# UNIVERSIDAD CATÓLICA DE SANTA MARÍA

## FACULTAD DE CIENCIAS E INGENIERÍAS FÍSICAS Y FORMALES

## PROGRAMA PROFESIONAL DE INGENIERÍA INDUSTRIAL

# "DISEÑO Y PROPUESTA DE UNA METODOLOGÍA PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO, BASADO EN LA NORMA ISO/IEC 22301:2012"

**Presentado por:**

**DELGADO CONCHA,**
**KEVIN GILMAR**

**AREQUIPA – PERÚ**

**2015**

**DEDICATORIA**

*A Dios Todopoderoso por estar a mi lado en todo momento*

*A mis padres, por todo el esfuerzo y dedicatoria*

*que pusieron a mis estudios y a mi desarrollo*

*como persona, siendo motivadores*

*y partícipes de este logro.*

# RESUMEN

El presente trabajo de investigación, busca establecer y definir una metodología para la implementación de un Sistema de Gestión de Continuidad del Negocio (SGCN), teniendo como base principal los requisitos y recomendaciones de la norma ISO/IEC 22301:2012 “Seguridad de la Sociedad: Sistemas de Continuidad del Negocio-Requisitos” para que pueda ser aplicada en cualquier tipo de organización, orientada a la realidad del Perú y de la región Arequipa.

El objetivo principal es tener una secuencia de actividades y tareas específicas y explicadas sistemáticamente, que permitan en una organización el soporte y continuidad de los procesos más importantes; y a su vez considere el contenido de la norma ISO/IEC 22301:2012, dando la posibilidad de acercar a una empresa a obtener la certificación.

Se busca también la difusión de la importancia de contar con este Sistema para cualquier organización, sin importar su tamaño ni giro de negocio resulta una acción que puede lograr evitar las pérdidas más grandes evaluadas como resultado de su aplicación.

## ABSTRACT

This investigation, seeks to establish and define a methodology for the implementation of a Management System Business Continuity (BCMS) , having as main base the requirements and recommendations of the ISO / IEC 22301 : 2012 "Safety Society : Business Continuity Systems - Requirements "that can be applied to any type of organization , geared to the reality of Peru and the Arequipa region

The main objective is to have a sequence of activities and specific tasks that are systematically explained and enable an organization support and continuity of the most important processes; and in turn consider the contents of the ISO / IEC 22301 : 2012 , giving the possibility of bringing a company to obtain certification.

This paper also seeks spreading the importance of this system for any organization, regardless of size or line of business is an action that can achieve avoid bigger losses estimated as a result of the application.

# INDICE DE CONTENIDO

# ÍNDICE DE ILUSTRACIONES

# ÍNDICE DE TABLAS

# ÍNDICE DE GRÁFICAS

# CAPÍTULO I

# PLANTEAMIENTO TEÓRICO

## 1.1. TÍTULO

"Diseño y propuesta de una metodología para la implementación de un Sistema de Gestión de Continuidad del Negocio, basado en la norma ISO/IEC 22301:2012".

## 1.2. IDENTIFICACIÓN DEL PROBLEMA

En todo el mundo, existe un gran incremento del número de organizaciones que plantean empíricamente diferentes iniciativas para normalizar los Sistemas de Gestión de Continuidad del Negocio (a falta de una metodología definida y clara) ya que se viene experimentando la importancia de tenerlo implantado para asegurar el funcionamiento continuo de las operaciones de las empresas.

El problema radica en que en Perú, la mayoría de las empresas no cuenta con un plan adecuado que asegure la continuidad operativa de sus funciones, ante eventuales desastres o problemas que afecten sus procesos críticos. Asimismo, pocas son las empresas que asignan recursos para abordar la continuidad operativa (excepto el sector bancario que está regulado y obligado por la SBS); y sólo existe una

empresa (la Bolsa de Valores de Lima), que tiene certificación de la norma ISO/IEC 22301 sobre la Gestión de Continuidad del Negocio.

