 39

**2.2 ELABORACIÓN DE LA ENCUESTA 39**
2.2.1 INFORMACIÓN DE APOYO 39
2.2.2 LA ENCUESTA 39
2.2.3 DESCRIPCIÓN DE RESULTADOS 42
**2.3 CONCLUSIONES DE LA METODOLOGÍA 42**

**3 RELACIÓN DE PROCESOS CRÍTICOS PARA LA CONTINUIDAD DEL NEGOCIO 42**

**3.1 OBJETIVO 42**
**3.2 APLICACIÓN Y RESULTADO 43**

**4 MODELADO DE PROCESOS CRÍTICOS 43**

**4.1 OBJETIVO 43**
**4.2 ALCANCE: 43**

**CAPÍTULOS 4 – ANÁLISIS DE RIESGOS E IMPACTO EN EL NEGOCIO 44**

**1 INTRODUCCIÓN 44**

**2 ANÁLISIS DE IMPACTO DE NEGOCIO 44**

**2.1 OBJETIVO 44**
**2.2 TIEMPOS DEL NEGOCIO 44**
**2.3 ALCANCE 45**
**2.4 INDICADORES DE CONTINUIDAD 45**
**2.5 RECURSOS ASOCIADOS A LA RECUPERACIÓN 45**

**3 ESTRATEGIAS DE CONTINUIDAD 46**

**3.1 OBJETIVO 46**
**3.2 RECURSOS 47**
**3.3 ESTRATEGIAS PROPUESTAS POR TIPO DE RECURSO 47**

**4 ANÁLISIS DE RIESGOS 47**

Tesis publicada con autorización del autor
No olvide citar esta tesis

CAPÍTULOS 5 – PLAN DE MANEJO DE CRISIS 49

1 INTRODUCCIÓN 49

2 OBJETIVO 49

3 ALCANCE 49

4 DEFINICIONES 49

5 ESTRUCTURA PARA EL MANEJO DE CRISIS 50

5.1 DESCRIPCIÓN 51
5.1.1 EQUIPO DE GESTIÓN DE CRISIS (EGP) 51
5.1.2 GESTIÓN DE EMERGENCIAS, INCIDENTES DE TI Y EVENTOS 51

6 ESTRUCTURA DE ACCIÓN 53

6.1 NOTIFICACIÓN 53
6.2 ANÁLISIS Y EVALUACIÓN 53
6.3 RESPUESTA 54
6.3.1 REALIZAR SEGUIMIENTO CONJUNTO 54
6.3.2 EQUIPO DE MANEJO DE CRISIS 54

7 MANTENIMIENTO DEL PLAN 57

CAPÍTULOS 6 – PLAN DE RESPUESTA A EMERGENCIAS 59

1 INTRODUCCIÓN 59

2 OBJETIVO 59

3 ESTRATEGIAS DE RESPUESTA A EMERGENCIAS 59

3.1 ETAPA I: ANTES 59
3.2 ETAPA II: DURANTE 60
3.3 ETAPA III: DESPUÉS 60

Tesis publicada con autorización del autor
No olvide citar esta tesis

4 EQUIPO DE RESPUESTA A EMERGENCIAS 61

5 FUNCIONES Y RESPONSABILIDADES 62

6 ANTES: ACTIVIDADES DE PREVENCIÓN Y PREPARACIÓN 62

7 DURANTE: ACTIVIDADES DE RESPUESTA Y ACTIVACIÓN 63

7.1 ESCENARIO 1: SISMO O TERREMOTO 63

8 COMUNICACIÓN EN CASO DE EMERGENCIAS 64

8.1 COMUNICACIÓN INICIAL DE LA EMERGENCIA 64
8.2 COMUNICACIÓN A CLÍNICAS Y HOSPITALES (EMERGENCIA MÉDICA) 65
8.3 COMUNICACIÓN A ENTIDADES DE APOYO EXTERNO 65

9 PROCEDIMIENTOS GENERALES DE EVACUACIÓN 65

10 DIRECTORIO DE SERVICIOS DE EMERGENCIA 67

11 REQUISITOS EN EL SITIO ALTERNO DE OPERACIÓN 67

CAPÍTULOS 7 – PLAN DE RECUPERACIÓN ANTE DESASTRES 68

1 INTRODUCCIÓN 68

2 OBJETIVO 68

3 ALCANCE 68

4 ESTRATEGIAS 69

5 EQUIPOS Y ROLES DE RECUPERACIÓN 70

5.1 EQUIPO DE RECUPERACIÓN PRINCIPAL DE TI 70
5.2 HABILIDADES POR ROL 71

6 FASES DE RECUPERACIÓN 71

Tesis publicada con autorización del autor
No olvide citar esta tesis

6.1 FASE I: ANTES 71
6.2 FASE II: RESPUESTA Y DE OPERACIÓN ALTERNA 71
6.3 FASE III: ACTIVIDADES DE RESTAURACIÓN Y RETORNO 76

CAPÍTULOS 8 – PLAN DE CONTINUIDAD DE NEGOCIO 79

1 INTRODUCCIÓN 79

2 OBJETIVO 79

3 ALCANCE 79

4 OBJETIVOS ESPECÍFICOS 79

5 EQUIPOS DE RECUPERACIÓN 79

6 INSTRUCCIONES PARA EL USO DEL PLAN 80

6.1 INVOCAR EL PLAN 80
6.2 DECLARAR EL DESASTRE 80
6.3 NOTIFICAR 80
6.4 COMUNICAR A MEDIOS DE COMUNICACIÓN 80
6.5 USO DE PLANES 81
6.5.1 FASE I: PREVENCIÓN 81
6.5.2 FASE II: OCURRENCIA DE SISMO 82
6.5.3 FASE III: EVALUACIÓN INICIAL 83
6.5.4 FASE IV: ACTIVACIÓN DE PLANES DE CONTINGENCIA 84
6.6 MONITOREO 85

CAPÍTULOS 9 – PLAN DE PRUEBAS 87

1 INTRODUCCIÓN 87

2 OBJETIVO 87

3 CONSIDERACIONES 87

Tesis publicada con autorización del autor
No olvide citar esta tesis

4 PRUEBAS Y ACTUALIZACIÓN 88

4.1 EJECUCIÓN DE PRUEBAS 88
4.1.1 TABLETOP 88
4.1.2 PRUEBAS DE ESCRITORIO OPERATIVAS 88
4.2 ACTUALIZACIÓN DE LOS PLANES 88

CAPÍTULOS 10 – CONCLUSIONES, OBERVACIONES, RECOMENDACIONES Y TRABAJOS FUTUROS 89

1 CONCLUSIONES 89

2 OBSERVACIONES 90

3 RECOMENDACIONES 91

4 TRABAJOS FUTUROS 92

REFERENCIAS BIBLIOGRÁFICAS 94

Tesis publicada con autorización del autor
No olvide citar esta tesis

## RESUMEN

En la actualidad, las empresas se enfrentan a un entorno cada vez más variable y retador, donde factores como procesos, personas, tecnología y eventos externos hacen que las operaciones y servicios se vean expuestos a interrupciones que pueden afectar la continuidad de las mismas. Dentro de los eventos externos, al estar ubicados geográficamente dentro del llamado “cinturón de fuego del Pacifico”, eventos como los sismos se han convertido en serias amenazas para la continuidad de las operaciones de las empresas.

Frente a esto, entidades reguladoras como la Superintendencia de Banca Seguros y AFP, se han preocupado por dar lineamientos que permitan a las empresas reguladas adaptarse a estándares y normas internacionales relacionadas a la continuidad de negocios que les brinden las herramientas necesarias para hacer frente a esta situación.

La presente tesis ha realizado una investigación de la ISO/IEC 22301:2012, norma exigida por el ente regulador mencionado anteriormente, permitiendo realizar un análisis y diseño que se adapta a la naturaleza y las necesidades de una empresa aseguradora específica de modo que pueda ser utilizada por dicha institución facilitando que ésta cumpla con la norma de regulación vigentes relacionada a la Continuidad de Negocios.


Tesis publicada con autorización del autor
No olvide citar esta tesis

# CAPÍTULO 1

## 1 Introducción

En los últimos años, la continuidad de negocios se ha convertido en una de las principales preocupaciones de toda organización, especialmente para aquellas reguladas por la Superintendencia de Banca, Seguros y AFP (SBS), que consiente de la importancia de una adecuada Gestión de Continuidad de Negocios, a través de la circular N° G-139-2009, ha decidido incluirla como parte de la Gestión de Riesgo Operacional definiendo los requisitos que se deben cumplir, es decir, se indica el "qué hacer" mas no el "cómo lograrlo", dejando a las empresas en problemas y en búsqueda de una solución.

Por otro lado, geográficamente el Perú se encuentra propenso a la ocurrencia de diversos desastres naturales. Para el caso de las empresas de seguros esta preocupación es doble, ya que frente al acaecimiento de un desastre natural tendrán que proteger sus principales activos de información para garantizar la continuidad de sus operaciones y además cubrir todos los gastos que incluyan los servicios que ofrecen a sus asegurados.

Las empresas de seguros requieren establecer por tanto, un Sistema de Gestión de Continuidad de Negocios (SGCN), sin embargo, a causa del gran número de escenarios de desastres que existen, el presente proyecto de fin de carrera plantea el análisis y diseño de un SGCN para una empresa aseguradora local en caso de ocurrencia de un sismo.

Para esto, se contará con el apoyo de especialistas en el negocio, quienes brindarán al tesista información de los principales procesos sin comprometer información confidencial de la empresa donde trabajan. Además se establecerá un cronograma para el control y seguimiento de cada una de las actividades que involucre el proyecto.

## 2 Problemática

El Perú está comprendido entre una de las regiones de más alta actividad sísmica y de probabilidad de desastres naturales por encontrarse dentro del Cinturón de Fuego del Pacífico y por diversas características geográficas que hacen que esté expuesto permanentemente a este peligro. Basado en los estudios del Instituto Nacional de Defensa Civil (INDECI), quienes a lo largo de estos años han publicado una serie de

Tesis publicada con autorización del autor
No olvide citar esta tesis

reportes sobre los daños y la cantidad de desastres naturales ocurridos en el país. A continuación, se muestran los siguientes cuadros resúmenes que permitirán evaluar las incidencias en el periodo 2006 -2011 (Ver Anexo 1).

Además, al evaluar las ocurrencias de dichos desastres naturales se tiene:

| NÚMERO DE DESASTRES NATURALES POR AÑO | | | | | | |
|---|---|---|---|---|---|---|
| | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 |
| Aluvión | 4 | 2 | 5 | 5 | 10 | 5 |
| Desplazamiento | 158 | 126 | 128 | 116 | 92 | 141 |
| Huayco | 73 | 53 | 50 | 64 | 60 | 43 |
| Inundación | 348 | 272 | 242 | 219 | 216 | 256 |
| Maretazo | 12 | 1 | 1 | 0 | 7 | 20 |
| Sismo | 32 | 200 | 24 | 8 | 17 | 41 |
| **Total** | **627** | **654** | **450** | **412** | **402** | **506** |

Figura 1. Resumen de ocurrencias de desastres naturales por año. (INDECI 2012)

De esta información, se observa que los desastres naturales están siempre presentes en el Perú y dentro de ellos resalta el sismo como evento con gran cantidad de incidencias anuales, pérdidas humanas, materiales y por ende de dinero. Bajo este contexto, empresas como las de Seguros tienen la misión de ayudar a sus clientes a proteger su estabilidad económica ofreciéndoles soluciones y servicios disponibles de manera oportuna que protejan aquello que valoran teniendo la suficiente capacidad de respuesta en caso de desastres naturales.

La Superintendencia de Banca y Seguros (SBS), como ente regulador, en su circular N° G-139-2009 indicó que como parte de una adecuada Gestión del Riesgo Operacional considera conveniente tomar como referencia estándares internacionales como la BS-25999 (SBS 2009), demostrando una vez más la gran importancia e impacto que se le ha ido dando al riesgo operacional dentro de empresas como las aseguradoras (Ver figura 2).

Además, en la Resolución SBS N° 2116 (SBS 2009) se establece un cambio importante, indicándose como nuevo criterio para una adecuada Gestión de la Continuidad del Negocio establecer clases de riesgos y líneas de negocio (ver Anexo 2). Frente a todos estos cambios empresas como las del rubro de seguros, como entes regulados, están en la necesidad y obligación de cubrir los nuevos requerimientos de la SBS en cuanto a la Continuidad de Negocios dentro de la Gestión de riesgo operacional, viéndose frente a una gran dificultad pues se ha indicado qué se debe hacer pero no el cómo conducir este cambio para alinearse a los nuevos

Tesis publicada con autorización del autor
No olvide citar esta tesis

criterios poniendo en riesgo su continuidad y el resultado de las evaluaciones que realiza la SBS para las memorias anuales.

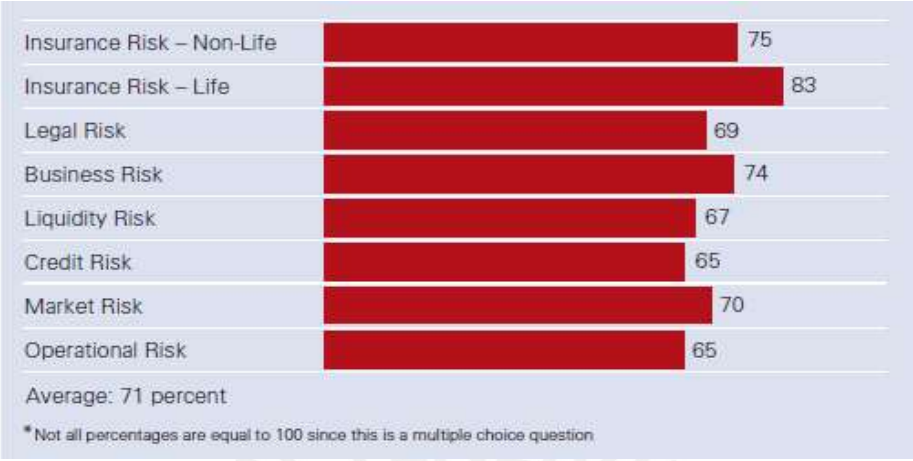


Figura 2. Avance del desarrollo de frameworks para la gestión de riesgos de acuerdo a su tipo (KPMG 2006: 8)

Frente a esta problemática, se plantea un diseño de Sistema de Gestión de Continuidad del Negocio (SGCN) para escenarios de sismo, que permita cumplir con parte de lo exigido por la SBS para autorizar el uso del Método Estándar Alternativo para el cálculo del requerimiento patrimonial, ya que éste permite una mejor adaptación al concepto de gestión del riesgo operacional dividiendo las actividades por líneas de negocio y determinando el cálculo del requerimiento patrimonial en función a ello (SBS 2009). Para dicho propósito se plantea usar como base la norma ISO/IEC 22301:2012 “Seguridad de la sociedad – Sistemas de gestión de la continuidad del negocio”, publicada en mayo del 2012, aceptada en julio del mismo año y actualmente considerada la mejor opción para remplazar a la norma BS 25999.

# 3 Marco teórico

A continuación, se presentan algunos temas importantes relacionados a tema de gestión de la continuidad del negocio y el marco legal asociado:

## 3.1 Marco conceptual

Para un mejor entendimiento, se agruparán en los siguientes aspectos:

### 3.1.1 Conceptos relacionados al problema

A continuación, se presentarán algunos conceptos relacionados a la problemática actual que facilitarán el entendimiento del mismo.

#### 3.1.1.1 Gestión Integral de Riesgos

En el artículo 3° de la Resolución SBS N° 37 – 2008, se define que "la Gestión Integral de Riesgos es un proceso, efectuado por el Directorio, la Gerencia y el personal aplicado en toda la empresa y en la definición de su estrategia, diseñado para identificar potenciales eventos que pueden afectarla, gestionarlos de acuerdo a su apetito por el riesgo y proveer una seguridad razonable en el logro de sus objetivos". (SBS 2008)

Dentro de sus objetivos, considera las siguientes categorías:

- *Estrategia,* objetivos de alto nivel vinculado a la visión y misión empresarial.
- *Operaciones,* vinculado al uso eficaz y eficiente de los recursos asignados a las diferentes operaciones.
- *Información,* vinculado a la confiabilidad de la información suministrada.
- *Cumplimiento,* vinculado al cumplimiento de las leyes y regulaciones aplicables.

Cabe mencionar que actualmente, se define a la Gestión de Continuidad del Negocio como parte de una adecuada Gestión de Riesgo operacional (SBS 2009) dando disposiciones más claras en cuanto al manejo y a este nuevo enfoque.

#### 3.1.1.2 Gestión de Riesgo Operacional

Para la SBS, la Gestión de Riesgo Operacional es la "posibilidad de ocurrencia de pérdidas debido a procesos inadecuados, fallas del personal, de la tecnología de información, o eventos externos." (SBS 2009).

Dentro de los factores que pueden originar el riego operacional se encuentran:

- **Procesos internos**

  Se refiere a los procesos internos de una organización implementados para la realización de sus operaciones y servicios, relacionados al diseño inapropiado de los procesos o a políticas y procedimientos inadecuados o inexistentes que, como consecuencia, puedan llevar a un desarrollo deficiente de las operaciones y servicios o la suspensión de los mismos. " (SBS 2009)

- **Personal**

  Se refiere a la adecuada gestión que deben tener las empresas sobre los riesgos asociados a su personal, pueden estar relacionados a la inadecuada capacitación,

Tesis publicada con autorización del autor
No olvide citar esta tesis

negligencia, error humano, sabotaje, fraude, robo, paralizaciones, apropiación de información sensible, entre otros. (SBS 2009)

- **Tecnología de información**

Se refiere a la adecuada gestión que deben tener las empresas sobre los riesgos relacionados a la tecnología de información, a fallas en la seguridad y continuidad operativa de los sistemas informáticos, errores en el desarrollo e implementación de dichos sistemas y la compatibilidad e integración de los mismos, la inadecuada inversión en tecnología, entre otros aspectos. (SBS 2009)

- **Eventos externos**

Se refiere a la adecuada gestión de los riesgos asociados a eventos externos ajenos al control de la empresa. Ejemplo: Fallas en los servicios públicos, la ocurrencia de desastres naturales, atentados y actos delictivos, entre otros.

#### 3.1.1.3 Reconocimiento y medida del riesgo en empresas aseguradoras

Según una publicación de gestión de riesgo y capital para empresas aseguradoras realizada por KPMG en el 2005, “el riesgo operacional es la causa de los fallos de muchos seguros, con las personas que practican directrices externas, empresas que no reaseguran adecuadamente o sistemas fallando, por lo que es tranquilizador saber que casi dos tercios de los participantes están tratando de medir y comprender la materia. Sin embargo, el hecho mismo de que el riesgo operacional cubre una amplia gama de cuestiones hace que sea difícil de cuantificar” (KPMG LLP. 2006: 6). Esto deja ver la importancia, el gran impacto y la complejidad que implica una adecuada gestión de riesgo operacional.

En cuanto a los principales riesgos del rubro se menciona: “Entre los diferentes grupos de aseguradores, los reaseguradores tienen más probabilidades de tener un marco de gestión de riesgo para el riesgo de crédito, reflejo de la exposición que tienen a su riesgo de impago de la póliza. Vida y banca aseguradora por otra parte parecen estar más preocupados por el riesgo de liquidez, lo que refleja la necesidad de una gestión detallada de activos y pasivos (ALM) en este sector” (KPMG LLP. 2006: 6).

#### 3.1.1.4 Gestión de la Continuidad de Negocio (GCN)

En la Circular N° G-139-2009 se define que “la gestión de la continuidad del negocio es un proceso, efectuado por el Directorio, la Gerencia y el personal, que implementa respuestas efectivas para que la operatividad del negocio de la empresa continúe de

una manera razonable, con el fin de salvaguardar los intereses de sus principales grupos de interés, ante la ocurrencia de eventos que pueden crear una interrupción o inestabilidad en las operaciones de la empresa" (SBS 2009).

De manera general, la GCN es un conjunto de procesos holísticos que permiten la identificación de las potenciales amenazas así como el impacto en las organizaciones. Si se ve a la GCN dentro de diferentes contextos, se tiene (THE BUSINESS CONTINUITY INSTITUTE 2010):

- **GCN y la Resiliencia del Negocio**

  La aplicación de una adecuada GCN incrementa su resiliencia y mejora su desempeño corporativo proporcionando un marco de referencia para entender el ciclo de valor dentro de la organización estableciendo una relación directa con las vulnerabilidades inherentes a la entrega de este valor.

- **GCN y la Gestión de Riesgos**

  Usualmente está posicionada debajo de la Gestión de Riesgos, siendo ésta última una disciplina estratégica firmemente integrada en muchas organizaciones grandes. Por otro lado, en cuanto a desarrollo, mientras que la GCN ha evolucionado a partir del mundo de la Tecnología y de la "recuperación ante desastres", la Gestión de Riesgos Empresariales (GRE), ha evolucionado a partir del mundo de los seguros.

- **La GCN y La Gestión de Crisis**

  Ambas se encuentran fuertemente ligadas por el componente Gestión del Incidente. Dentro de la GCN, los incidentes son los que invocarán al plan de GCN, sin embargo muy pocos son designados como "crisis". La Gestión de Crisis es vista también como la respuesta a eventos tanto físicos como no físicos y a diversos tipos de incidentes como financieros y de daños a la reputación de la organización.

#### 3.1.1.5 Líneas de negocio en empresas de seguros

La Superintendencia de Banca Seguros y AFP, en la Resolución SBS N° 2116, establece como criterio definir la exposición al riesgo operacional por línea de negocio (SBS 2009), haciendo que la Gestión de Continuidad sea enfocada desde el mismo punto de vista (Ver Anexo 2).

Tesis publicada con autorización del autor
No olvide citar esta tesis

### 3.1.2 Conceptos relacionados a la propuesta de solución

#### 3.1.2.1 International Organization for Standardization (ISO)

Organización encargada de desarrollar estándares internacionales. Fundada en 1947 y desde entonces ha publicado más de 19000 estándares (ISO 2012) cubriendo casi todos los aspectos de tecnología y negocios. Los beneficios que brinda esta entidad abarcan aspectos como (ISO 2012):

**a. Los negocios:**

- Ahorro de costos, las Normas internacionales ayudan a optimizar las operaciones y por lo tanto mejorar la línea de fondo.
- Mayor satisfacción del cliente, las Normas Internacionales ayudan a mejorar la calidad, aumentar la satisfacción del cliente y aumentar las ventas.
- Acceso a nuevos mercados, las Normas Internacionales ayudan a prevenir las barreras del comercio y abrir los mercados mundiales.
- Aumento de cuota de mercado, las normas internacionales ayudan a aumentar la productividad y ventaja competitiva.
- Beneficios ambientales, las Normas internacionales ayudan a reducir los impactos negativos sobre el medio ambiente.

**b. La sociedad:**

Cuando los productos y servicios están de acuerdo a las Normas Internacionales, los consumidores pueden tener la confianza de que son seguros, fiables y de buena calidad.

Para asegurarse de que los beneficios de las Normas Internacionales ISO sean posibles, ISO apoya la participación de los consumidores en la labor de elaboración de normas de la Comisión de Política de Consumo (COPOLCO).

Las normas internacionales de calidad del aire, el agua y el suelo, sobre las emisiones de gases y la radiación y los aspectos ambientales de los productos contribuyen a los esfuerzos para preservar el medio ambiente y la salud de los ciudadanos.

**c. El gobierno:**

- Opinión de expertos, las normas ISO son desarrolladas por expertos. Mediante la integración de una norma ISO en la regulación nacional, los gobiernos

Tesis publicada con autorización del autor
No olvide citar esta tesis

pueden beneficiarse de la opinión de expertos sin tener que recurrir a sus servicios directamente.

- La apertura del comercio mundial, las normas ISO son internacionales y adoptadas por muchos gobiernos. Mediante la integración de las normas ISO en la regulación nacional, los gobiernos ayudan a asegurar que los requisitos para la importación y exportación son los mismos en todo el mundo facilitando la circulación de bienes, servicios y tecnologías de país a país.

#### 3.1.2.2 ISO/IEC 22301: 2012

Norma internacional que especifica los requerimientos para establecer, implementar, operar, monitorear y mejorar continuamente un sistema de gestión documentado para proteger, reducir la probabilidad de ocurrencia, prepararse, proteger y recuperarse de incidentes perjudiciales cuando ocurren.

Los requisitos especificados en la norma son genéricos y aplicables a todas las organizaciones o parte de las mismas sin importar el tamaño ni su naturaleza. Además, las necesidades de cada organización deben estar formadas por un marco regulatorio, requerimientos organizacionales, productos y servicios, los procesos empleados, el tamaño, la estructura de la organización y los requerimientos de las partes interesadas.

En general, la ISO 22301 es aplicable a todas las organizaciones que deseen:

- Establecer, implementar, mantener y mejorar un plan de gestión de continuidad de negocio.
- Asegurar la conformidad con las políticas establecidas de gestión de la continuidad del negocio.
- Alcanzar una certificación o registro de su Plan de Gestión de Continuidad de Negocio por un tercero.
- Determinar y declarar su conformidad con este estándar internacional.

Este estándar brinda el llamado modelo “Plan – Do – Check - Act” (PDCA) para planificar, establecer, implementar, monitorear, revisar y mantener continuamente mejorando la efectividad del Plan de Gestión de Continuidad del Negocio (SGCN). La figura 3 ilustra cómo una SGCN toma las entradas y a través de acciones y procesos logra la los resultados esperados (ISO 2012).

Tesis publicada con autorización del autor
No olvide citar esta tesis

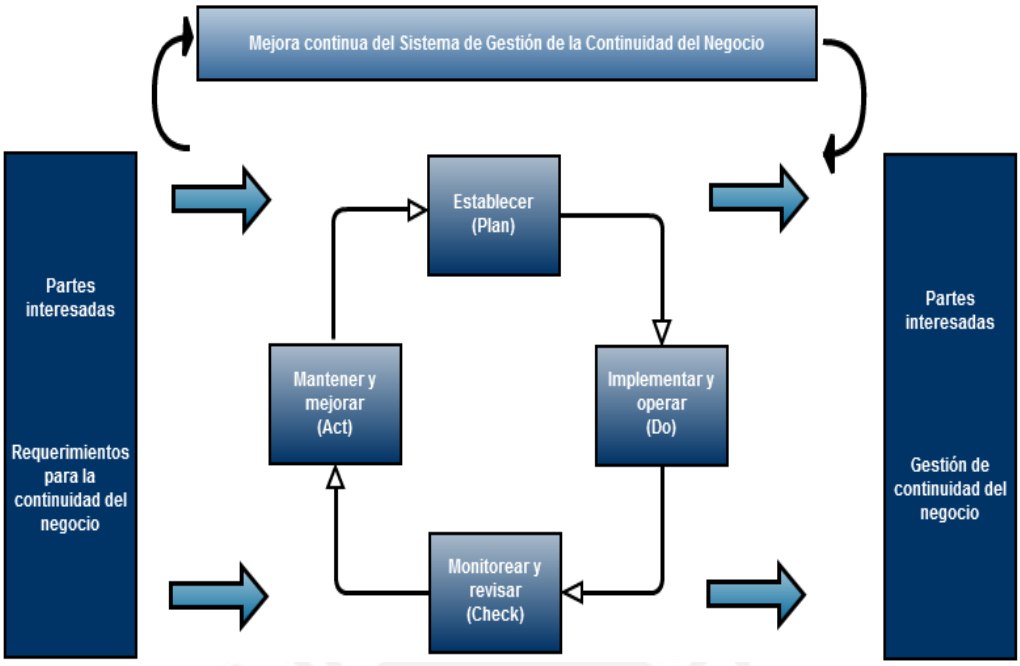


Figura 3. Plan – Action – Do – Check de ISO/IEC 22301: 2012 (ISO 2012: 6)

#### *3.1.2.3 Norma BS 25999*

Norma creada por el British Standards Institution, es uno de los 3 estándares para el uso en Sector Privado Voluntario de Acreditación y Preparación de Certificación. Esta norma está dividida en 2 partes (BSI 2009):

- **BS 25999:2006 – 1**

  Es un enfoque holístico de gestión de procesos que identifica los posibles impactos que amenazan a una organización en su entorno, ofreciendo un marco para incrementar la resiliencia y la capacidad de respuesta que protege los intereses de los grupos interesados clave, la reputación y el valor de la creación de las actividades. A continuación, se presenta el ciclo de vida de la Gestión de Continuidad bajo este enfoque (Ver figura 4):

  - *Entender la organización,* a través de la identificación de servicios y productos clave, actividades críticas y los recursos que las sostienen.
  - *Determinar la estrategia de Continuidad de Negocio,* determinar una estrategia con el objetivo de alcanzar los objetivos de la organización dependiendo del tiempo máximo de interrupción de actividades, costos de implementación y costos por no tomar acciones.
  - *Desarrollo e implementación de una respuesta,* obteniendo los planes y medidas adecuadas para garantizar la continuidad de actividades críticas y la gestión de incidentes.

- *Ejercicio, mantenimiento y revisión,* asegura que los acuerdos de BCM de una organización son validados y revisados con el ejercicio.

Figura 4. Ciclo de vida de la Continuidad del Negocio (BSI 2009: 16)

- **BS 25999 – 2**

Establece los requerimientos para operar, monitorear, revisar y mejorar un SGCN (BSCMS por sus siglas en inglés, Business Continuity Management System) dentro del contexto de los riesgos generales de una organización. A continuación se presenta las etapas y su relación con el PDCA (Ver figura 5):

- *Establecer y gestionar el BCMS (Plan),* definiendo el alcance asegurando que los objetivos de la organización sean claramente establecidos, que hayan los recursos necesarios y que los responsables del BCM sean competentes.
- *Implementar el BCMS (Do),* identificando las actividades críticas y los recursos necesarios para soportarla; determinar los arreglos que permitan la recuperación de dichas actividades dentro del tiempo definido y facilitar el desarrollo e implementación de planes BCM.
- *Monitorear y revisar el BCMS (Check),* asegurando la efectividad y eficiencia del BCMS, revisar la correctitud de las políticas de continuidad, alcance y determinar acciones para la reparación y mejora.
- *Mantener y mejorar el BCMS (Act),* sosteniendo y mejorando su efectividad tomando medidas preventivas y correctivas.

Tesis publicada con autorización del autor
No olvide citar esta tesis

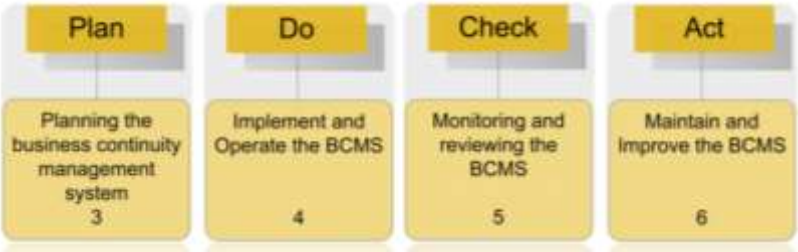


Figura 5. Distribución del PDCA en el BCMS (BSI 2009: 35)

#### *3.1.2.4 Comparativa BS 25999 – ISO/IEC 22301:2012*

A continuación, se presenta el siguiente cuadro que brinda un mapeo de ambos estándares indicando los principales cambios encontrados en las cláusulas:

No changes or negligible changes | Moderate changes | Major changes

| Most important areas | Clauses in ISO 22301 | Clauses in BS 25999-2 | Change |
|---|---|---|---|
| Understanding the organization | 4.1 | - | ■■■ |
| Understanding the needs and expectations of interested parties | 4.2 | - | ■■■ |
| Determining the scope | 4.3 | 3.2.1 | ■■ |
| Management commitment | 5.2 | - | ■■■ |
| Business continuity policy | 5.3 | 3.2.2 | ■■ |
| Business continuity objectives | 6.2 | 3.2.1.1 | ■■ |
| Competences | 7.2 | 3.2.4 | ■ |
| Awareness | 7.3 | 3.3 | ■ |
| Communication & warning system | 7.4, 8.4.2, 8.4.3 | 4.3.3.3 | ■■■ |
| Documented information | 7.5 | 3.4 | ■■ |
| Business impact analysis | 8.2.1, 8.2.2 | 4.1.1 | ■ |
| Risk assessment | 8.2.1, 8.2.3 | 4.1.2 | ■■ |
| Business continuity strategy | 8.3.1 | 4.2 | ■ |
| Resource requirements | 8.3.2 | 4.3.2.2, 4.3.3.3 | ■■ |
| Risk treatment (protection and mitigation) | 8.3.3 | 4.1.3 | ■ |
| Incident response structure | 8.4.2 | 4.3.2 | ■ |
| Business continuity plans / recovery plans | 8.4.4, 8.4.5 | 4.3.3 | ■ |
| Exercising and testing | 8.5 | 4.4.2 | ■ |
| Monitoring, measurement, analysis and evaluation | 9.1 | 4.4.3 | ■■■ |
| Internal audit | 9.2 | 5.1 | ■ |
| Management review | 9.3 | 5.2 | ■ |
| Nonconformity and corrective action | 10.1 | 6.1.3 | ■■ |
| Preventive action | 6.1, 9.1.1 | 6.1.2 | ■■ |

Figura 6. Comparativa entre las cláusulas de la ISO/IEC 22301: 2012 y BS 25999-2 (INFORMATION SECURITY & BUSINESS CONTINUITY ACADEMY 2012)

Además, se presenta el siguiente cuadro resumen de las características de cada una de estas normas:

| Criterio | Descripción |
|---|---|
| **Semejanzas** | Incluyen:<br>• Política de continuidad de negocio.<br>• Análisis de impacto.<br>• Valoración del riesgo.<br>• Estrategia de continuidad de negocio (llamada "Opciones de continuidad de negocio" en la ISO 22301).<br>• Planes de continuidad de negocio.<br>• Pruebas. |
| **Diferencias** | • Modelo menos claro del PDCA comparado al de la BS 25999, sin embargo aún están organizados de un modo lógico.<br>• La ISO 22301 da un mayor énfasis al establecimiento de objetivos, control de desempeño y métricas dándole un perfil más cercano al de la Alta Gerencia. |

Figura 7. Comparativa de entre la norma BS 25999 e ISO/IEC 22301:2012

En conclusión, no hay cambios significativos entre ambas normas y se considera que los elementos de la BS 25999 están contenidos en la ISO/IEC 22301:2012, dándole además un enfoque más orientado a la gestión del negocio y al ser una norma internacional, brindará un lenguaje de trabajo común con los clientes logrando una mayor ventaja competitiva.

#### 3.1.2.5 ISO/DIS 22313 - Seguridad Social – Sistemas de Gestión de Continuidad de Negocio

Publicada a inicios del 2013, es una guía, describe los pasos que las empresas deben seguir a fin de cumplir con los requisitos de la ISO 22301. En conjunto, ambas normas, ISO 22301 e ISO 22313, buscan apoyar a las organizaciones en su continuo reto para mejorar su resiliencia empresarial frente a circunstancias imprevistas (BSI Group 2013).

#### 3.1.2.6 ISO 31000: 2009

Es un estándar internacional de Gestión de Riesgos que brinda una serie de herramientas y directrices de modo que pueda ser aplicada a toda la organización, sus diferentes áreas y niveles en cualquier momento (ISO 2009).

La norma sugiere que para una adecuada Gestión de Riesgos, una organización debe cumplir con los siguientes principios:

- **La Gestión de Riesgos crea y protege el valor.**

  Contribuyendo al alcance de los objetivos y la mejora del desempeño en, por ejemplo, las operaciones, el gobierno y reputación. (ISO 2009)

- **La Gestión de Riesgos es una parte integral de los procesos de la organización**

  Haciendo que la gestión de riesgos no sea una actividad independiente de los demás procesos de la organización, sino, siendo parte de las actividades de gestión y una parte integral de todos los procesos de negocio. (ISO 2009)

- **La Gestión de Riesgos es parte de la toma de decisiones**

  Ayudando a los responsables a tomar de decisiones informadas priorizando acciones y distinguiendo todas las alternativas. (ISO 2009)

- **La Gestión de Riesgos aborda explícitamente la incertidumbre**

  Tomando en cuenta la incertidumbre, su naturaleza y buscando la forma de abordarla. (ISO 2009)

- **La Gestión de Riesgos es sistemática, estructurada y oportuna**

  Contribuyendo a la eficiencia y consistencia y confiabilidad de lo resultados.

- **La Gestión de Riesgos está basada en una mejor disponibilidad de información**

  Haciendo que los responsables de la toma de decisiones se informen y tomen en cuenta cualquier limitación de la data o modelamiento usado o divergencia entre expertos. (ISO 2009)

- **La Gestión de Riesgos es adaptable**

Tesis publicada con autorización del autor
No olvide citar esta tesis

Alineándose con el contexto interno y externo de la organización así como al perfil de riesgo. (ISO 2009)

- **La Gestión de Riesgos toma en cuenta factores humanos y culturales**

Reconociendo las capacidades, percepciones e intenciones de las personas que pueden facilitar o ayudar el logro de los objetivos de la organización. (ISO 2009)

- **La Gestión de Riesgos es transparente e inclusiva**

Generando una apropiada participación de los stakeholders y en particular de los que toman las decisiones en todos los niveles de la organización. Esta participación también permite a los stakeholders estar adecuadamente representados tomándose en cuenta sus puntos de vista para determinar el criterio de riesgo. (ISO 2009)

- **La Gestión de Riesgos es dinámica, iterativa y sensible a los cambios**

Haciendo que mientras ocurran eventos internos o externos, cambios en el contexto y el conocimiento, el monitoreo y revisión de riesgos tendrá lugar apareciendo nuevos riesgos, cambiando algunos y eliminando otros. (ISO 2009)

- **La Gestión de Riesgos facilita la mejora continua de la organización**

Llevando a la organización a desarrollar e implementar estrategias para mejorar la madurez de la gestión de riesgos de la mano de los demás aspectos de la organización. (ISO 2009)

### 3.1.3 Otros conceptos

#### 3.1.3.1 Informe de Gestión de Riesgo Operacional (IG – Rop)

"El IG-ROP, Informe de Gestión de Riesgo Operacional, es un servicio disponible en el Portal del Supervisado que permite reportar, a través de medios electrónicos, el informe anual de riesgo operacional, requerido mediante el artículo 15° del Reglamento para la Gestión del Riesgo Operacional, aprobado mediante Resolución SBS N° 2116-2009." (SBS 2009)

Este servicio será manejado por el responsable de gestión de riesgo operacional y por el personal que la empresa supervisada autorice como usuario. Estos responsables ingresarán la información al sistema de acuerdo a la estructura definida para este tipo de informe, que incluye aspectos de cumplimiento normativo, mejores prácticas en la

gestión de este riesgo así como aspectos referidos a la continuidad del negocio y la seguridad de la información.

## 3.2 Marco Regulatorio / legal

### 3.2.1 Superintendencia de Banca, Seguros y AFP (SBS)

Organismo encargado de la regulación y supervisión de los Sistemas Financiero, de Seguros y del Sistema Privado de Pensiones, así como de prevenir y detectar el lavado de activos y financiamiento del terrorismo. Su objetivo primordial es preservar los intereses de los depositantes, de los asegurados y de los afiliados al Sistema Privado de Pensiones (SPP) trabajando bajo dos principios básicos: Regulación y Supervisión (Ver Anexo 3).

### 3.2.2 Ley General del Sistema Financiero – Ley N° 26702

Esta ley establece el marco de regulación y supervisión a la que se someten las empresas que operen en el sistema financiero y de seguros, así como aquellas que realizan actividades vinculadas o complementarias al objeto social de dichas personas teniendo como objeto principal propender al funcionamiento de un sistema financiero y un sistema de seguros competitivo, sólidos y confiables, que contribuyan al desarrollo nacional (SBS 2011).

### 3.2.3 Circular N° G - 139 – 2009

Establece los criterios para la gestión de la continuidad del negocio como parte de una adecuada gestión del riesgo operacional tomando como referencia los estándares internacionales como el BS-25999. Esta circular aplica para las empresas señaladas en los artículos 16 y 17 de la Ley General así como las Administradoras de Fondos y Pensiones AFP.

En sus artículos 3°, 4°, 5°, 6°, 7°, 8° y 9° especifica todas las consideraciones a tener en cuenta para una adecuada gestión de la continuidad del negocio, desde las personas y unidades responsables, las fases, las pruebas para su implementación así como la adecuada documentación sustentatoria (SBS 2009).

### 3.2.4 Resolución SBS N° 2115

Emitida en abril del 2009, establece el requerimiento de patrimonio efectivo por riesgo operacional a lo largo de los cuatro capítulos descritos en el Anexo 4 (SBS 2012).

Tesis publicada con autorización del autor
No olvide citar esta tesis

### 3.2.5 Resolución SBS N° 2116

Emitida en abril del 2009, establece el reglamento para la gestión de riesgo operacional a lo largo de los cinco capítulos descritos en el Anexo 5 (SBS 2012).

## 3.3 Normas aplicables a la Gestión de la Continuidad del negocio nacionales e internacionales

A continuación, se presentará una serie de normas nacionales e internacionales que sirven de guía para el diseño e implementación de los diversos Sistemas de Gestión de la Continuidad del negocio.

### 3.3.1 NFPA 1600 – Standard on Disaster/Emergency Management and Business Continuity Programs

Esta norma establece un conjunto común de criterios para la gestión de desastres y/o emergencias y continuidad del negocio denominados en lo sucesivo como programa, siendo aplicable solo para empresas públicas y no para organizaciones sin fines de lucro o empresas privadas. El programa incluye los siguientes elementos, descritos a lo largo de las secciones 5.2 a la 5.16 (NATIONAL FIRE PROTECTION ASSOCIATION 2006):

- Leyes y autoridades.
- Valoración del riesgo.
- Prevención de incidentes.
- Mitigación.
- Gestión de recursos y logística.
- Asistencia.
- Planificación.
- Gestión de Incidentes.
- Comunicaciones y advertencias.
- Procedimientos operacionales
- Facilidades
- Pruebas
- Ejercicios, evaluaciones y acciones correctivas
- Comunicación ante crisis e información pública.
- Administración y finanzas.

Tesis publicada con autorización del autor
No olvide citar esta tesis

### 3.3.2 HB 221:2004 Business Continuity Management (BCM)

Manual recomendado por el Disaster Recovery Institute (DRI) considerándola una herramienta esencial para el logro de un BCM viable. Este manual está alineado con el marco de gestión de riesgos que se indica en AS / NZS 4360:2004, Risk Management. El BCM juega un papel fundamental como parte del proceso de gestión del riesgo de la organización proporcionando un proceso de mitigación fundamental para determinados tipos de riesgos. Este manual demuestra que la gestión de riesgos y BCM están intrínsecamente relacionados, como parte de una gestión de riesgo efectiva (STANDARDS AUSTRALIA 2004).

### 3.3.3 Basilea II en el Perú

El desarrollo financiero de los últimos años llevó al Comité de Basilea a desarrollar un esquema más amplio, basándose en 3 pilares, de los riesgos que asumen los bancos (Ver Anexo 6). Se establece como objetivo de este nuevo documento "lograr una medición del capital regulatorio más sensible al riesgo, complementada con la profundización del proceso de supervisión bancaria y la disciplina de mercado" (SBS 2003).

En abril de 2003, la SBS asume la tarea de implementar y adecuar lo propuesto por el comité de Basilea y establece el Comité Especial Basilea II (CEB), en el cual se encuentran representadas las diversas áreas de la Superintendencia involucradas. Entre las principales labores que viene realizando este Comité se encuentran:

- Diseño de la supervisión según los principios de Basilea II.
- Adecuación de la estructura orgánica.
- Acceso a información a nivel de operación: Nueva Central de Riesgos.
- Establecimiento de procedimientos de supervisión y mecanismos de alerta.
- Evaluación cuantitativa del impacto de la implementación del Nuevo Acuerdo de Capital (NAC) en el sistema financiero peruano.
- Identificación de los principales cambios en la regulación y estudio de nuevas normas.
- Diseño del marco de transparencia ajustado a Basilea II.

## 4 Estado del arte

A continuación, se presentará una de serie productos comerciales que ofrecen soluciones y apoyo en la gestión de continuidad del negocio:

Tesis publicada con autorización del autor
No olvide citar esta tesis

### 4.1 Formas exactas de resolver el problema

Al no existir aun una solución exacta al problema planteado en el rubro de seguros específicamente, se presentará el ejemplo de una empresa financiera que cuenta con el servicio de seguros:

#### 4.1.1 Banco Internacional Español - Bankinter

Es una de las principales entidades financieras en España y como tal está sujeta a la supervisión del Banco de España y de la Comisión Nacional del Mercado de Valores e inscrita en el Registro Oficial de Bancos y Banqueros con el número 0128 (BANCO INTERNACIONAL ESPAÑOL – BANKINTER 2012). Entre sus principales servicios se tiene (BANCO INTERNACIONAL ESPAÑOL – BANKINTER 2012):

- Cuentas.
- Tarjetas.
- Depósitos.
- Fondo de inversión.
- Planes de pensiones.
- Seguros.
- Hipotecas.

El 18 de Julio del 2012, el BSI le hizo entrega de su primer certificado a nivel internacional de la nueva norma ISO 22301:2012. El certificado avala que la entidad financiera mantiene un SGCN conforme a los requisitos de esta nueva norma, dejando a Bankinter como la primera entidad financiera a nivel mundial certificada en ISO 22301 (BSI 2009).

### 4.2 Formas aproximadas de resolver el problema

Las formas alternativas de solucionar el problema con brindadas a través de servicios de consultoría (Ver Anexo 7).

### 4.3 Productos comerciales para resolver el problema

Se presentan algunas de las principales herramientas de software comercial usadas como apoyo en la Gestión de Continuidad del Negocio (Ver Anexo 8).

En el Anexo 9 se presenta un cuadro comparativo que resume las características de las herramientas mencionadas.

Tesis publicada con autorización del autor
No olvide citar esta tesis

### 4.4 Conclusiones sobre el estado del arte

En conclusión, dadas las recientes modificaciones de la SBS para una adecuada gestión del riesgo operacional, el surgimiento de nuevas normas y las soluciones encontradas se puede determinar que:

- Aún no hay productos y/o empresas que estén completamente alineados a los nuevos requerimientos. Es por ello que dada la coyuntura, es de suma importancia definir un diseño específico para las necesidades regulatorias peruanas, ya que de lo contrario, las empresas reguladas por la SBS incurrirían en faltas que podrían traer como consecuencias multas, pérdidas y daño reputacional.
- El tema del BCM ha ido evolucionando en los últimos años, desde normas, servicios de consultoras hasta herramientas de software; sin embargo, como en todo proceso de gestión es necesario coger todas estas herramientas y adecuarlas a las necesidades de un empresa o rubro, especialmente en el caso de las empresas aseguradoras, ya que al ser un negocio tan específico necesita de un estudio especializado que le permita tener un SGCN acorde a los riesgos del funcionamiento operativo de la misma empresa y a los riesgos que cubren sus seguros.
- La propuesta de manejar el plan de gestión de la continuidad por líneas de negocio basada en la ISO 22301 y usando el método alternativo estándar para el cálculo del requerimiento patrimonial aún no ha sido explotada en conjunto para el rubro de los seguros, lo cual representa una propuesta nueva y una oportunidad de mejora alternativa, con normas actualizadas, orientadas a una mejor gestión más eficiente y ordenada, brindando una herramienta que podría ser la base de una mayor ventaja competitiva en las empresas aseguradoras garantizando la continuidad de sus operaciones en caso de situaciones de desastre.

Tesis publicada con autorización del autor
No olvide citar esta tesis

# CAPÍTULO 2

## 1 Objetivo general

Diseñar un Sistema de Gestión de Continuidad de Negocio (SGCN) para una empresa de Seguros específica en caso de ocurrencia de sismos, acorde a las regulaciones de la Superintendencia de Banca, Seguros y AFP (SBS) basado en la Norma ISO/IEC 22301:2012, como parte de la Gestión de Riesgo Operacional.

## 2 Objetivos específicos

**OE1:** Elaborar una metodología para identificar los procesos, productos y/o servicios críticos para la continuidad del negocio.

**OE2:** Modelar los procesos, productos y/o servicios de negocio identificados en el punto anterior.

**OE3:** Elaborar los análisis de impacto de negocio (BIA, por sus siglas en inglés).

**OE4:** Elaborar un análisis de riesgos asociados a los escenarios de desastres establecidos.

**OE5:** Elaborar un plan de manejo de crisis.

**OE6:** Elaborar un plan de emergencia.

**OE7:** Elaborar un Plan de Recuperación de Desastres (DRP, por sus siglas en inglés) asociado a los escenarios de desastres establecidos.

**OE8:** Desarrollar un Plan de continuidad de negocios (BCP, por sus siglas en inglés) en caso de la ocurrencia de un sismo.

**OE9:** Elaborar un plan de pruebas para cada escenario de desastre establecido.

## 3 Resultados esperados

**Resultado 1 para el OE1:** Metodología para la identificación de procesos vitales de continuidad de negocio.

**Resultado 2 para el OE1:** Listado de los procesos, productos y/o servicios críticos para la continuidad clasificados por líneas de negocio.

Tesis publicada con autorización del autor
No olvide citar esta tesis

**Resultado 1 para el OE2:** Modelado de los procesos de negocio identificados como críticos para la continuidad.

**Resultado 1 para el OE3:** Análisis de impacto de negocio definiendo los requerimientos de recuperación en caso de la ocurrencia de un sismo.

**Resultado 1 para el OE4:** Análisis de riesgos considerando como escenario la ocurrencia de un sismo.

**Resultado 1 para el OE5:** Plan de manejo de crisis considerando como escenario la ocurrencia de un sismo.

**Resultado 1 para el OE6:** Plan de emergencia considerando como escenario la ocurrencia de un sismo.

**Resultado 1 para el OE7:** Plan de recuperación de desastres considerando como escenario la ocurrencia de un sismo.

**Resultado 1 para el OE8:** Plan de pruebas considerando como escenario la ocurrencia de un sismo.

**Resultado 1 para el OE9:** BCP considerando como escenario la ocurrencia de un sismo.

# 4 Herramientas, métodos y procedimientos

A continuación se describen las diferentes metodologías y procedimientos que se usarán para la gestión de cada uno de los resultados esperados.

## 4.1 Mapeo

En el Anexo 9, se presenta un mapeo de los resultados esperados con las herramientas, métodos y procedimientos que se van a emplear para su desarrollo.

## 4.2 Herramientas y metodologías

Para la gestión del producto, se usará principalmente los lineamientos brindados por la norma ISO/IEC 22301:2012 “Seguridad de la sociedad – Sistemas de gestión de la continuidad del negocio”, apoyándose además en algunas buenas prácticas de otras metodologías como la norma NFPA 1600 y Gestión de Procesos de Negocio (BPM, por sus siglas en inglés). A continuación se describirá cada una de estas metodologías así como su uso específico para el logro de los resultados esperados del producto.

Tesis publicada con autorización del autor
No olvide citar esta tesis

### 4.2.1 ISO/IEC 22301:2012

Según lo mencionado en su contenido, “Esta norma internacional aplica el “Plan-Do-Check-Act” (PDCA) para planificar, establecer, implementar, operar, funcionamiento, monitoreo, revisión, mantenimiento y mejora continua mejorando la actividad del SGCN.” (ISO 2012: 5).

Esta metodología será básicamente la que guiará la obtención del producto final. A continuación, se presentará un cuadro donde se describen las cláusulas que fueron incluidas a lo largo de todo el proyecto según la Norma definida por ISO además de la lista de resultados esperados que estarían asociados a cada proceso:

| Proceso | Cláusula | Descripción | Resultado esperado |
|---|---|---|---|
| Plan | Cláusula 4 | Presenta los requerimientos necesarios para establecer el contexto del SGCN así como el alcance del mismo. (ISO 2012). | Metodología de identificación de procesos críticos de continuidad.<br>Listado procesos críticos para la continuidad de negocio.<br>Modelado de los procesos críticos para la continuidad del negocio.<br>Análisis de impacto de negocio definiendo los requerimientos de recuperación en caso de ocurrencia de sismo.<br>Análisis de riesgos asociados a la ocurrencia de un sismo.<br>Plan de manejo de crisis asociado a la ocurrencia de un sismo.<br>Plan de emergencia asociado a la ocurrencia de un sismo.<br>Plan de Recuperación de desastres asociado a la ocurrencia de un sismo.<br>Plan de pruebas asociado a la ocurrencia de un sismo |
| | Cláusula 5 | Resume los requerimientos específicos a los roles Gerentes del SGCN además de la declaración de políticas de las expectativas de los líderes para la organización. . (ISO 2012). | |
| | Cláusula 6 | Describe los requerimientos así como su relación estratégica y una guía integral de los principios del SGCN. . (ISO 2012). | |
| | Cláusula 7 | Soporta las operaciones del SGCN en lo referido a la competencia y el establecimiento de la comunicación en forma recurrente y oportuna con las partes interesadas mientras se documentar, controla, mantiene y conserva la documentación requerida. . (ISO 2012). | |
| Do | Cláusula | Define los requerimientos del | |

| Proceso | Cláusula | Descripción | Resultado esperado |
|---|---|---|---|
| | 8 | SGCN, como direccionarlos y desarrollar los procedimientos en caso de un incidente destructivo. (ISO 2012). | BCP en caso de ocurrencia de un sismo. |

Figura 8. Cláusulas incluidas en el proyecto de fin de carrera

Además, en el siguiente cuadro se resumirán las cláusulas que no se incluirán en el presente proyecto, así como la justificación que sustenta el porqué de esta decisión.

| Proceso | Cláusula | Descripción | Justificación |
|---|---|---|---|
| **Check** | Cláusula 9 | Sintetiza los requerimientos necesarios para medir el desempeño, conformidad del SGCN con esta Norma y el manejo de las expectativas. (ISO 2012). | ✓ El proyecto de fin de carrera, al cubrir sólo el diseño y la implementación del SGCN no medirá el desempeño ni efectuará acciones correctivas sobre el mismo. |
| **Act** | Cláusula 10 | Actúa en base debilidades identificadas ejecutando medidas correctivas. . (ISO 2012). | |

Figura 9. Cláusulas no incluidas en el proyecto de fin de carrera

### *4.2.2 ISO 31000: 2009*

Norma internacional que brinda un framework para el proceso de gestión de riesgo. Puede ser usada por cualquier organización sin importar su tamaño o sector. A pesar de que esta norma no puede ser usada para certificación, provee directrices internas y externas para evaluaciones de auditoría (ISO 2009).

Las directrices de esta norma servirán para elaborar el análisis de riesgos asociados a los escenarios de sismo. Este resultado será guiado por el proceso de gestión de riesgos definido (Ver figura 10), el cual contiene las siguientes actividades:

- **Comunicación y consulta**

  Este proceso debe tomar a lugar durante todo el proceso de gestión de riesgos. Esto facilitará la veracidad, relevancia y el entendimiento de la información intercambiada tomando en cuenta los aspectos de confidencialidad. (ISO 2009)

Tesis publicada con autorización del autor
No olvide citar esta tesis

- **Establecimiento de contexto**

Ayudando a articular los objetivos de la organización, definiendo los parámetros internos y externos a tomar en cuenta para los demás procesos. (ISO 2009)

- **Valoración del riesgo**

Proceso universal para la identificación del riesgo, su análisis y evaluación. (ISO 2009)

- **Tratamiento del riesgo**

Involucra la selección de una o más opciones para modificar el riesgo e implementar estas opciones. (ISO 2009)

- **Monitoreo y revisión**

Ambos deben ser planeados y ejecutados periódicamente definiendo claramente las responsabilidades. (ISO 2009)

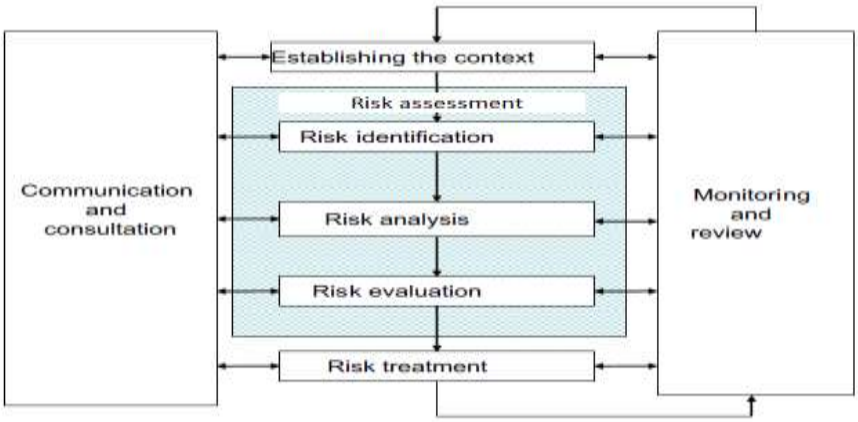


Figura 10: Proceso de gestión de riesgos (ISO 2009: 22)

### *4.2.3 NFPA 1600*

Norma australiana creada por el Comité de Gestión de Desastres que proporciona una base estandarizada para la planificación y gestión de programas de continuidad de negocio en caso de desastres o emergencia en los sectores público y privado. En la edición del 2007, se expande un framework conceptual para la gestión de desastres o emergencias y programas de continuidad de negocio. Además, esta edición identifica la prevención como un aspecto del programa como adicional a los 4 ya establecidos (mitigación, preparación, respuesta y recuperación), haciendo que esta norma esté alineada con disciplinas relacionadas a la Gestión de Riesgos, seguridad y prevención de pérdidas. (NFPA 1600 2007).

Tesis publicada con autorización del autor
No olvide citar esta tesis

La Norma contiene una sección de valoración de riesgos, la cual está orientada básicamente en vulnerabilidades que puedan ser explotadas por la ocurrencia de un desastre. Se menciona que:

> La valoración de riesgos debe clasificar los peligros por su frecuencia relativa y su severidad, teniendo en cuenta que podrían existir varias posibles combinaciones de frecuencia y severidad. La entidad debe intentar mitigar, prepararse, planificar y recuperarse de algunos peligros que podrían impactar significativamente a las personas, la propiedad, las operaciones, el entorno o la entidad en sí misma. (NFPA 1600 2007: 10)

En resumen, esta norma brinda muy buenas directrices para el diseño de un SGCN y por estar relacionada directamente con los riesgos y controles correspondientes a desastres naturales se tomarán como referencia las directrices de valoración de riesgos para el *análisis de riesgos asociados a los escenarios de sismo y* para *elaborar el plan de respuesta ante emergencias* mencionados como objetivo. De este modo, se podrá hacer un análisis de riesgos más adecuado al contexto del proyecto con un punto de vista mucho más especializado.

### *4.2.4 Business Process Management and Notation BPMN 2.0*

Es una metodología asociada al ciclo de vida de los procesos de negocio. Este se descompone en tramos identificando y mejorando procesos que pueden llevar a desarrollar la capacidad de los negocios y gestionarlos cuando estén operativos. (WORKPOINT LLC 2006)

Sin embargo, una de las fases más importantes para este modelo es la gestión del desenvolvimiento del proceso después de que este entra en operación para así poder monitorear el alcance de sus objetivos y poder encontrar el problema.

Esta metodología ha evolucionado a partir de un número de precursores de la tecnología. Algunas de estas tecnologías incluyen una serie de herramientas útiles; particularmente, para *el modelado de los procesos de negocio que brindan soporte a los servicios o productos que soporte a los servicios o productos identificados como objetivo* se utilizará la siguiente herramienta:

**Flujo de trabajo**

Es la automatización de un proceso de negocio, en su totalidad o en parte, por un tiempo definido durante el cual los documentos, información o las tareas se pasan de un participante a otro para la acción de acuerdo con un conjunto de reglas de procedimiento. (WORKPOINT LLC 2006)

# 5 Alcance

## 5.1 Limitaciones

El proyecto pertenece al área de Tecnologías de Información y pretende obtener el análisis y diseño de un SGCN en caso de desastres naturales basada en la Norma ISO/IEC 22301:2012 para empresas de seguros medianas en base a un modelo general del negocio. Se ha elegido este sector no sólo por el gran crecimiento que presenta este rubro, sino porque el tesista trabajó en una empresa del rubro, lo cual le permitió conocer parte del negocio así como personas con mucha más experiencia. Sin embargo, debido a la gran amplitud, complejidad y tiempo que tomaría desarrollar un SGCN para todos los tipos de desastres naturales que podrían ocurrir en el país, sólo se tomará en cuenta la ocurrencia de sismos.

De acuerdo a su definición, las líneas de negocio que serán cubiertas por el SGCN son las siguientes:

| NIVEL 1 | NIVEL 2 | Definición |
|---|---|---|
| **Ramos de vida** | Seguros de Vida en Grupo | Se refiere a las siguientes pólizas:<br>- Seguro de Vida en Grupo Particular<br>- Seguro de Vida para Trabajadores<br>- Seguro de Desgravamen<br>- Seguro de Vida Individual de Corto Plazo<br>- Sepelio de Corto Plazo |
| | Seguros de Vida Individual y Rentas | Se refiere a las siguientes pólizas:<br>- Seguro de Vida Individual de Largo Plazo<br>- Sepelio de Largo Plazo<br>- Seguro de Vida para ex - Trabajadores<br>- Renta Particular<br>- Pensiones del Seguro Complementario de Trabajo de Riesgo<br>- Renta de Jubilación |

Tesis publicada con autorización del autor
No olvide citar esta tesis

| NIVEL 1 | NIVEL 2 | Definición |
|---|---|---|
| | | - Pensión de Invalidez<br>- Pensión de Sobrevivencia<br>- Pensión de Invalidez-Régimen Temporal<br>- Pensión de Sobrevivencia-Régimen Temporal |
| | Seguros Previsionales y SCTR | Se refiere a las siguientes pólizas:<br>- Seguro Complementario de Trabajo de Riesgo<br>- Invalidez<br>- Sobrevivencia<br>- Gastos de Sepelio |

Figura 11. Líneas de negocio definidas por la SBS que podrían ser afectadas por la ocurrencia de un desastre natural

Cabe mencionar que, como complemento de la ISO/IEC 22301:2012, está planificado que se publique la ISO/DIS 22313 "Societal Security – Business Continuity Management Systems – Guidance" a fines de este año o a inicios del próximo año (BSI Group 2012) por lo que el presente proyecto también contempla la posibilidad de tomar esta nueva norma como referencia para el análisis y el diseño del SGCN.

Dentro de los principales obstáculos para el desarrollo del proyecto se encuentran:

Dificultad de acceso a determinada información por políticas de confidencialidad de las empresas se seguros.

Dado que el negocio de los seguros tiene procesos diferentes a los negocios convencionales; de venta y comercialización, por ejemplo, se podrá considerar entrevistas con personas involucradas en los distintos procesos de negocio para obtener una mejor orientación. Sin embargo, al poder tocarse temas riesgos de negocio y cumplimiento de regulación de la SBS, es los entrevistados omitan o se nieguen a dar cierto tipo de información para no perjudicar a la empresa donde trabajan.

Visitas de la SBS a las empresas donde laboran los especialistas, ya que estas podrían ocasionar dificultades en las reuniones por un tiempo porque tendrían que atender pendientes con la entidad reguladora originando posibles retrasos en la validación de resultados esperados a entregar.

Tesis publicada con autorización del autor
No olvide citar esta tesis

Finalmente, cabe resaltar que, si bien el presente proyecto sólo toma como alcance un de 3 desastre natural, el modelo de SGCN podrá ser seguido para realizar el diseño de un sistema que cubra los demás desastres, dando pie a uno mucho más completo que actualmente por cuestiones de tiempo y recursos no podrá ser cubierto.

### 5.2 Riesgos

| Riesgo identificado | Impacto en el proyecto | Medidas correctivas para mitigar |
|---|---|---|
| Posibilidad de no contar con la disponibilidad suficiente de la empresa para el desarrollo del proyecto | Retraso en la presentación de los resultados esperados. | Reprogramación de cronograma y avance con la información brindada hasta el momento. |
| Probabilidad de acumular observaciones de en los resultados esperados. | Retraso en la presentación de los resultados esperados. | Realizar pequeñas entregas validadas por la empresa y elaboradas con la dirección conjunta del asesor. |
| Posibilidad de obstáculos para brindar información confidencial de la empresa. | Imposibilidad para continuar con el análisis y diseño del SGCN. | Firma de acuerdos de confidencialidad entre la empresa y el tesista |
| Posibilidad de visitas de la SBS a la empresa. | Indisponibilidad de la empresa para programar reuniones. | Programación de entrevistas antes de la fecha de visita programada por la SBS. |

Figura12. Riesgos involucrados en el proyecto

## 6 Justificación y viabilidad

### 6.1 Justificativa del proyecto de tesis

Es importante para las aseguradoras del Perú efectuar el análisis y diseño de un SGCN en función de los nuevos requerimientos que pide la SBS y de sus propias necesidades de modo que la implementación del mismo permita a la organización alcanzar sus objetivos estratégicos.

Para las aseguradoras es necesario prevenir y planificar su respuesta frente a los diversos desastres naturales a los que está expuesto nuestro país no sólo por un tema regulatorio sino también porque este tipo de empresas tendrá que afrontar los gastos

Tesis publicada con autorización del autor
No olvide citar esta tesis

de su recuperación y principalmente la de sus asegurados, cubriendo todas las obligaciones que tengas los servicios que ofrecen sus productos.

Además, el proyecto es conveniente ya que a partir de él se podrán cubrir una serie de desastres naturales que, por razones académicas, no podrán ser abordados ahora haciendo que el diseño del proyecto pueda ser extendido por otro tesista u organización.

### 6.2 Análisis de viabilidad del proyecto de tesis

A continuación, se presentarán aspectos que influyen en la viabilidad del proyecto:

En cuanto a los conocimientos necesarios del negocio para poder alcanzar los objetivos del proyecto, serán proporcionados por la asesoría de personas que trabajan en el rubro, quienes brindarán su apoyo al tesista explicando la lógica del negocio y facilitando la información que crea sea necesaria.

En referencia al aspecto temporal, el proyecto es viable ya que a pesar de que el diseño de un SGCN puede tomar más de un año, el alcance se ha definido de modo que este ha quedado reducido a un escenario de desastre natural. Por otro lado, el proyecto solo es viable en cuanto al análisis y diseño ya que de haber optado por su implementación, este estaría sujeto a la gestión del cambio que pueden sufrir los procesos del negocio durante el periodo de ejecución de proyecto, lo que podría invalidar su implementación en una empresa.

Asimismo, se han encontrado una serie de metodologías que se ajustan a cada uno de los resultados esperados, haciendo que la elaboración de cada uno de ellos esté guiada por una serie de actividades, herramientas y criterios que ayuden al tesista a mejorar la calidad del contenido de los mismos.

Además, en cuanto al ámbito económico, el proyecto no requerirá de una inversión significativa de dinero, ya que al ser ejecutado por un estudiante de pre grado el factor económico pudo ser un gran obstáculo.

En conclusión, a pesar de las posibles limitaciones u obstáculos mencionados anteriormente, el presente proyecto es viable principalmente porque el tesista cuenta con los principales recursos para llevar a cabo su ejecución.

## 7 Plan de actividades

Ver Anexo 11.

Tesis publicada con autorización del autor
No olvide citar esta tesis

# CAPÍTULOS 3 – LA EMPRESA

## 1 Introducción

En el presente capítulo se muestra la información consolidada de la empresa según los lineamientos de la norma establecida. El apartado comprende la evaluación de los procesos para determinar su criticidad en la continuidad del negocio así como el modelado de los mismos.

## 2 Metodología para la Identificación de Procesos Críticos de Continuidad

### 2.1 Objetivo

La presente metodología tiene como objetivo identificar los procesos críticos para la continuidad del negocio mediante un proceso ordenado y cuantitativo que permita ver y evaluar al proceso de diferentes perspectivas brindando rangos de criticidad para finalmente, obtener una evaluación ponderada del mismo que nos permita clasificarlos y priorizarlos acorde a las necesidades reales de la empresa.

### 2.2 Elaboración de la encuesta

A continuación, se describirán los principales aspectos tomados en cuenta para la elaboración de la encuesta, la cual fue la principal herramienta de apoyo para la recopilación y consolidación de resultados.

#### *2.2.1 Información de apoyo*

Los principales documentos de apoyo para la elaboración de la encuesta son:

- ✓ **Análisis de Impacto del Negocio (BIA) de la empresa al 2012,** el cual sirve para identificar los principales factores y/o criterios a ser tomados en la evaluación, así como para determinar los umbrales y márgenes que debían ser aplicados a cada factor.

- ✓ **Lista de líneas de negocio, productos y procesos vigentes,** las cuales sirven para complementar la información disponible en la encuesta, de modo que el usuario pueda encontrar todas al momento de responder las preguntas.

#### *2.2.2 La encuesta*

A continuación, se explicará la estructura de la encuesta así como la forma de evaluación:

#### 2.2.2.1 *Estructura de las preguntas*

Se definen en base a los requerimientos y necesidades de la empresa de seguros, tomando en cuenta a los principales interesados del negocio, así como los factores que podrían afectar a los mismos. A continuación se muestra la descripción de la estructura, para mayor detalle ver el Anexo 12.

| Estructura de Encuesta | |
|---|---|
| **Presentación** | |
| Objetivo | Se explica al usuario la finalidad y los criterios a usar para la evaluación (Tiempo de interrupción, rentabilidad, cumplimiento y reputación). |
| Instrucciones | Se detalla al usuario las instrucciones a seguir para el correcto ingreso de los datos. |
| **Información** | |
| Datos generales | Se solicita la información básica del proceso a evaluar:<br>✓ Línea de negocio<br>✓ Producto asociado<br>✓ Nombre del proceso |
| Tiempo de interrupción | Solicita al usuario la información sobre el tiempo máximo de interrupción durante el cual el proceso puede dejar de funcionar. |
| Rentabilidad neta | Solicita al usuario determinar el impacto monetario que podría sufrir la empresa en caso de alguna interrupción. |
| Cumplimiento | Solicita al usuario identificar el tipo de sanciones que podría recibir la empresa en caso de alguna interrupción. |
| Reputación | Solicita al usuario identificar al stakeholder o interesado que se vería más afectado en caso de una interrupción. |
| Clasificación | Muestra al usuario el resultado obtenido después de la evaluación, permitiendo validar y comparar el mismo con su juicio experto. |

Figura 13. Estructura de la encuesta

#### 2.2.2.2 *Estructura de la calificación*

El cuestionario está formado por cuatro (4) tipos de preguntas, cada una de la cuales evalúa al proceso desde diferentes perspectivas; a cada una de ellas se le asignó un peso de acuerdo a las prioridades y necesidades de la empresa.

Tesis publicada con autorización del autor
No olvide citar esta tesis

Esta determinación de prioridades es elaborada bajo el juicio y conocimiento de los expertos del negocio, quienes acorde a sus necesidades y prioridades determinan que el mayor peso sería para el tiempo de interrupción con un 35%, un 30% para la rentabilidad neta, un 20% para el cumplimiento y un 15% en cuanto a su reputación (Ver Figura 14).

| N° | Tipo | Peso |
|---|---|---|
| 1 | Tiempo de interrupción | 35% |
| 2 | Rentabilidad | 30% |
| 3 | Cumplimiento | 20% |
| 4 | Reputación | 15% |

Figura 14. Pesos por pregunta

Además, se asigna un valor numérico específico a cada respuesta de modo que pueda ser ponderada. A partir de esto se define la siguiente distribución:

| Tipo | Peso | Respuesta | | | | | |
|---|---|---|---|---|---|---|---|
| | | a | b | c | d | e | f |
| | | 1 | 2 | 3 | 4 | 5 | 6 |
| **Tiempo de Interrupción** | 35% | | | | | | |
| **Rentabilidad** | 30% | | | | | | |
| **Cumplimiento** | 20% | | | | | | |
| **Reputación** | 15% | | | | | | |

Respuestas

Figura 15. Distribución de pesos y puntajes

Así, se obtiene el puntaje del proceso mediante una fórmula ponderada (ver Figura 16) para después clasificar al mismo en función de rangos definidos por el negocio (ver Figura 17).

$$\boldsymbol{Calificación} = \sum_{i=1}^{4} \boldsymbol{peso} * \boldsymbol{puntaje}$$

Figura 16. Fórmula para la obtención de la calificación

| Prioridad | Clasificación | Calificación |
|---|---|---|
| 4 | Bajo | [0 - 2> |
| 3 | Medio | [2 - 4> |

| Prioridad | Clasificación | Calificación |
|---|---|---|
| 2 | Alto | [4 - 5> |
| 1 | Muy Alto | [5 – 6] |

Figura 17. Rangos de clasificación

### *2.2.3 Descripción de resultados*

A continuación, se describe el significado de la clasificación:

| Calificación | Significado |
|---|---|
| **Bajo** | El proceso no es crítico para la continuidad del negocio y no se incurre en grandes pérdidas financieras, sanciones o daños en la reputación. |
| **Medio** | El proceso tiene un tiempo de recuperación promedio pero no es vital para la continuidad del negocio, su recuperación podría evitar algunas pérdidas financieras, sanciones o daños en la reputación. |
| **Alto** | El proceso soporta a productos claves de negocio, por lo que el tiempo de interrupción aceptable es muy corto y su continuidad es importante para evitar grandes pérdidas financieras, sanciones o daños en la reputación. |
| **Muy Alto** | El proceso soporta a productos críticos de negocio por lo que su recuperación inmediata es vital para evitar grandes pérdidas financieras, sanciones, cierre temporal o daños en la reputación. |

Figura 18. Descripción de clasificación de procesos

## 2.3 Conclusiones de la metodología

La presente metodología permite lograr un enfoque global del proceso, obteniendo resultados cualitativos que permitan a la empresa distinguir y clasificar fácilmente sus procesos. Cabe mencionar que esta evaluación puede realizarse periódicamente, acorde a los cambios que puedan existir en el negocio.

# 3 Relación de procesos críticos para la continuidad del negocio

## 3.1 Objetivo

Aplicar la metodología establecida a los procesos de la empresa aseguradora para determinar cuáles son los más críticos e iniciar el análisis y diseño en base a ellos.

Tesis publicada con autorización del autor
No olvide citar esta tesis

### 3.2 Aplicación y resultado

La evaluación es aplicada a cada uno de los procesos de negocio de la empresa aseguradora, obteniéndose una relación que muestra la clasificación de la criticidad obtenida como resultado (Ver Anexo 13).

Como estrategia, se plantea tomar los procesos con calificación “Alto” y “Muy Alto” para continuar con el análisis y diseño del SGCN.

## 4 Modelado de procesos críticos

### 4.1 Objetivo

Conocer y graficar cada una de las actividades involucradas en el análisis, de modo que el presente resultado sirva de base y referencia para el diseño del SGCN.

### 4.2 Alcance:

Para el modelado, se consideran los procesos con clasificación “Muy Alto” y “Alto” debido a la prioridad que tienen en el negocio, es decir, se consideran los siguientes:

| Línea de negocio | Producto | Proceso | Clasificación |
|---|---|---|---|
| Ramos de vida | Desgravamen | Atención de solicitudes de Cobertura | Muy Alto |
| Ramos de vida | Desgravamen | Suscripción, emisión y registro de información | Muy Alto |
| Ramos de vida | RV Pensión de Jubilación | Emisión de la póliza y endoso | Alto |
| Ramos de vida | No aplica | Gestión de servicio al cliente | Alto |
| Todos | No aplica | Gestión de Pagos | Alto |

Figura 19. Procesos involucrados en el desarrollo de SGCN

**Nota:** El detalle del modelado se encuentra en el Anexo 14.

Tesis publicada con autorización del autor
No olvide citar esta tesis

# CAPÍTULOS 4 – ANÁLISIS DE RIESGOS E IMPACTO EN EL NEGOCIO

## 1 Introducción

El presente capítulo muestra el análisis de los procesos realizado en relación a los riesgos y a su impacto en el negocio.

## 2 Análisis de impacto de negocio

### 2.1 Objetivo

El objetivo del análisis de impacto es determinar, por medio de un proceso formal y documentado, los impactos, efectos y pérdidas que podrían resultar si la organización sufre un evento de grandes magnitudes. Así mismo, este análisis permite establecer las funciones críticas, las prioridades de recuperación e interdependencias a fin de determinar Tiempos del Negocio acorde a sus necesidades.

### 2.2 Tiempos del Negocio

Son los rangos de tiempo asociados a la atención de una interrupción, los cuales son parámetros importantes para la definición de una adecuada estrategia de gestión de continuidad del negocio. Los tiempos del negocio definidos son:

**MTPD (Periodo Máximo Tolerable de Interrupción),** es el periodo de tiempo después del cual la viabilidad de una organización se verá amenazada de forma irrevocable si no puede reiniciar la entrega de un producto, proceso o servicio específico. Acorde a las necesidades del negocio, se consideró al MTPD desde 3 perspectivas diferentes: Financiera, Reputacional y de Cumplimiento.

**RTO (Tiempo de Recuperación Objetivo),** define el tiempo de recuperación objetivo de los recursos críticos que puede transcurrir desde el inicio de la interrupción operativa, hasta la recuperación de los servicios con un nivel estable brindando al negocio la continuidad operativa esperada. Este parámetro deberá definirse en función a la tolerancia del dueño del proceso.

**RPO (Punto de Recuperación Objetivo),** es el punto (tiempo) desde el que la información debe ser restaurada para brindar una adecuada línea base de información permitiendo la operación de una actividad una vez que ésta se haya reiniciado.

Tesis publicada con autorización del autor
No olvide citar esta tesis

## 2.3 Alcance

El alcance está acotado principalmente a los procesos incluidos dentro de la línea de negocio de Ramos de Vida que, como resultado de la evaluación de la metodología de procesos críticos, obtuvieron la clasificación de “Alto” y “Muy Alto”. A continuación se detallan los procesos involucrados en el análisis:

**Desgravamen:**

- ✓ Suscripción, emisión y registro de información.
- ✓ Atención de solicitudes de Cobertura.

**Renta Vitalicia:**

- ✓ Emisión de la póliza y endoso.

**Vida y accidentes:**

- ✓ Gestión de servicio al cliente.
- ✓ Gestión de Pagos

## 2.4 Indicadores de Continuidad

| Producto | Proceso | MTPD | RTO | RPO |
|---|---|---|---|---|
| Desgravamen | Suscripción, emisión y registro de información | 5 días | 24 horas | 3 días |
| | Atención de solicitudes de Cobertura | 10 días | 24 horas | 3 días |
| Jubilación | Emisión de la póliza y endoso | 2 días | 24 horas | 24 horas |
| Vida y Accidentes | Gestión de Pagos | 48 horas | 24 horas | 24 horas |
| | Gestión de servicio al cliente | 48 horas | 24 horas | 24 horas |

Figura 20. Indicadores de continuidad por proceso

## 2.5 Recursos Asociados a la recuperación

A continuación, se muestra la lista de recursos asociados a la recuperación de los servicios:

| Tipo | Nombre de recurso |
|---|---|
| Recursos humanos | Especialistas en operaciones, contabilidad y finanzas. |
| Infraestructura | Oficinas de operación |
| | Teléfonos / celulares |
| | Computadoras / laptop |

Tesis publicada con autorización del autor
No olvide citar esta tesis

| Tipo | Nombre de recurso |
|---|---|
| Tecnología | Servidores |
| | Redes |
| | Correo electrónico |
| | Sistemas “core”:<br>✓ Sistema de vida<br>✓ Sistema Sic CRM<br>✓ Sistema operativo contable<br>✓ Sistema contable<br>✓ Sistema de cotización<br>✓ Sistema de producción<br>✓ Sistema de atención al cliente |
| Información | ✓ Información personal del cliente<br>✓ Declaración personal de salud<br>✓ Información de póliza<br>✓ Órdenes de pago<br>✓ Órdenes de liquidación<br>✓ Estados financieros<br>✓ Cheques u otros documentos de pago. |
| Proveedores | ✓ Telefónica (Comunicaciones)<br>✓ Innovacción (Gestión de TI)<br>✓ Polfiile (Custodia de documentos físicos)<br>✓ Courier (Envío de documentos al cliente)<br>✓ Luz del sur (Fluido eléctrico) |

Figura 21. Recursos asociados a la recuperación

# 3 Estrategias de continuidad

## 3.1 Objetivo

Evaluar, priorizar y seleccionar estrategias de continuidad acorde a las necesidades reales del negocio, de modo que estén alineados a los requerimientos de los procesos críticos definidos inicialmente. Estas estrategias fueron diseñadas tomando en cuenta la información y los tiempos objetivos de recuperación definidos en el BIA.

## 3.2 Recursos

Los recursos considerados en el presente análisis se clasifican en: Personal, Tecnología, Información/Documentos, Proveedores e Infraestructura.

- **Aspectos considerados**

Se debe tomar en cuenta las siguientes consideraciones para el análisis:

- ✓ La seguridad del personal es primordial.
- ✓ La seguridad de la información es considerada dentro de las prioridades.
- ✓ Implementación de sitios alternos de operaciones.

- **Tipos de centros de hardware de respaldo en sede alterna**

**Hot Site:**

Recuperación inmediata. El Sitio Alterno requiere de soluciones de replicación "espero" tanto a nivel de infraestructura como de datos (0- 4 horas).

**Warm Site:**

Recuperación basada en copias de respaldo. El Sitio Alterno debe existir con conectividad, enlaces de terceros y equipos listos para restaurar las copias de respaldo (24 a 48 horas).

**Cold Site:**

Recuperación basada en copias de respaldo. El Sitio Alterno debe contar como mínimo con la conectividad necesaria (1 semana).

## 3.3 Estrategias propuestas por tipo de Recurso

Las estrategias planteadas se elaboran en base a los recursos de finidos anteriormente: Personas, información, tecnología, infraestructura y proveedores (Ver Anexo 15).

# 4 Análisis de riesgos

A continuación, se presenta el análisis de riesgo por proceso. Para determinar el nivel de riesgo (ver Figura 24) se evaluó principalmente el impacto (ver Figura 22) y la probabilidad de ocurrencia (ver Figura 23).

Tesis publicada con autorización del autor
No olvide citar esta tesis

| Impacto | |
|---|---|
| **Calificación** | **Descripción** |
| 1 | Insignificante |
| 2 | Bajo |
| 3 | Medio |
| 4 | Alto |
| 5 | Muy Alto |

Figura 22. Calificación de impacto

| Probabilidad | |
|---|---|
| **Calificación** | **Descripción** |
| 1 | No ha ocurrido en 5 años |
| 2 | Al menos una ocurrencia en 5 años |
| 3 | Al menos una ocurrencia en 3 años |
| 4 | Al menos una ocurrencia cada año |
| 5 | Ocurre frecuentemente |

Figura 23. Descripción de la probabilidad de ocurrencia

| Nivel de riesgo | | Criticidad |
|---|---|---|
| **Desde** | **Hasta** | |
| 0 | 3 | Bajo |
| 3 | 6 | Moderado |
| 6 | 8 | Alto |
| 8 | 10 | Extremo |

Figura 24. Clasificación del nivel de riesgo

**Nota:** La matriz de riesgos por proceso se encuentra en el Anexo 16.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS PUCP

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

# CAPÍTULOS 5 – PLAN DE MANEJO DE CRISIS

## 1 Introducción

En el presente capítulo se establecen los lineamientos para el manejo de crisis acorde a las necesidades, capacidades y recursos de la empresa aseguradora.

## 2 Objetivo

El presente plan describe procedimientos para realizar una respuesta estratégica efectiva ante la ocurrencia de una crisis, con el fin de evitar o reducir el impacto negativo que este pueda generar en la empresa, protegiendo la integridad de los empleados, su reputación y su estabilidad financiera

## 3 Alcance

El alcance del plan está acotado por los siguientes lineamientos:

- El plan involucra a todas las personas que se encuentren en las instalaciones de la empresa.
- El presente plan contempla básicamente los procesos críticos de continuidad con clasificación “Alto” y “Muy Alto” en la empresa.
- Las actividades mencionadas a continuación se han diseñado principalmente frente a la ocurrencia de un sismo, sin embargo, se puede contemplar la ampliación de escenarios.

## 4 Definiciones

**Incidente**, es una situación que causa o puede causar una interrupción o una reducción en la operación y calidad del servicio de TI.

**Evento**, es una situación que puede afectar significativamente la reputación, seguridad de los colaboradores o clientes la empresa, continuidad del negocio

**Crisis**, es un evento que ocasiona o amenaza con ocasionar, un efecto negativo y grave en la integridad de las personas, operación de los procesos del negocio, los resultados financieros y/o la reputación del banco, afectando el cumplimiento de sus objetivos estratégicos.

Tesis publicada con autorización del autor
No olvide citar esta tesis

**Manejo de Crisis**, es el marco estratégico que guía una organización y a sus líderes a estar preparados para manejar y recuperarse de eventos y acontecimientos adversos que amenazan las operaciones, las personas, estrategia, reputación y el futuro de la organización.

- Identifica acontecimientos, riesgos y vulnerabilidades.
- Establece políticas de gobierno para la preparación general, gestión, respuesta, y la recuperación.
- Proporciona una guía para gestionar la crisis y la toma de decisiones a todo nivel en la organización.
- Orquesta y alinea actividades de respuesta a incidentes relacionadas incluyendo continuidad, seguridad, respuesta de emergencia, impacto humano, comunicaciones, etc.
- Inculca confianza en los inversionistas y protege la marca
- El manejo de las crisis involucra a la más alta dirección de la Empresa.

## 5 Estructura para el Manejo de Crisis

A continuación, se muestra la estructura diseñada por el tesista como modelo de gestión de crisis:

Figura 25. Estructura para el manejo de crisis

## 5.1 Descripción

### *5.1.1 Equipo de Gestión de Crisis (EGP)*

Equipo clave para la gestión de crisis, con el poder de decisión para elaborar respuestas estratégicas sobre la crisis o ante situaciones que pueden convertirse en una.

Entre las responsabilidades del EGP se encuentran:

- ✓ Definir y aprobar las políticas y estrategias.
- ✓ Evaluar el impacto y las consecuencias de una crisis.
- ✓ Distribuir y asignar los recursos necesarios acorde a la crisis.
- ✓ Supervisar el avance de las operaciones de respuesta.
- ✓ Informar periódicamente y según sea el caso al Directorio o entidades gubernamentales.
- ✓ Aprobar las solicitudes de los distintos equipos de soporte como lo son el de comunicaciones y el de asistencia humanitaria.
- ✓ Aprobar la estrategia de comunicaciones.
- ✓ Aprobar los cambios tácticos y operacionales solicitados.
- ✓ Autorizar, si fuera necesario, la activación del Sitio Alterno de operaciones.
- ✓ Convocar, dependiendo de la crisis, a un miembro ad hoc como apoyo.

#### *5.1.1.1 Estructura del Equipo de Gestión de Crisis*

En el Anexo 17, se muestra la estructura diseñada por el tesista acorde a la estructura organizacional de la empresa.

Cabe mencionar que a la reunión pueden ser convocadas otras personas (Miembro Ad-Hoc), esto según el criterio del EGP, de modo que pueda servir de apoyo con información especializada y apoyo en la definición de acciones.

### *5.1.2 Gestión de Emergencias, Incidentes de TI y Eventos*

#### *5.1.2.1 Equipo de Gestión de Incidentes de TI*

Equipo responsable de dar seguimiento a las diferentes actividades relacionadas a TI y monitorear las alertas de incidentes y fallas en la infraestructura o servicios ofrecidos a la empresa. Dentro de sus responsabilidades se encuentra:

- Brindar soporte de primer y segundo nivel (transfiriendo el incidente a los expertos)
- En caso de transferir el incidente a los expertos, monitorear el estado de los mismos.
- Coordinar con el Equipo TIC las actividades a realizar para adecuada recuperación de los servicios.
- Comunicar a los interesados involucrados en el incidente (responsables del producto, proceso o servicio) así como a los miembros de la unidad de riesgos (especialistas en Continuidad del negocio) para que puedan dar un seguimiento adecuado.

#### *5.1.2.2 Equipo de Respuesta a Emergencias*

Equipo encargado de monitorear y dar una respuesta adecuada y oportuna ante la ocurrencia de una emergencia, buscando controlar la situación y mitigando las consecuencias que se puedan presentar, resguardando principalmente a las personas.

Las actividades de este equipo (y el plan respectivo) se activan ante situaciones como incendios, emergencias médicas, sismos, saqueos, manifestaciones entre otros.

#### *5.1.2.3 Equipos especializados*

Son grupos de personas especializadas en determinadas actividades, que servirán de apoyo a los Equipos de Gestión de Crisis y Gestión de Emergencias, Incidentes de TI y Eventos.

#### *5.1.2.4 Equipo de Comunicación en Crisis*

Tiene como objetivo principal apoyar la respuesta ante una crisis y proteger la reputación de la empresa frente a los diferentes medios de comunicación. Este equipo brindará estrategias adecuadas de comunicación durante la ocurrencia de una crisis o evento grave a los diferentes equipos involucrados.

#### *5.1.2.5 Equipo de Asistencia Humanitaria*

Tiene como objetivo brindar el apoyo necesario a todos los empleados de la empresa en caso se vean afectados por la ocurrencia de un evento grave o crisis, facilitando le manejo y asignación de provisiones y atención médica a las personas que lo requieran.

Tesis publicada con autorización del autor
No olvide citar esta tesis

#### *5.1.2.6 Unidad de Riesgos – Continuidad de Negocio*

Equipo conformado por los especialistas en Continuidad de Negocio de la Unidad de Riesgos. Tiene como objetivo filtrar y apoyar en el análisis de los diversos incidentes y eventos que se puedan originar. Asesora a los diferentes niveles de manejo de crisis en las posibles soluciones y las principales implicancias que estas tienen en el negocio.

## 6 Estructura de acción

### 6.1 Notificación

En esta fase, las unidades receptoras, notifican la ocurrencia de un incidente o evento. Dependiendo del tipo y la visibilidad del mismo, podría ser reportado por:

- Servicio de atención al cliente.
- Unidades de negocio
- Oficial de Cumplimiento Normativo
- Oficial de cumplimiento – LAFT

Las notificaciones son vía correo electrónico o llamadas a las unidades correspondientes y a los especialistas en Continuidad de Negocio, de modo que monitoreen las ocurrencias y evalúen el impacto que estos pueden generar en el negocio para tomar las medidas respectivas.

### 6.2 Análisis y Evaluación

Luego de la notificación del incidente, los especialistas de Continuidad de Negocio realizarán una evaluación del impacto con los responsables involucrados, a la vez que realizan un monitoreo o seguimiento del estado de la solución del incidente. En base a esto, se decidirá si escalar o no a través de la estructura definida anteriormente.

Las acciones a ejecutarse a través de la estructura jerárquica son:

- ✓ No ejecutar acciones.
- ✓ Realizar seguimiento conjunto.
- ✓ Activar el EGC.

Tesis publicada con autorización del autor
No olvide citar esta tesis

## 6.3 Respuesta

Dependiendo de la estrategia definida por los especialistas de Continuidad de Negocios, se puede proceder a diferentes procedimientos. A continuación se describen los principales.

### *6.3.1 Realizar seguimiento conjunto*

En caso el incidente esté relacionado a TI, gestionar las comunicaciones para conocer los planes de acción a ejecutar y estimar el impacto en el negocio a través del tiempo para determinar en qué momento escalar.

Por otro lado, si el incidente se debe a una emergencia, se deberá activar el Plan de manejo de Emergencia. Finalmente, en caso la ocurrencia del incidente se deba a un error operativo en la ejecución de algún proceso de negocio, comunicarse directamente con los usuarios para determinar la mejor solución.

Una vez que el plan de acción se ejecute y haya solucionado el incidente, debe ser comunicado a los interesados correspondientes (incluyendo a los especialistas en Continuidad de Negocio). De no solucionar el evento y habiendo transcurrido un tiempo que ponga en riesgo a la empresa (dependiendo del tipo de evento), se deberá escalar al EGC.

### *6.3.2 Equipo de Manejo de Crisis*

**Notificación y/o Escalamiento**

Los criterios de notificación para escalar un evento al Equipo de Manejo de Crisis son:

| **Las situaciones que el especialista debe considerar para la notificación son:** |
|---|
| **Eventos de Seguridad**: Accidentes graves, secuestro, manifestaciones, saqueos u otro incidente que afecte a cualquier empleado de la empresa. |
| **Desastres Naturales**: Sismos, inundaciones o huaycos que afecten la operatividad parcial o total de la empresa. |
| **Operacional**: Interrupción total o parcial de procesos de negocio y TI que, a pesar de haber aplicado un plan de acción no se soluciona con el pasar de las horas. |
| **Entorno político y social**: Situaciones que se pueden originar producto de |

| |
|---|
| cambios o eventos políticos y/o sociales. |
| **Regulaciones**: Surgimiento o cambios de normas que puedan afectar severamente el cumplimiento regulatorio de la empresa. |
| **Difusión en medios de comunicación**: Rumores o noticias que puedan generar un impacto negativo en la reputación frente a los clientes y los principales interesados de la empresa. |

Figura 25. Situaciones de notificación de la empresa

**Activación del EGP**

Este equipo será activado de acuerdo a la magnitud y duración del evento. A modo de información, los especialistas en Continuidad deberán brindar la siguiente información:

- Descripción del evento
  - Tipo de evento
  - Estado actual del evento
  - Áreas o unidades involucradas

- Lugar de reunión
  - Si el evento ocurre en horario de trabajo, la reunión se llevará a cabo en la sala del Piso 8 de la empresa. En caso las instalaciones hayan sido afectadas por el incidente, la reunión se llevará a cabo en las instalaciones del sitio alterno de operaciones.
  - Si el evento ocurre fuera del horario de trabajo, la reunión física dependerá del día y la hora en la que se presente, de lo contrario las coordinaciones serán vía telefónica o correo electrónico.

**Operación del EGP**

El líder de este equipo dirige la reunión bajo la asesoría de los especialistas en Continuidad del Negocio. Durante la sesión, se deberá determinar las acciones de respuesta y los recursos convenientes para ejecutarlas en base al tipo de evento y al impacto que este genera en el negocio a corto, mediano o largo plazo. Además se definirán los plazos para las reuniones de revisión de estado del evento.

Cuando se activa el EGP, el Líder de este equipo es quien dirige la reunión y gestiona las actividades del equipo. Durante la reunión se deberá determinar la frecuencia y la ubicación de las reuniones, de acuerdo al acontecimiento y acciones de respuesta necesarias.

Con el objetivo de llevar a cabo una reunión más ordenada, se ha definido las siguientes etapas:

**a. Diagnóstico**

En esta etapa, se informa a los miembros el EGP, se evalúa y estima el impacto en el negocio para que, en función a ello, se pueda establecer prioridades y medidas correctivas que mitiguen el impacto negativo.

- **Descripción de escenario**, el líder del equipo se encargará de completar el formato "Informe de escenario" (Ver Anexo 18) y proporcionarlo a los demás miembros.

- **Análisis de impacto**, se utilizará la "Guía de Análisis" (Ver Anexo 19) para determinar las implicancias y consecuencias de un evento determinado en el negocio.

- **Elaboración de estrategia**, como resultado del análisis previo y determinando las actividades o recursos necesarios.

**b. Coordinación**

En este punto, se realizará una pausa para que, cada uno de los miembros del equipo pueda obtener información adicional y realizar las coordinaciones necesarias para apoyar la ejecución de la estrategia

**c. Monitoreo**

En esta etapa, los miembros se reunirán nuevamente con el fin de informar los avances logrados así como el nuevo estado del evento para realizar un nuevo diagnóstico e iniciar el ciclo nuevamente hasta que la situación esté bajo control para proceder a desactivar el Equipo.

A continuación, se muestra el ciclo del desarrollo de las reuniones, diseñado por el tesista, para la empresa:

Tesis publicada con autorización del autor
No olvide citar esta tesis

Figura 26. Ciclo de manejo de crisis

**Desactivación del EGP**

Se deberá considerar los siguientes aspectos:

- Los medios de comunicación han dejado de comentar el evento referente a la empresa.
- El impacto ha sido mitigado totalmente o ha sido reducido a niveles aceptables para el negocio.
- Se acordarán las fechas para posteriores reuniones, de modo que se compruebe la estabilidad de las soluciones y el estado de recuperación de la empresa después de superado el incidente.

## 7 Mantenimiento del Plan

El presente plan debe ser adecuadamente revisado y actualizado teniendo en cuenta las siguientes consideraciones:

- Todo el plan debe ser revisado y actualizado por lo menos una vez al año, validando que cumpla con los requerimientos de la empresa y sobretodo regulatorios.

Tesis publicada con autorización del autor
No olvide citar esta tesis

- En caso se presente algún cambio organizacional, el plan deberá adaptarse a la nueva estructura.
- De realizarse alguna auditoría o revisión externa a la Unidad de Riesgos, se deberá tomar en cuenta las observaciones y oportunidades de mejora, estimando el tiempo para la respectiva actualización.
- En caso ocurran nuevos escenarios de eventos que no se hayan incluido dentro del presente análisis, se deberá actualizar las acciones y estructura de ser necesario.

Tesis publicada con autorización del autor
No olvide citar esta tesis

# CAPÍTULOS 6 – PLAN DE RESPUESTA A EMERGENCIAS

## 1 Introducción

En el presente capítulo se establece el diseño de un plan de respuesta a emergencias acorde a las necesidades, capacidades y recursos de la empresa.

## 2 Objetivo

El presente plan tiene como objetivo definir y desarrollar procedimientos para prevenir, responder y estabilizar las situaciones después de un incidente y administrar el centro de operaciones de emergencia, considerando además como prioridad el cuidado y atención de las personas involucradas.

## 3 Estrategias de Respuesta a Emergencias

Los procedimientos se dividirán en 3 etapas:

### 3.1 Etapa I: Antes

La estrategia se basa principalmente en el establecimiento de procedimientos que permitan prevenir y/o manejar los eventos que pueden originar situaciones de emergencia. Estas se enfocarán en los siguientes componentes:

- **Estrategias de Infraestructura**
  - ✓ Asegurar y verificar periódicamente la adecuada señalización de las instalaciones de la empresa.
  - ✓ Asegurar el mantenimiento y operatividad de los sistemas de alarmas de evacuación.
  - ✓ Asegurar el mantenimiento y operatividad de los sistemas contra incendios (extintores, detectores de humo, hidratantes)
  - ✓ Realizar la evaluación anual de seguridad física de las instalaciones, manteniendo y/o implementando nuevos controle de acuerdo a los riesgos identificados.
  - ✓ Solicitar anualmente al INDECI el servicio de “Inspección Técnica de Seguridad en Defensa Civil de Detalle”.
  - ✓
- **Estrategias de RRHH**
  - ✓ Mantener el compromiso a nivel institucional a través de las iniciativas de la Alta Dirección respecto a la importancia de contar con un Plan de

Respuesta a Emergencias actualizado, difundido y probado en un proceso de mejora continua.

- ✓ Establecer un plan de seguridad de defensa civil, definiendo brigadas con el apoyo y asesoría del INDECI.
- ✓ Organizar simulacros semestrales de evacuación y asegurar el correcto desempeño de los brigadistas.
- ✓ Realizar capacitaciones semestrales, internas o externas, en temas afines al manejo de emergencias (manejo de equipos contra incendios, primeros auxilios, entre otros).
- ✓ Asegurar el mantenimiento del esquema de comunicación con las entidades o agencias externas de apoyo (Bomberos, Defensa Civil, etc.).

- **Estrategias de Recursos**
  - ✓ Asegurar la provisión del botiquín de emergencias.
  - ✓ Realizar acuerdos con proveedores para asegurar el aprovisionamiento de donaciones humanitarias a los miembros de la organización, en caso sea necesario.
  - ✓ Mantener una lista de contactos de miembro de la organización actualizada.

### 3.2 Etapa II: Durante

Las estrategias para actuar durante la ocurrencia de un sismo son:

- Activar el Plan de Emergencias, ejecutando primero el plan de defensa civil definido, movilizando al personal hacia las zonas seguras bajo la dirección de los brigadistas.

- Asegurar que el botiquín de emergencias sea llevado al punto de reunión para poder hacer uso de él en caso sea necesario.

### 3.3 Etapa III: Después

Las estrategias de acción posteriores a la ocurrencia de un sismo se enfocarán en los siguientes componentes:

- **Estrategias de Infraestructura**
  - ✓ Activar los procedimientos de evaluación de daños en las instalaciones de la empresa.
  - ✓

- **Estrategias de RRHH**
  - ✓ Resguardar y asistir a los miembros de la organización.
  - ✓ Contactar a las agencias externas de apoyo convenientes.

- **Estrategias de Recursos**
  - ✓ En casi aplique, activar los procedimientos para la asistencia humanitaria de los miembros de la organización.

## 4 Equipo de Respuesta a Emergencias

Considera un conjunto de roles y funciones claramente establecidos y definidos, los cuales son los pilares para la definición de las estrategias del Plan de Respuesta a Emergencias. A continuación, se muestra la estructura del equipo:

| Posición/Rol | Prioridad | Crítico |
|---|---|---|
| *Posición o rol dentro del equipo* | *1= Alto*<br>*2=Medio*<br>*3=Bajo* | *¿Posición crítica/indispensable dentro del equipo?* |
| **Coordinador General de Emergencia** | 1 | Sí |
| • Coordinador de Seguridad y Salud Ocupacional | 1 | Sí |
| ○ Coordinador de Brigada Contra Incendios | 1 | Sí |
| ○ Coordinador de Brigada de Primeros Auxilios | 1 | Sí |
| ○ Coordinador de Evaluación y Control de Daños | 2 | Sí |
| ○ Coordinador de Brigada de Mantenimiento | 2 | Sí |
| • Coordinador de Brigada de Evacuación | 1 | Sí |

Figura 27. Estructura del equipo de respuesta a Emergencia

A continuación, se presenta la estructura organizacional del Equipo de Respuesta a Emergencias diseñada por el tesista para el caso específico de la empresa de seguros local:

Tesis publicada con autorización del autor
No olvide citar esta tesis

Figura 28. Organigrama del equipo

## 5 Funciones y Responsabilidades

Las funciones y responsabilidades asignadas a cada rol del Equipo de Emergencias se encuentran detalladas en el Anexo 20.

## 6 ANTES: Actividades de Prevención y Preparación

**Escenario: Sismo / Terremoto con posible ocurrencia de incendio**

| Rol | Nombre del Rol |
|---|---|
| R1 | Coordinador General de Emergencia (CGE) |
| R2 | Coordinador de Seguridad y Salud Ocupacional (SSO) |
| R3 | Coordinador de Brigada de Evacuación (CBE) |
| R4 | Coordinador de Brigada Contra Incendios (CBCI) |
| R5 | Coordinador de Brigada de Primeros Auxilios (CBPA) |
| R6 | Coordinador de Evaluación y Control de Daños (CECD) |
| R7 | Coordinador de Mantenimiento |

Figura 29. Leyenda por roles

Las responsabilidades y roles por tipo de escenario se encuentran especificadas en el Anexo 21.

Tesis publicada con autorización del autor
No olvide citar esta tesis

# 7 DURANTE: Actividades de Respuesta y Activación

## 7.1 Escenario 1: Sismo o Terremoto

| N° | Descripción de Tarea | Rol |
|---|---|---|
| 1. | Evaluar y decidir la ejecución del Plan de Respuesta a Emergencia | Coordinador General de la Emergencia |
| 2. | Alertar al personal con el objetivo de que se proteja en las zonas seguras debidamente señalizadas. En caso de que no pueda acceder a dichas zonas, colocarse debajo de los escritorios o mesas sólidas. | Brigadista de Emergencia de Evacuación |
| 3. | En coordinación con el Coordinador General de Emergencia, activar el sistema de alarma correspondiente al evento. | Coordinador de Evaluación y Control de Daños |
| 4. | Evaluar si es pertinente escalar el incidente al Comité de Crisis | Coordinador General de la Emergencia |
| 5. | Inspeccionar el edificio a fin de verificar si existen incendios, derrames de sustancia, escapes de gas u otra situación que ponga en peligro la vida de las personas. | Brigadista de Emergencia por local |
| 6. | Iniciar la evacuación y monitorear al personal, proveedores y/o clientes a fin de cultivar el orden y la calma. | Brigadista de Emergencia de Evacuación |
| 7. | Validar que todos hayan desalojado el local | Líder de Emergencia por local |
| 8. | Ubicar al personal evacuado en las áreas de reunión o círculos de seguridad. | Líder de Emergencia por local |
| 9. | Realizar el conteo del personal evacuado | Brigada de Emergencia por local de Evacuación |
| 10. | Coordinar el traslado de heridos a establecimiento especializados de salud | Coordinador de Brigada de Primeros Auxilios |
| 11. | Recibir la orden por parte del Coordinador de Brigada para ejecutar acciones de rescate y/o primeros auxilios. | Brigadista de primeros auxilios |
| 12. | Realizar una evaluación preliminar del impacto ocasionado por el evento a fin de evaluar activar al Comité de Crisis | Coordinador General de Emergencia |
| 13. | Coordinar el rescate de los siguientes:<br>– Materiales y Bienes: Los que podrían contribuir a | Coordinador General de Emergencia |

Tesis publicada con autorización del autor
No olvide citar esta tesis

| N° | Descripción de Tarea | Rol |
|---|---|---|
| | aumentar los riesgos de destrucción y los recursos que podrían ser útiles para Primeros Auxilios y, aquellos que por su costo y/o vulnerabilidad sea oportuno evacuar.<br>– Documentación: Documentos clasificados y/o valorados que son irremplazables o de difícil sustitución, que no se encuentran dentro de los recursos identificados como registros vitales o que no se disponga de copias en el sitio alterno. | |
| 14. | Informar al Coordinador General de Emergencia, el detalle de lo acontecido durante la evacuación. | Coordinador de Brigada de Evacuación |

Figura 30. Roles y responsabilidades de acción durante un sismo

## 8 Comunicación en caso de Emergencias

Se definirán 3 tipos de comunicaciones alternativas de acuerdo a la emergencia:

### 8.1 Comunicación inicial de la emergencia

El empleado que detecte una emergencia deberá comunicar de inmediato al Operador del Centro de Monitoreo (salvo en caso de sismos), quien a su vez comunicará al Coordinador de la Brigada pertinente según el tipo de emergencia, al Coordinador General de Emergencias (CGE) y demás miembros del Comité de Emergencias (CE), así como a las entidades de apoyo externo según corresponda. El comunicado debe contener la siguiente información:

- Nombre de empleado
- Área de trabajo.
- Datos generales de la emergencia (Tipo, ubicación y descripción breve de la misma).
- Número de personas heridas si las hubiera- así como las condiciones de salud en las que se encuentran.
- No colgar hasta haber dado toda la información requerida y mantenerse en línea hasta que el operador le brinde su conformidad.

Así mismo la persona que detecte la emergencia deberá de comunicarlo al Líder o Brigadista de emergencia más cercano, de modo que este pueda evaluar la situación y ejecutar las acciones pertinentes lo antes posible.

### 8.2 Comunicación a Clínicas y Hospitales (emergencia médica)

En caso se trate de una emergencia que requiera asistencia médica, el operador debe comunicarse con las Clínicas y Hospitales más cercanos y se realizará seguimiento a la situación ante cualquier eventualidad. Además el Centro de Monitoreo comunicará lo suscitado al Coordinador de Primeros Auxilios o algunos de sus brigadistas para que tomen las medidas correspondientes.

En caso no se reciba una respuesta efectiva de Centro de monitoreo y los brigadistas, la persona deberá contactar directamente con la clínica cercana.

### 8.3 Comunicación a entidades de Apoyo externo

El Centro de Monitoreo realiza la comunicación de la situación de emergencia a las siguientes entidades de apoyo externo, según corresponda:

- ✓ Cuerpo General de Bomberos Voluntarios del Perú (CGBVP).
- ✓ Policía Nacional del Perú (PNP).
- ✓ Instituto Nacional de Defensa Civil (INDECI), previa aprobación del Coordinador General de Emergencias.

En caso de que no se reciba respuesta del CC, la comunicación deberá ser directa del líder o brigadista de emergencia más cercano al que accede la persona que detecta la emergencia a la entidad de apoyo externo correspondiente. En caso de no encontrar al líder o brigadista de emergencia, la comunicación deberá ser directa de la persona que detecta la emergencia a la entidad de apoyo externo correspondiente, proporcionando la misma información al Operador del Centro de monitoreo.

## 9 Procedimientos Generales de Evacuación

La evacuación del personal estará guiada por los siguientes procedimientos:

- El Coordinador General de Emergencias (CGE) decidirá la necesidad de evacuación (total o parcial) del edificio.
- En coordinación con el CGE, el Operador del Centro de Monitoreo deberá tocar la sirena de evacuación y dar las indicaciones iniciales con ayuda de altavoces. Los brigadistas se colocarán los chalecos que los identifican y procederán orientar a los trabajadores durante la emergencia hacia las zonas de concentración o puntos de reunión.

Tesis publicada con autorización del autor
No olvide citar esta tesis

- Como medida de seguridad de la información, al sonar la sirena, todo el personal debe bloquear su equipo con las teclas *Control* + *Alt* + *Suprimir*, apagar su monitor y seguir las indicaciones de los brigadistas. No lleve consigo cosas de valor (como billetera, celulares u otros dispositivos) a menos que se encuentren a su alcance.
- No usar ascensores durante sismo, movilizarse por las escaleras de seguridad.
- Si el sismo ocurre cuando está dentro de un ascensor, mantenga la calma y espere que el evento pase. Una vez termine, presione el botón de alarma para que los brigadistas acudan en su ayuda.
- Alejarse de las ventanas, repisas, de cualquier utensilio o artefacto caliente y de objetos que pueden rodar o caer.
- Promover el desplazamiento del personal fuera de las instalaciones, guiándolos por las rutas de evacuación previamente establecidas.
- En caso de corte de fluido eléctrico, recuerde que se encenderán las luces de emergencia.
- Si el sismo ocurre cuando está en el estacionamiento, busque la salida a campo abierto más cercana, en caso no pueda salir del lugar ubíquese en las columnas hasta que el sismo termine.
- Evite hacer comentarios alarmistas u otras conversaciones mientras evacua para no generar más alarma.
- No transporte bultos y objetos pesados, pueden entorpecer la evacuación u originar accidentes.
- No se detenga a recoger objetos personales caídos. Si es posible, trate de patearlos a un costado de la ruta de evacuación.
- Si se cae durante la evacuación y se encuentra en una ruta de tránsito, ruede a un costado, levántese e incorpórese a la fila, si no puede levantarse, pida ayuda siempre a un costado de la fila.
- Si alguna persona cae, levántela y ayúdela. En caso de no poder hacerlo informar a los brigadistas a la brevedad.
- Al momento de bajar las escaleras el personal tendrá que hacerlo por el costado derecho y en el retorno también será por el costado derecho para poder tener despejado el costado izquierdo que será utilizado para que se desplacen los rescatistas.
- El Líder o Brigadista de Emergencia designado por piso procederá de la siguiente manera:

Tesis publicada con autorización del autor
No olvide citar esta tesis

- Una vez reunidos en la zona de seguridad, verificar que el personal que labora se encuentre a salvo, verificando los ausentes e informando al Coordinador de la Brigada de Evacuación, quien ordenará la búsqueda.
- Inspeccionar el edificio a fin de detectar: personas heridas, atrapadas o lesionadas y en coordinación con el Coordinador de Brigada de Primeros Auxilios, ayudar a que sean evacuadas.
- Verificar el estado de salud de las personas, determinando quienes necesitan asistencia médica para solicitar el apoyo externo.

## 10 Directorio de Servicios de Emergencia

Se elaboró un Directorio con los principales números de emergencia acorde a las necesidades y ubicación geográfica de la empresa (Ver Anexo 22).

## 11 Requisitos en el Sitio Alterno de Operación

| N° | Requisito |
|---|---|
| **Controles Generales** | |
| 1 | Detectores de Humo |
| 2 | Sensores de Temperatura |
| 3 | Extinguidores (Tipo A/B/C/D) |
| 4 | FM200 |
| 5 | Switch de corte de energía |
| 6 | Detector de aniego |
| 7 | Fuente de alimentación de energía externa |
| 8 | Aire acondicionado (requerimientos mínimos de BTU) |
| 9 | Falso piso / techo |
| 10 | Cableado debidamente etiquetado bajo el falso piso |
| 11 | Rack para servidores (con llave) |
| **Monitoreo de Seguridad física** | |
| 1 | Cámaras de vigilancia |
| 2 | Controles biométricos para el control de ingresos no autorizados. |
| **Controles de Contingencia** | |
| 1 | UPS |
| 2 | Grupo electrógeno |

Figura 31. Principales requistos

Tesis publicada con autorización del autor
No olvide citar esta tesis

# CAPÍTULOS 7 – PLAN DE RECUPERACIÓN ANTE DESASTRES

## 1 Introducción

En el presente capítulo se muestra el diseño realizado para la recuperación de las aplicaciones de TI en base al análisis de impacto de negocio y al análisis de riesgos realizados previamente.

## 2 Objetivo

Diseñar y establecer las políticas y procedimientos que permitan la reactivación del servicio dentro del tiempo objetivo de recuperación definido por el negocio para las principales aplicaciones de TI que brindan soporte a los procesos críticos de continuidad.

## 3 Alcance

Los servicios y/o aplicaciones de Sistemas TI involucrados en la recuperación son:

| Nombre del Servicio y/o Aplicación de TI | Descripción | Periodo de respaldo | RTO del Negocio |
|---|---|---|---|
| Sistema de vida | Sistema integral encargado de la gestión de los seguros. | No aplica | 24 horas |
| Sistema operativo contable | Sistema que genera las tramas de información en un formato adecuado para poder ser usado por el Sistema contable. | 24 horas (*) | 24 horas |
| Sistema contable | Sistema encargado de administrar los pagos, finanzas y cuentas bancarias. | 24 horas (*) | 24 horas |
| Sistema de cotización | Sistema encargado de transferir las cotizaciones ganadas automáticamente al sistema de producción. | 24 horas (*) | 24 horas |
| Sistema de producción | Genera la póliza y la pre-póliza. | 24 horas (*) | 24 horas |
| Sistema de atención al | Aplicativo web encargado de | 24 horas (*) | 24 horas |

Tesis publicada con autorización del autor
No olvide citar esta tesis

| Nombre del Servicio y/o Aplicación de TI | Descripción | Periodo de respaldo | RTO del Negocio |
|---|---|---|---|
| cliente | gestionar las consultas y reclamos hechas por los clientes. | | |
| Servidor de correos | Servidor que almacena todas las comunicaciones electrónicas de los miembros de la empresa. | 24 horas (*) | 24 horas |
| Servidor de aplicaciones | Servidor de clasificación "Confidencial" administrado por el área de TI que ejecuta las principales aplicaciones de la empresa. | 24 horas (*) | 24 horas |
| Servidor de base de datos | Servidor de clasificación "Restringida" administrado por el área de TI que almacena y organiza la información para ser usada por una serie de aplicaciones. | 24 horas (*) | 24 horas |

Figura 32. Resumen de servicios y/o aplicaciones involucrados en la recuperación

*(*) El tiempo es referencial ya que el respaldo se realiza cada vez que se alcanza una determinada cantidad de datos, la cual es fijada por el proveedor*.

## 4 Estrategias

Las estrategias planteadas fueron diseñadas a partir de distintas capacidades con las que cuenta la empresa tales como presupuesto, personal, estructura y cultura organizacional.

La recuperación de las aplicaciones y/o servicios de TI están en función a la infraestructura (instalaciones), infraestructura de TI (servidores), infraestructura de comunicaciones (enlaces), medios de transporte, personal alterno, medios de comunicación, soporte a usuarios, información (física o digital) y servicios de proveedores (Ver Anexo 23)

## 5 Equipos y Roles de Recuperación

A continuación, se describirán los principales equipos necesarios para la recuperación de los sistemas y aplicaciones de TI.

| Nombre | Descripción |
|---|---|
| Rol | Posición o rol perteneciente al grupo. |
| Prioridad | Importancia de las posiciones:<br>1: Primero en ejecutar, dirigiendo las acciones de recuperación.<br>2: Ejecuta las acciones y realiza coordinaciones según las decisiones tomadas por los líderes.<br>3: Brinda soporte en el desarrollo de las actividades. |

Figura 33. Leyenda

### 5.1 Equipo de Recuperación Principal de TI

Responsables de Recuperar los servicios y aplicaciones de Sistemas TI, lo cual comprende principalmente a las plataformas, base de datos, comunicaciones y accesos a los sistemas.

| Código | Rol | Prioridad |
|---|---|---|
| **CTI** | **Coordinador de Recuperación de TI** | 1 |
| CIL | • Coordinador de Infraestructura de Locales | 2 |
| CRB | • Coordinador de Redes y BD | 2 |
| CIR | • Coordinador de Información y Registros | 2 |
| CPO | • Coordinador de Personal Operativo | 3 |
| CAP | • Coordinador de Aplicaciones (Soporte de Equipo TIC) | 3 |

Figura 34. Miembros del Equipo de recuperación de TI

El líder de recuperación que es el Coordinador de Recuperación de TI y cada uno de los roles definidos en el plan, realizan actividades de coordinación con el personal de la empresa y los respectivos proveedores para la activación del DRP, lo cual permitirá recuperar los servicios y/o aplicaciones críticas del negocio. Cabe mencionar que el Coordinador de Recuperación de TI del plan actúa acorde a las instrucciones del Comité de Gestión de Crisis.

### 5.2 Habilidades por Rol

En el Anexo 24, se presentan los las funciones y habilidades que cada rol debe cumplir.

## 6 Fases de Recuperación

Las actividades de recuperación se realizarán en 3 fases:

### 6.1 FASE I: Antes

Es fase determina las actividades previas que se deben realizar, a fin de garantizar el éxito y la viabilidad de la ejecución del presente plan.

| Símbolo | Descripción |
|---|---|
| X | Rol encargado de gestionar la ejecución de la tarea o actividad ya sea personalmente o por medio de algún tipo de consultoría o auditoría. |
| ⊙ | Rol que, como parte del equipo recuperación de TI participa en el desarrollo de las actividades del plan. |

Figura 35. Leyenda

En el Anexo 25, se describen las principales actividades de prevención diseñadas para la recuperación de TI en la organización.

### 6.2 FASE II: Respuesta y de Operación Alterna

En esta fase, de plantean las principales actividades en respuesta al sismo para poder llevar a cabo la recuperación de los principales sistemas y aplicaciones de TI.

A continuación se describen las actividades ordenadas cronológicamente estimando la duración aproximada de las mismas:

Tesis publicada con autorización del autor
No olvide citar esta tesis

| N° | Descripción de la tarea | Duración estimada (HH:MM) |
|---|---|---|
| ***A.*** | ***Respuesta al sismo: Define las actividades necesarias para escalar el evento catalogado como "Alerta de Desastre" y luego de la evaluación correspondiente, decidir el plan de acción más idóneo en función a los recursos disponibles en ese momento.*** | |
| Estado de la Situación: Alerta de Desastre | | |
| 1. | El **Coordinador de Recuperación de TI** debe recibir la notificación de parte del Equipo de Gestión de Crisis sobre el estado actual del desastre. | No aplica |
| 2. | Notificar a los miembros del equipo sobre el estado actual. | 00:10 |
| 3. | El **Coordinador de Personal Operativo** debe evaluar el estado y cantidad de personal afectado. | 00:30 |
| 4. | El **Coordinador de Infraestructura de Locales** debe solicitar información al equipo de manejo de emergencias sobre el estado de la infraestructura del edificio principal para obtener un diagnóstico inicial. | 00:30 |
| Estado de la Situación: Desastre en evaluación | | |
| 5. | El **Coordinador de Infraestructura de Locales** debe recibir la información del equipo de manejo de emergencias y evaluar si la infraestructura ofrece las condiciones adecuadas para la recuperación garantizando la seguridad de las personas y los equipos. | 01:00 |
| 6. | El **Coordinador de Recuperación de TI,** en colaboración con **Coordinador de Infraestructura de Locales, Coordinador de Redes y BD, Coordinador de Información y Registros** y el **Coordinador de Personal Operativo** deben evaluar los RTOs y el vencimiento de los mismo a fin de solicitar la declaración de "Respuesta a Desastre" | 02:00 |
| 7. | Comunicar al Equipo de Gestión de Crisis sobre los resultados obtenidos informando las decisiones tomadas a partir de ello. | 00:30 |
| Estado de la Situación: Desastre evaluado | | |

Tesis publicada con autorización del autor
No olvide citar esta tesis

| N° | Descripción de la tarea | Duración estimada (HH:MM) |
|---|---|---|
| 8. | El **Coordinador de Recuperación de TI** debe recibir la conformidad del Equipo de Gestión de Crisis para dar inicio al plan de acción. | No Aplica |
| 9. | Determinar, en conjunto con el **Coordinador de Infraestructura de Locales** la necesidad o no de activar el centro alterno de operaciones. | 00:30 |
| 10. | Determinar, en conjunto con **el Coordinador de Redes y BD**, el estado de los sistemas o aplicaciones para determinar el funcionamiento del centro de datos alterno (ya que este se activa automáticamente frente a una interrupción). | 01:00 |
| 11. | El **Coordinador de Personal Operativo** deber notificar al personal titular y alterno disponible del plan, sobre situación actual, con todos los datos coordinados con el resto del equipo y aprobados previamente con el Equipo de Gestión de Crisis, a fin de que se preparen para una eventual movilización al centro alterno de operaciones. | 03:00 |
| 12. | El **Coordinador de Recuperación de TI** y el **Coordinador de Infraestructura de Locales** deben realizar la validación de las condiciones del centro alterno de operaciones. | 03:00 |
| 13. | Comunicar al Equipo de Gestión de Crisis sobre el estado actual de los planes de acción tomados. | 00:30 |
| ***B.*** | ***Plan de Acción: Define las actividades a ser efectuadas luego de evaluar el desastre y proceder a la activación del ambiente alterno en caso sea necesario.*** | |
| Estado de la Situación: En Atención | | |
| 14. | El **Coordinador de Recuperación de TI** debe recibir notificación de parte del Equipo de Gestión de Crisis sobre el estado actual de “Desastre Declarado” | No Aplica |

Tesis publicada con autorización del autor
No olvide citar esta tesis

| N° | Descripción de la tarea | Duración estimada (HH:MM) |
|---|---|---|
| 15. | El **Coordinador de Recuperación de TI** y el **Coordinador de Redes y BD** deberán notificar al proveedor del centro de cómputo alterno la activación del plan para que tomen las medidas y consideraciones necesarias. | 00:30 |
| 16. | El **Coordinador de Infraestructura de Locales** debe coordinar con el proveedor respectivo la provisión de unidades de transporte para la movilización del personal necesario. | 01:00 |
| 17. | El **Coordinador de Información y Registros** debe coordinar con el proveedor correspondiente el traslado, en caso sea necesario, de la información física custodiada. Además deberá notificar el cambio de ubicación de operaciones para el almacenamiento de la información generada durante la operación en contingencia. | 01:00 |
| 18. | El **Coordinador de Personal Operativo** debe notificar al personal titular y alterno del plan, sobre situación actual y comunicarles el punto de reunión para iniciar el traslado. | 04:00 |
| 19. | Según llegue el personal:<br>✓ Asignar colaborador al rol correspondiente.<br>✓ Entregar parte del plan que le corresponde (desmembrar el plan impreso en caso sea necesario).<br>✓ En caso de llegar más de un colaborador para el mismo rol, asignar a otros roles hasta completar los puestos de recuperación. | 04:30 |
| 20. | El **Coordinador de Redes y BD** y el **Coordinador de Aplicaciones** (Soporte de Equipo TIC) deben trasladarse al centro alterno de operaciones para:<br>✓ Preparar los equipos con las aplicaciones y sistemas necesarios.<br>✓ Brindar los accesos correspondientes.<br>✓ Verificar la correcta ejecución de las pruebas iniciales de los equipos en sitio alterno (servidores, tape librerías, discos, SAN storage). | 03:30 |

Tesis publicada con autorización del autor
No olvide citar esta tesis

| N° | Descripción de la tarea | Duración estimada (HH:MM) |
|---|---|---|
| 21. | Una vez que el personal haya llegado al centro alterno de operaciones, el **Coordinador de Recuperación de TI** debe solicitar al personal lo siguiente:<br>✓ Verificar validez de los equipos y materiales de operación<br>✓ Verificar validez de los sistemas de tecnología (acceso y datos).<br>✓ Verificar la existencia de la información física necesaria.<br><br>El **Coordinador de Aplicaciones (Soporte de Equipo TIC)** debe monitorear y atender la ocurrencia de posibles incidentes de TI que pudieran ocurrir durante la estabilización y operación en contingencia. | 06:30 |
| 22. | Comunicar al Equipo de Gestión de Crisis:<br>✓ Resultados de pruebas iniciales.<br>✓ Solicitar indicaciones de qué hacer con el personal sobrante.<br>✓ Solicitar recursos y materiales adicionales en caso sea necesario. | 03:00 |
| 23. | El **Coordinador de Recuperación de TI** debe, según indicaciones del Equipo de Gestión de Crisis coordinar la logística para la adquisición de los recursos adicionales | 16:00 |
| ***C.*** | ***Operación Alterna: Define las actividades de coordinación a ser efectuadas para reanudar la operación diaria.*** | |
| Estado de la Situación: Desastre atendido | | |
| 24. | El **Coordinador de Recuperación de TI**, en colaboración con el **Coordinador de Redes y BD** y el **Coordinador de Aplicaciones** debe monitorear la recuperación de procesos y actividades afectadas. | 12:00 |
| 25. | El **Coordinador de Recuperación de TI** debe solicitar información sobre el estado de la recuperación de las instalaciones principales de la empresa para determinar en qué momento iniciar las actividades de normalización. | 12:00 |

Tesis publicada con autorización del autor
No olvide citar esta tesis

| N° | Descripción de la tarea | Duración estimada (HH:MM) |
|---|---|---|
| 26. | El **Coordinador de Redes y BD** y el **Coordinador de Aplicaciones** deben gestionar y realizar revisiones en el edificio de la empresa para asegurar que la infraestructura de red y comunicaciones sea la adecuada. | 12:00 |
| 27. | Informar situación de avance al Equipo de Gestión de Crisis. | 15:00 |
| 28. | El **Coordinador de Recuperación de TI** debe informar al Equipo de Gestión de Crisis la recuperación de las aplicaciones y/o servicios de TI cuando alcancen un estado aceptable. | 24:00 |

Figura 35. Actividades de Respuesta y Operación Alterna

### 6.3 FASE III: Actividades de Restauración y Retorno

A continuación, se presentan las principales actividades a seguir una vez el Equipo de Gestión de Crisis ha desactivado la alerta de desastre debido a que las operaciones y las instalaciones ya se encuentran dentro de un nivel óptimo.

A continuación se describen las actividades ordenadas cronológicamente estimando la duración aproximada de las mismas:

| N° | Descripción de la tarea | Duración estimada (HH:MM) |
|---|---|---|
| ***A.*** | ***REPARACIÓN: Define las actividades a ser efectuadas para realizar la reparación de los daños ocurridos al ambiente NORMAL y la preparación para dejar "a punto" el retorno a la normalidad*** | |
| Estado de la Situación: Desastre Controlado | | |
| 1. | El **Coordinador de Recuperación de TI** debe recibir la notificación de parte del Equipo de Gestión de Crisis informando que el Desastre ha sido controlado. | No aplica |
| 2. | El **Coordinador de Recuperación de TI** debe coordinar con el Equipo de Gestión de Crisis el esquema o plan de reparación del centro de cómputo dañado | 48:00 |

Tesis publicada con autorización del autor
No olvide citar esta tesis

| N° | Descripción de la tarea | Duración estimada (HH:MM) |
|---|---|---|
| 3. | El **Coordinador de Recuperación de TI**, con coordinación con el resto del equipo, debe planificar la fecha de retorno considerando los recursos y la situación actual | 120:00 |
| 4. | Preparar plan de acción para retorno y asignar responsabilidades. Se debe considerar lo siguiente:<br>✓ El **Coordinador de Redes y BD** debe verificar que las conexiones del edificio de la empresa se encuentren adecuadamente instaladas y permitan condicionar los ambientes.<br>✓ El **Coordinador de Información y Registros** debe verificar y coordinar el traslado de la información necesaria al edificio y al proveedor.<br>✓ El **Coordinador de Infraestructura de Locales** debe verificar que las instalaciones del edificio de la empresa se encuentren en óptimas condiciones garantizando la seguridad de las personas y de los activos. | 36:00 |
| 5. | Cada coordinador deber tomar puntos de control para la posterior verificación en el edificio de la empresa (centro normal de operaciones). | 24:00 |
| ***B.*** | ***Operación normal: Define las actividades a ser efectuadas para realizar el retorno a la normalidad, lo que implica desactivar el centro alterno y activar la operación normal*** | |
| Estado de la Situación: Fin del Desastre | | |
| 6. | El **Coordinador de Infraestructura de Locales** con la aprobación del resto del equipo, solicita desactivar el centro alterno de operaciones. | 24:00 |
| 7. | El equipo debe dirigir cada una de las actividades de retorno, cumpliendo las responsabilidades asignadas. | 48:00 |
| 8. | El **Coordinador de Recuperación de TI** debe informar al Equipo de Gestión de Crisis el fin del proceso y esperar la notificación de “Fin de desastre”. | 01:00 |

Tesis publicada con autorización del autor
No olvide citar esta tesis

| N° | Descripción de la tarea | Duración estimada (HH:MM) |
|---|---|---|
| 9. | El **Coordinador de Recuperación de TI** debe coordinar reuniones posteriores con el Equipo de Gestión de Crisis para realizar el análisis de Lecciones Aprendidas. | 02:00 |
| 10. | El equipo debe actualizar los Planes de Continuidad y documentación de soporte. | 72:00 |

Figura 36. Actividades de Restauración y Retorno

Tesis publicada con autorización del autor
No olvide citar esta tesis

# CAPÍTULOS 8 – PLAN DE CONTINUIDAD DE NEGOCIO

## 1 Introducción

En el presente capítulo se desarrolla el Plan de Continuidad de Negocios en caso de ocurrencia de sismos. En este acápite, se tomará como referencia los principales planes elaborados anteriormente para articularlos bajo una única dirección.

## 2 Objetivo

Diseñar un plan que prepare a la empresa en caso de cortes totales o parciales de servicio, articulando una serie de planes previamente definidos y permitiéndole una recuperación dentro de los plazos acordados según las necesidades y requerimientos del negocio.

## 3 Alcance

El alcance del presente plan está limitado a la ocurrencia de sismos, abarcando la recuperación de los procesos o servicios críticos para la continuidad del negocio. Cabe resaltar que este plan no es una guía de solución de incidentes diarios.

## 4 Objetivos específicos

Los principales objetivos específicos del plan son:

- Servir de guía para los diferentes equipos de recuperación de la empresa.
- Brindar procedimientos y recursos necesarios para asistir en la recuperación.
- Evitar confusiones durante la ocurrencia del desastre documentando los procedimientos a seguir.
- Evidenciar la relación y el intercambio constante entre los diferentes equipos de recuperación.

La recuperación de las aplicaciones y/o servicios de TI están en función a la disponibilidad de los componentes mencionados a continuación:

## 5 Equipos de Recuperación

Los principales equipos que dirigen y orientan al resto del personal en la ejecución del plan son:

- Equipo de Recuperación de TI.
- Equipo de Respuesta ante emergencias.
- Equipo de Gestión de Crisis.
- Equipo de comunicaciones.
- Equipo de asistencia humanitaria.

# 6 Instrucciones para el uso del plan

## 6.1 Invocar el plan

Este plan se hace efectivo frente a la ocurrencia de un sismo. Los procedimientos normales de gestión de incidentes activarán el plan, poniendo en contacto a todos los miembros de los diferentes equipos de recuperación, permaneciendo vigente hasta que las operaciones se reanuden en la ubicación original de manera normal.

## 6.2 Declarar el Desastre

Los equipos de Manejo de Emergencias e incidentes de TI, bajo la asesoría del equipo de Continuidad de Negocios, notificarán al Equipo de Gestión de Crisis la ocurrencia del desastre tomando en cuenta los criterios de escalamiento definidos en el Plan de Manejo de Crisis.

## 6.3 Notificar

El Equipo de Gestión de Crisis, conforme a lo establecido en el Plan de Manejo de Crisis, deberá iniciar una sesión para determinar si activar o no las medidas de contingencia tomando en cuenta las indicaciones de análisis y evaluación.

Por otro lado, el Equipo de Manejo de emergencias y el de Recuperación de TI deberán realizar un diagnóstico inicial para informar al equipo de Gestión de Crisis el impacto en los principales recursos.

## 6.4 Comunicar a medios de comunicación

El equipo de Gestión de Crisis, bajo la asesoría del equipo de Comunicaciones y el de Continuidad de Negocio, son los designados para ser el contacto con los medios de comunicación, reguladores, Gobierno y alguna otra comunicación que se requiera.

Tesis publicada con autorización del autor
No olvide citar esta tesis

## 6.5 Uso de planes

A continuación, se mostrará la interacción de los diferentes planes desarrollados a lo largo de las diferentes fases en la ocurrencia de un sismo tomando en cuenta los siguientes planes desarrollados:

| Código | Descripción |
|---|---|
| PMC | Plan de Manejo de Crisis |
| PRE | Plan de Respuesta a Emergencias |
| PRD | Plan de Recuperación de Desastres |

Figura 37. Planes incluidos en le BCP

### *6.5.1 Fase I: Prevención*

Esta fase se desarrolla a lo largo de las operaciones diarias, manteniendo a la empresa preparada y sentando las bases de una cultura organizacional sólida.

| Componente o Recurso cubierto | Descripción | Planes utilizados | | |
|---|---|---|---|---|
| | | PM | PR | PR |
| **Personas** | El **Equipo de Respuesta a Emergencias** programa los simulacros, capacitaciones y revisiones periódicas de modo que le personal conozca y difunda el plan.<br><br>El **Equipo de Recuperación de TI** mantiene actualizada la relación de personal necesario y lo capacita para estar preparado ante a una posible operación en contingencia. | | X | X |
| **Infraestructura de local de operaciones y centro de datos** | El **Equipo de Respuesta a Emergencias** se encarga de proveer al edificio de una adecuada señalización para facilitar la evacuación en caso de emergencia<br><br>El **Equipo de Recuperación de TI** realiza pruebas periódicas a los centros principales | | X | X |

| Componente o Recurso cubierto | Descripción | Planes utilizados | | |
|---|---|---|---|---|
| | | PM | PR | PR |
| | y alternos con los proveedores respectivos además de realizar los mantenimientos correspondientes para asegurar la disponibilidad y nivel de servicio esperado durante la operación en contingencia. | | | |
| **Información** | El **Equipo de Recuperación de TI** realiza las pruebas necesarias con el proveedor para asegurar que el traslado de la información física al centro al alterno de operaciones sea oportuno y seguro. Además, los especialistas en redes y base de datos aseguran la integridad, seguridad y confidencialidad de la información mediante revisiones periódicas al proveedor. | | | X |
| **Equipos (laptops, celulares, anexos, entre otros)** | El **Equipo de Recuperación de TI** verifica y asegura el dimensionamiento adecuado para equipar el centro de operaciones alterno. | | | X |

Figura 38. Actividades de la Fase I - Prevención

### *6.5.2 Fase II: Ocurrencia de sismo*

Esta fase abarca la ejecución de los planes durante la ocurrencia de un sismo, manteniendo como prioridad las acciones orientadas al cuidado de las personas.

| Componente o Recurso cubierto | Descripción | Planes utilizados | | |
|---|---|---|---|---|
| | | PM | PR | PR |
| **Personas** | El **Equipo de Respuesta a Emergencias** activa el plan, evacuando a las personas según las indicaciones y activando las alarmas correspondientes. Este equipo es | | X | |

| Componente o Recurso cubierto | Descripción | Planes utilizados | | |
|---|---|---|---|---|
| | | PM | PR | PR |
| | vital en esta etapa ya que serán los principales guías en la ejecución de las buenas prácticas establecidas en el plan. | | | |

Figura 39. Actividades de la Fase II – Ocurrencia de Sismo

### *6.5.3 Fase III: Evaluación Inicial*

Esta fase determina la interacción de los planes instantes después de la ocurrencia del sismo, realizado verificaciones iniciales y diagnósticos que brindarán información valiosa para la toma de decisiones estratégicas.

| Componente o Recurso cubierto | Descripción | Planes utilizados | | |
|---|---|---|---|---|
| | | PM | PR | PR |
| **Personas** | El **Equipo de Respuesta a Emergencias** atiende a los heridos en caso sea necesario y se comunica con las entidades externas pertinentes según lo indicando en el plan.<br><br>El **Equipo de Gestión de Crisis** es notificado, convocándose a una reunión y, según agenda, disponen las indicaciones convenientes al **Equipo de Asistencia Humanitaria.** | X | X | |
| **Infraestructura de local de operaciones y centro de datos** | El **Equipo de Respuesta a Emergencias** realiza las revisiones a la infraestructura del edificio para realizar el diagnóstico inicial.<br><br>El **Equipo de Recuperación de TI** realiza las revisiones necesarias a la infraestructura del centro de datos principal para realizar el diagnóstico inicial. | | X | X |
| **Información** | El **Equipo de Recuperación de TI** realiza | | | X |

| Componente o Recurso cubierto | Descripción | Planes utilizados | | |
|---|---|---|---|---|
| | | PM | PR | PR |
| | un revisión del estado de la información física y digital para realizar un diagnóstico inicial | | | |
| **Equipos (laptops, celulares, anexos, entre otros)** | El **Equipo de Recuperación de TI** realiza una revisión del estado de los equipos para un diagnóstico inicial y tener un aproximado de los recursos necesarios para la recuperación | | | X |

Figura 40. Actividades de la Fase III – Evaluación Inicial

### *6.5.4 Fase IV: Activación de Planes de Contingencia*

Para el desarrollo de esta fase es importante resaltar el papel del **Equipo de Gestión de Crisis** como orquestador de todas las decisiones a tomarse, aprobando medidas y monitoreando constantemente el impacto actual de la situación en el negocio.

| Componente o Recurso cubierto | Descripción | Planes utilizados | | |
|---|---|---|---|---|
| | | PM | PR | PR |
| **Personas** | El **Equipo de Recuperación de TI**, según lo dispuesto en el plan, convoca y moviliza al personal alterno y/o titular necesario para retomar las operaciones en contingencia.<br><br>El **Equipo de Respuesta a Emergencias** debe seguir alerta debido a la probabilidad de ocurrencia de réplicas, en cuyo se procederá a activar nuevamente dicho plan. | X | X | X |
| **Infraestructura de local de operaciones y** | El **Equipo de Recuperación de TI** activará los centros alternos e iniciará las configuraciones e instalaciones respectivas | X | | X |

| Componente o Recurso cubierto | Descripción | Planes utilizados | | |
|---|---|---|---|---|
| | | PM | PR | PR |
| **centro de datos** | según el plan | | | |
| **Información** | El **Equipo de Recuperación de TI** gestiona las coordinaciones necesarias con el proveedor para obtener la información necesaria para la ejecución de sus procesos. | X | | |
| **Equipos (laptops, celulares, anexos, entre otros)** | El **Equipo de Recuperación de TI** se encarga del uso y manejo adecuado de los recursos asignados, brindando soporte cuando sea necesario según los roles definidos en el plan. | X | | X |

Figura 41. Actividades de la Fase IV – Activación de Planes de Contingencia

Además, cabe mencionar que paralela a estas actividades, y según lo estipulado en el **Plan de Manejo de Crisis**, el Equipo de Comunicación en Crisis protegerá la reputación de la empresa frente a los diferentes medios de comunicación, manteniendo informados a los interesados y dando los anuncios necesarios.

## 6.6 Monitoreo

Una vez activados los planes de contingencia, se realizarán revisiones constantes del estado del proceso de recuperación y de la estabilidad de los procesos para que, cuando sea conveniente, se proceda a desactivar los planes o de lo contrario, se elaboren nuevas estrategias y planes de acción.

Esta retroalimentación será centralizada a través del Equipo de Gestión de Crisis, quienes bajo la asesoría del Equipo de Continuidad de Negocios serán los encargados de tomar las decisiones y de la mano con los equipos de apoyo, plantear las mejores soluciones para asegurar la continuidad operativa del negocio.

En la siguiente figura, se muestra el diseño realizado por el tesista para el flujo de información que se da a lo largo del proceso mencionado:

Tesis publicada con autorización del autor
No olvide citar esta tesis

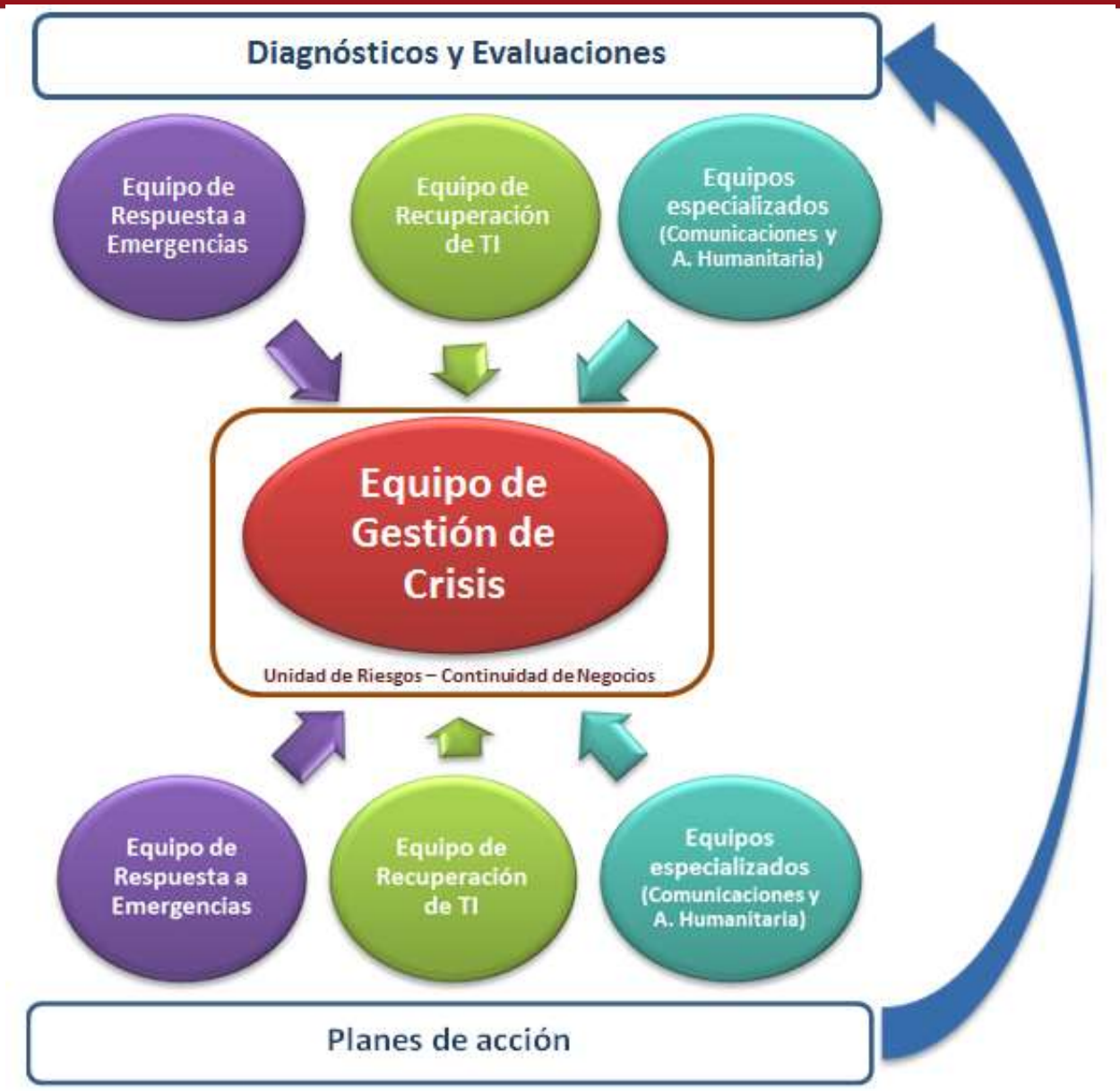


Figura 42. Flujo del proceso de monitoreo de actividades

# CAPÍTULOS 9 – PLAN DE PRUEBAS

## 1 Introducción

En el presente capítulo se muestra el manejo de pruebas y el mantenimiento de los planes de continuidad elaborados. Además, se describen los procedimientos para llevar a cabo cada una de las pruebas así como las consideraciones para evaluar los resultados obtenidos.

## 2 Objetivo

Diseñar y establecer los diferentes tipos de prueba que, acorde a las necesidades y dimensiones del SGCN, permitan validar el diseño y las estrategias definidas en cada plan identificando así oportunidades de mejora además de mantener el plan actualizado.

## 3 Consideraciones

Para la elaboración del diseño del presente plan de pruebas se consideraron los siguientes componentes:

| Componente | Aporte en el diseño |
|---|---|
| Análisis de Impacto de Negocio. | ✓ Proporciona información de los recursos involucrados, detallando su criticidad y el nivel de riesgo al que están expuestos.<br>✓ Permite identificar los posibles escenarios de riesgo a los que están expuestos los procesos, brindando un aporte importante en la elaboración de los escenarios de crisis. |
| Análisis de Riesgos | |
| Plan de Manejo de Crisis | ✓ Permite identificar a las personas a ser incluidas en las pruebas así como las decisiones que cada uno debe tomar.<br>✓ Permite tener una línea base de referencia para evaluar los resultados de las reacciones durante las pruebas comparando lo real con lo esperado. |
| Plan de Recuperación de Desastres | |
| Plan de Respuesta ante Emergencias | |

Figura 43. Aportes de componentes del plan en el diseño de las pruebas

# 4 Pruebas y actualización

Acorde a la Circular de Gestión de Continuidad de Negocio de la SBS vigente, los planes de continuidad de negocio deben ser probados por lo menos una vez al año incluyendo las siguientes actividades (SBS, 2009).

## 4.1 Ejecución de pruebas

En este punto, se determinaron 2 tipos de pruebas consistentes con el alcance de los planes de continuidad de negocio:

### *4.1.1 Tabletop*

Método en el que, dado un determinado escenario, se reúne a los involucrados en la toma de decisiones, es decir a la Alta Dirección, quienes revisan la situación planteada y discuten las decisiones tomarían sin llegar a ejecutarlas (DRJ, 2013). Normalmente, este ejercicio se realiza bajo la dirección de un facilitador, quien guía a los involucrados en el desarrollo de las diferentes actividades.

### *4.1.2 Pruebas de Escritorio Operativas*

Este tipo de pruebas permite verificar la capacidad de respuesta los responsables frente a un escenario de desastre y principalmente verificar que los tiempos de recuperación se cumplan dentro de los límites establecidos en el Análisis de Impacto de Negocio. Por ende, la actividad central de este ejercicio será activar los centros alternos de datos y de operaciones en coordinación con los proveedores involucrados.

El detalle de las pruebas se encuentra en el Anexo 26.

## 4.2 Actualización de los planes

La actualización se los planes se dará como consecuencia de las siguientes situaciones:

- Identificación de oportunidades de mejora como resultado de la ejecución de pruebas.
- Cambios internos o externos que impacten a la empresa.
- Independientemente de lo mencionado, los planes deberán ser revisados por lo menos una vez al año por los especialistas.

Tesis publicada con autorización del autor
No olvide citar esta tesis

# CAPÍTULOS 10 – CONCLUSIONES, OBERVACIONES, RECOMENDACIONES Y TRABAJOS FUTUROS

## 1 Conclusiones

- Respecto a la metodología para la identificación de procesos críticos de continuidad, se identificó que es importante que las prioridades del negocio estén claramente establecidas y sean aceptadas por todas las gerencias de la empresa, ya que de este modo se asegura la conformidad de la evaluación de la criticidad aplicada a todos los procesos.

- Los resultados obtenidos producto de la evaluación fueron la base primordial para el inicio del análisis y diseño del SGCN, ya que estos definen qué procesos serán cubiertos en la elaboración de los planes acotando su alcance, siendo este un factor determinante para el éxito del proyecto de fin de carrera.

- Respecto al modelado de procesos, se identificó el rol del especialista o dueño del proceso es importante para brindar información relevante y detallada durante el relevamiento de información. Asimismo, valida los resultados obtenidos por proceso, de modo que la información brindada se refleje en el modelado de forma coherente y clara.

- Para el Análisis de Impacto de Negocio fue determinante contar con información detallada sobre los recursos involucrados; además, otro factor importante es la correcta determinación de los indicadores de continuidad, tales como el MTPD, RTO y RPO. Esto en conjunto determinó las estrategias de continuidad adecuadas a la empresa y sus necesidades.

- Respecto al Análisis de Riesgos, se puede concluir que, los procesos de la empresa aseguradora compartían recursos en común y por ende muchos riesgos son transversales a la organización, sin embargo, es importante realizar una evaluación independiente por proceso ya que la criticidad y el porcentaje de interrupción que puede generar en cada uno podría ser diferente, siendo esto un factor determinante para la definición de controles.

- El Plan Manejo de Crisis y el Plan de Respuesta a Emergencias lograron establecer una estructura de gestión escalable, que define las

responsabilidades y roles de cada equipo en las diversas etapas del manejo de la crisis y/o emergencia según criterios previamente establecidos. Además refuerza la importancia y el protagonismo del Equipo de Continuidad de Negocios como guías y gestores transversales a nivel operativo, táctico y estratégico.

- El Plan de Recuperación de Desastres logró identificar las aplicaciones críticas para la reanudación de los principales servicios, estableciendo roles y procedimientos prácticos de aplicación directa que permitan a los responsables poder entenderlos y llevarlos a cabo bajo situaciones de alta tensión.

- El Plan de Continuidad de Negocios consolidó cada uno de los planes previamente desarrollados, identificando claramente la interacción entre ellos. Esto brinda a la empresa una guía de gestión y manejo que les permita determinar qué planes deben ser activados y cuál es la relación entre los principales equipos.

- Respecto al Plan de Pruebas, este logró definir y especificar detalladamente dos tipos importantes abarcando la parte estratégica y operativa.

- En general, a lo largo del desarrollo del proyecto, se identificó la importancia de contar con el apoyo de la Alta Dirección y de los especialistas del negocio para garantizar el éxito del proyecto de fin de carrera. Finalmente, es importante mencionar que el presente diseño del SCGN es de utilidad para la empresa aseguradora no sólo porque le permite cumplir con requerimientos regulatorios, sino porque provee un valor agregado que brinda la pauta inicial para futuros proyectos que fortalezcan la gestión de la continuidad en la empresa.

## 2 Observaciones

- El presente proyecto de fin de carrera está basado en los lineamientos de la norma ISO/IEC 22301:2012; sin embargo para la realización de la misma también se empleó algunas buenas prácticas del BCI, las cuales se encuentran estrechamente ligadas a la norma base de continuidad de negocios mencionada.

- Cada uno de resultados obtenidos con aplicables únicamente a la empresa aseguradora en mención, ya que cada entidad tiene necesidades, recursos y prioridades diferentes así operen dentro del mismo rubro.

- La ejecución de las pruebas no fue realizada por cuestiones de tiempo y coordinaciones con la empresa, sin embargo, en respuesta a ello se definieron las pruebas lo más detalladas posible, de modo que las pruebas puedan ser ejecutadas posteriormente sin mayor inconveniente.

## 3 Recomendaciones

- Se recomienda documentar y actualizar el modelado de procesos cada vez que ocurran cambios en cuanto a la estructura, recursos o criticidad de los mismos. Asimismo la metodología para la identificación de los procesos críticos se debe aplicar por lo menos una vez al año, cuando los procesos sufran cambios, cuando se agregue y/o eliminen procesos o servicios.

- Cada vez que se identifique un cambio en los procesos o en la estructura de la empresa se reevaluará lo siguiente:

    - El Análisis de Impacto de Negocio, ya que es posible que los recursos, su nivel de interrupción asociado y los indicadores de continuidad puedan variar afectado a la definición de las estrategias de continuidad.
    - El Análisis de Riesgos, debido a que los cambios en los procesos pueden implicar la aparición de nuevos riesgos o la variación en el impacto y probabilidad de ocurrencia.
    - El Plan de Manejo de Crisis y el Plan de Respuesta a Emergencias, principalmente se verán afectados por cambios organizacionales, por lo que es conveniente revisar si la estructura de los equipos, así como los integrantes, siguen siendo válidos o continúan disponibles.
    - El Plan de Recuperación de Crisis, debido a que al existir cambios en los procesos, Análisis de Impacto y Análisis de Riesgos, las prioridades de recuperación podrían cambiar, requiriendo revisar los procedimientos.
    - Por ende, al cambiar alguno de los planes, también es recomendable revisar el Plan de Continuidad de Negocios, asegurando de este modo que estén alineados a las necesidades del negocio.

Tesis publicada con autorización del autor
No olvide citar esta tesis

- Se debe tomar en cuenta la revisión de la carga de algunos roles operativos en la empresa, ya que esto puede generar mucha dependencia y cuellos de botella en la ejecución de los procesos.

- Se recomienda que, como parte de una adecuada gestión de continuidad de negocio, se establezcan políticas y procedimientos que permitan evaluar a los proveedores críticos de la empresa en cuanto a la existencia y calidad de un SGCN. Dichas políticas deberán ser formalizadas en la organización para asegurar la disponibilidad de los recursos y servicios tercerizados en caso de un sismo (o algún otro escenario).

- En cuanto a la selección de un centro alterno de operaciones, se recomienda optar por una opción que se encuentre fuera de Lima para asegurar la disponibilidad de la infraestructura así como la seguridad de los empleados.

- Finalmente, se recomienda que, en la etapa de implementación se realice un análisis exhaustivo de los servicios o recursos que podrían ser tercerizados, ya que acorde a la estructura actual de la Unidad de Riesgos, la carga laboral podría originar cuellos de botella ocasionando retrasos e insatisfacción por parte de la Alta Dirección.

## 4 Trabajos Futuros

El presente proyecto de fin de carrera, ofrece una serie de oportunidades para posibles trabajos futuros, entre los que se encuentra:

- Ampliación de escenarios para el SGCN, como por ejemplo otros desastres naturales, incendios manifestaciones o huelgas.

- Cobertura de procesos, es decir, ampliar el alcance de los mismos, tomando en cuenta aquellos con calificación “Media” o “Baja”, permitiendo incluir a toda la empresa en el SGCN.

- Tomar el presente proyecto como base para proceder a la implementación del mismo con apoyo de especialistas y del uso adecuado y pertinente de tecnología de información.

Tesis publicada con autorización del autor
No olvide citar esta tesis

- Desarrollo e implementación de una metodología de gestión de incidentes, ya que con las estrategias planteadas a lo largo del presente análisis y acorde al Plan de Manejo de Crisis, queda abierta la posibilidad de definir políticas y procedimientos para la gestión de eventos de TI, que suelen suceder de manera diaria sin llegar a ser una crisis.

Tesis publicada con autorización del autor
No olvide citar esta tesis

**Referencias bibliográficas**


[1] Instituto Nacional de Defensa Civil (INDECI)
2007 *"Emergencias y daños personales a nivel nacional según fenómeno año 2006"*. Estadística de emergencias. Consulta: 09 de Setiembre del 2012. <http://www.indeci.gob.pe/estadisticas/res_2006/res_2006_b.pdf>

[2] *"Emergencias y daños personales a nivel nacional según fenómeno año 2007".*
2008 Estadística de emergencias. Consulta: 09 de Setiembre del 2012. <http://www.indeci.gob.pe/estadisticas/2007/1er_tri_b.pdf>

[3] *"Emergencias y daños personales a nivel nacional según fenómeno año 2008".*
2009 Estadística de emergencias. Consulta: 09 de Setiembre del 2012. <http://www.indeci.gob.pe/estadisticas/2008/1er_tri_b.pdf>

[4] *"Emergencias y daños personales a nivel nacional según fenómeno año 2009".*
2010 Estadística de emergencias. Consulta: 09 de Setiembre del 2012. <http://www.indeci.gob.pe/estadisticas/2009/2_eme_dan_seg_fen.pdf>

[5] *"Emergencias y daños personales a nivel nacional según fenómeno año 2010".*
2011 Estadística de emergencias. Consulta: 09 de Setiembre del 2012. <http://www.indeci.gob.pe/objetos/secciones/MTM=/NTM=/lista/NTY5/201106161210221.pdf>

[6] *"Emergencias y daños personales a nivel nacional según fenómeno año 2011".*
2012 Estadística de emergencias. Consulta: 09 de Setiembre del 2012. <http://www.indeci.gob.pe/objetos/secciones/MTM=/NTM=/lista/NjUx/201203051717581.pdf>

[7] *"Emergencias a Nivel Nacional por Departamento y según tipo de fenómeno ocurrido año 2006".*
2007 Estadística de emergencias. Consulta: 09 de Setiembre del 2012. <http://www.indeci.gob.pe/estadisticas/res_2006/res_2006_a.pdf>

[8] *"Emergencias a Nivel Nacional por Departamento y según tipo de fenómeno ocurrido año 2007".*
2008 Estadística de emergencias. Consulta: 09 de Setiembre del 2012.

<http://www.indeci.gob.pe/estadisticas/2007/1er_tri_a.pdf> *

[9] *"Emergencias a Nivel Nacional por Departamento y según tipo de fenómeno ocurrido año 2008".*
2009 Estadística de emergencias. Consulta: 09 de Setiembre del 2012.
<http://www.indeci.gob.pe/estadisticas/2008/1er_tri_a.pdf >

[10] *"Emergencias a Nivel Nacional por Departamento y según tipo de fenómeno ocurrido año 2009".*
2010 Estadística de emergencias. Consulta: 09 de Setiembre del 2012.
< http://www.indeci.gob.pe/estadisticas/2009/1_eme_reg_fen.pdf >

[11] *"Emergencias a Nivel Nacional por Departamento y según tipo de fenómeno ocurrido año 2010".*
2011 Estadística de emergencias. Consulta: 09 de Setiembre del 2012.
<http://www.indeci.gob.pe/objetos/secciones/MTM=/NTM=/lista/NTY5/201106161210021.pdf >

[12] *"Emergencias a Nivel Nacional por Departamento y según tipo de fenómeno ocurrido año 2011".*
2012 Estadística de emergencias. Consulta: 09 de Setiembre del 2012.
<http://www.indeci.gob.pe/objetos/secciones/MTM=/NTM=/lista/NjUx/201203051717461.pdf >

[13] SUPERINTENDENCIA DE BANCA Y SEGUROS
2009 Circular N° G – 139 – 2009. 02 de Abril.

[14] SUPERINTENDENCIA DE BANCA Y SEGUROS
2009 Resolución SBS N° 2116. 02 de Abril.

[15] SUPERINTENDENCIA DE BANCA Y SEGUROS
2009 Resolución SBS N° 2115. 02 de Abril.

[16] SUPERINTENDENCIA DE BANCA Y SEGUROS
2008 Resolución SBS N° 37. 10 de Enero

[17] KPMG LLP.

2006 "Second annual survey of capital assessment practice in the insurance sector", *Risk and Capital Management for Insurers*, año 2, pp 6. Consulta: 22 de setiembre de 2012 <http://www.kpmginsiders.com/pdf/KP89_RCMI_WEB.pdf>

[18] THE BUSINESS CONTINUITY INSTITUTE
2010 Guía de Buenas Prácticas 2010. Edición Global. Ciudad: Lee Glendon.

[19] INTERNATIONAL STANDARD ORGANIZATION – ISO
2012 "Benefits of International Standards". Website de ISO. Consulta: 19 de Setiembre del 2012. <http://www.iso.org/iso/home/standards/benefitsofstandards.htm>

[20] INTERNATIONAL STANDARD ORGANIZATION – ISO
2012 ISO 22301. Societal Security – Business continuity management systems – Requirements. 15 de Mayo.

[21] BRITISH STANDARDS INSTITUTION – BSI
2009 *BS 25 999 - A framework for resilience and success* [Diapositivas]. <http://www.paramountassure.com/pdf/BCP_0.pdf>

[22] INFORMATION SECURITY & BUSINESS CONTINUITY ACADEMY
2012 *ISO 22301 vs. BS 25999-2 – An Infographic*. Consulta 22 de Noviembre del 2012. <http://blog.iso27001standard.com/2012/05/22/iso-22301-vs-bs-25999-2-an-infographic/>

[23] INTERNATIONAL STANDARD ORGANIZATION – ISO
2011 ISO/DIS 22313. Societal security — Business continuity management systems — Guidance. 13 de Diciembre <http://www.continuityinsights.com/sites/continuityinsights.com/files/legacyimages/ISO_DIS_22313_(E).pdf>

[24] BSI Group
2012 *Gestión de Continuidad de Negocio - De BS 25999 a ISO 2230.* Consulta 22 de noviembre del 2012.

<http://www.bsigroup.es/es/certificacion-y-auditoria/Sistemas-de-gestion/Biblioteca-de-BSI/Documentacion-corporativa/LD-corporative-docs-Source/Gestion-de-Continuidad-de-Negocio---De-BS-25999-a-ISO-22301/>

[25] BSI Group
2013 *BSI publica una nueva guía para ayudar a las organizaciones a mitigar el riesgo y gestionar la continuidad del negocio.* Consulta 25 de marzo del 2013. <http://www.bsigroup.es/certificacion-y-auditoria/Sistemas-de-gestion/Novedades/Noticias-2012/LD-News-Source-/BSI-publica-una-nueva-guia-para-ayudar-a-las-organizaciones-a-mitigar-el-riesgo-y-gestionar-la-continuidad-del-negocio/>

[26] INTERNATIONAL STANDARD ORGANIZATION – ISO
2009 *ISO 31000: 2009. Risk management — Principles and guidelines*. 15 de Noviembre.
< http://www.imeny.comyr.com/file/pdf/ISO-31000.pdf>

[27] SUPERINTENDENCIA DE BANCA Y SEGUROS
2012 *Sistema IG-ROP ("Informe de Gestión de Riesgo Operacional").* Lima.

[28] SUPERINTENDENCIA DE BANCA Y SEGUROS
2012 *"Acerca de la SBS".* 20 de Setiembre.
<http://www.sbs.gob.pe/0/modulos/JER/JER_Interna.aspx?ARE=0&PFL=0&JER=4>

[29] SUPERINTENDENCIA DE BANCA Y SEGUROS
2012 *"Filosofía de Regulación y Supervisión".* 20 de Setiembre.
<http://www.sbs.gob.pe/0/modulos/JER/JER_Interna.aspx?ARE=0&PFL=0&JER=46>

[30] SUPERINTENDENCIA DE BANCA Y SEGUROS
2011 *Ley N° 26702. Texto concordado de la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia De Banca Y Seguros.* 05 de Noviembre.
<http://www.sbs.gob.pe/repositorioaps/0/0/jer/regu_leygralbancseguro/2012/Ley26702_05-06-2012.pdf>

[31] NATIONAL FIRE PROTECTION ASSOCIATION
2010 *NFPA 1600. Standard on Disaster/Emergency Management and Business Continuity Programs.* Setiembre.
<http://www.nfpa.org/assets/files/pdf/nfpa1600.pdf>

[32] STANDARDS AUSTRALIA
2004 HB 221:2004. *Business Continuity Management*. Australiza. 2004, 2, pp 3 – 4.
<http://www.anao.gov.au/uploads/documents/Business_Continuity_Management_.pdf>

[33] SUPERINTENDENCIA DE ENTIDADES FINANCIERAS Y CAMBIARIAS
2003 *Basilea II: Hacia un nuevo esquema de medición de riesgos*. Consulta: 22 de Setiembre.
<http://www.felaban.com/boletin_clain/basileaII.pdf>

[34] BANCO INTERNACIONAL ESPAÑOL – BANKINTER
2012 *Información societaria.* Consulta: 23 de Setiembre.
<https://www.bankinter.com/www2/particulares/es/inicio/informacion_societaria#ID=ISOCIETARIA&attr=WEBHEBPDPC1>

[35] BANCO INTERNACIONAL ESPAÑOL – BANKINTER
2012 *Productos Bankinter.* Consulta: 23 de Setiembre.
<https://www.bankinter.com/www2/particulares/es/inicio/productos_bankinter#ID=PRODUCTOS&attr=WEBHEBPDPC2>

[36] BRITISH STANDARDS INSTITUTION – BSI
2012 *Bankinter recibe el primer certificado ISO 22301 emitido por BSI*. Consulta: 23 de Setiembre.
<http://www.bsigroup.es/certificacion-y-auditoria/Sistemas-de-gestion/Novedades/Noticias-2012/LD-News-Source-/Bankinter-recibe-el-primer-certificado-ISO-22301-emitido-por-BSI/>

[37] DELOITTE TTL.
2012 *Planeación la continuidad de negocio.* Consulta: 22 de Setiembre.
<http://www.deloitte.com/view/es_PE/pe/servicios/enterprise-risk-services/seguridad-y-privacidad/planeacion-de-la-continuidad-del-negocio/index.htm>

[38] PROTIVITI
2012 *Soluciones.* Consulta: 22 de Setiembre.
<http://www.intellityconsulting.com/soluciones/index.html>

[39] IBM
2012 *Continuidad empresarial*. Consulta: 22 de Setiembre.
<http://www-935.ibm.com/services/mx/es/it-services/servicios-de-continuidad-de-negocio.html>

[40] BUSINESS DEVELOPMENT ASSOTIATION
2012 *Consultoría para la continuidad del Negocio.* Consulta: 22 de Setiembre.
<http://www.bdaglobal.com/es/services/continuity.php>

[41] ICM
2012 *Business Continuity & Disaster Recovery.* Consulta: 22 de Setiembre.
<http://www.icm.co.uk/what-we-do/business-continuity-disaster-recovery/icm-shadow-planner.asp>

[42] BPSi
2012 *Business Protector*. Consulta: 22 de Setiembre.
<http://www.businessprotection.com/about-bpsi-2/the-company/>

[43] TAMP SYSTEMS
2012 *Tamp DRS.* Consulta: 22 de Setiembre.
<http://www.drsbytamp.com/Web/PDF/TAMP%20DRS%20Smartphone%20App.pdf>

[43] BUSINESS DEVELOPMENT ASSOTIATION
2012 *Continuum BCP.* Consulta: 22 de Setiembre.
<http://www.bdaglobal.com/es/aboutus/continuum.php>

[45] Guía de los Fundamentos para la Dirección de Proyectos (Guía del PMBOK) PROJECT MANAGEMENT INSTITUTE
2013 Quinta Edición. Pennsylvania: PMI Publications.

[46] WORKPOINT LLC
2006 *BPM Basis: What you need to know about Business Process Management.* <http://www.workpoint.com/wpDocs/WorkpointBPMBasicsWP.pdf>