En resumen, debido a la situación general del Perú, su complejidad geográfica, ya que está comprendida entre una de las localidades con mayor actividad sísmica y de probabilidad de desastres naturales, y experimentando que las metodologías de Plan de Continuidad que se tienen a nivel mundial, no son claras ni tienen lineamientos específicos, y no se ajustan a la realidad nacional; es que se busca plantear una metodología para implementar el sistema, de forma clara y sencilla; y que pueda ser aplicada a cualquier tipo de empresa.

Con esto se logrará también masificar los Planes de Continuidad en el Perú, incrementando notoriamente la competitividad de las empresas y contribuyendo a disminuir todas las pérdidas producto de interrupciones en los procesos, asegurando el mantenimiento y sostenibilidad sobretodo de pequeñas y micro empresas, teniendo como consecuencia disminución de desempleo.

## 1.3. DESCRIPCIÓN DEL PROBLEMA

La continuidad de las operaciones en una empresa es vital, en caso de presentarse una interrupción de los procesos críticos, simplemente no se puede operar. No se puede realizar la entrega del producto o servicio y se pierde la confiabilidad. Las estadísticas dicen: “… una empresa que deja de operar por el espacio de diez días consecutivos, jamás se recuperará” (Hiles, 2004).

No es de mucha utilidad, en esta situación, los planes estratégicos, ni modelos de investigación de mercados, ni modelos de aseguramiento de calidad, si no se cuenta con una metodología aplicada e implementada que asegure la continuidad de la cadena de suministros y de los procesos más importantes, si un desastre se presentara.

El atentado de las Torres Gemelas en el 2001, el accidente nuclear de la Central nuclear “Fukushima I” en el 2011 y como no el terremoto de Pisco del 2007, ha evidenciado la exigencia de poseer planes que aseguren que las operaciones vitales no se interrumpan. Luego del atentado de las Torres, una de las pocas firmas del área financiera que siguió operando fue Merryl Linch y se atribuyó al hecho de contar con un Plan de Continuidad del Negocio (Hiles, 2004).

Los desastres se generan en cualquier momento; sin embargo, las organizaciones no sólo se ven afectadas por estos, sino también por pequeños eventos que pueden interrumpir las operaciones de la empresa. Diversos factores como por ejemplo: a) incremento de la dependencia tecnológica, b) presiones de “velocidad de mercado”, en algunas ocasiones pueden afectar más. Así podemos evidenciar situaciones menores que generan perturbación, tales como: cortes de fluido eléctrico, fallas en los sistemas de información, defectos en equipos, materia prima contaminada, virus en las computadoras, etc.

Lamentablemente, pocas son las empresas que asignan recursos e invierten en la planificación de sus actividades para llevar al mínimo las consecuencias de posibles desastres y asegurar la continuidad después

de una calamidad. Todas estas dificultades pueden ser superadas implementando un Sistema de Continuidad del Negocio. Es por este motivo que se ha visto un aporte importante el establecer una metodología flexible y que pueda aplicarse a cualquier empresa, para definir un Plan de Continuidad del Negocio.

## 1.4. OBJETIVO

### 1.4.1. OBJETIVO GENERAL:

- Diseñar una propuesta metodológica para la implementación de un Sistema de Gestión de Continuidad del Negocio, que pueda ser aplicada a cualquier tipo de empresa en el Perú, basado en la norma ISO/IEC 22301.

### 1.4.2. OBJETIVOS ESPECÍFICOS:

- Evaluar las diferentes estándares internacionales sobre los elementos del Sistema de Continuidad del Negocio existentes, para extraer sus fortalezas; priorizando el contenido de la norma ISO 22301:2012.
- Realizar un diagnóstico situacional básico de las empresas en el Perú y Arequipa, para identificar el campo de acción que puede tener la metodología y su factibilidad para aplicarse.
- Definir una propuesta metodológica que identifique las actividades requeridas para implementar y mantener un Sistema de Gestión de Continuidad del Negocio, que contiene todos los requerimientos y consideraciones de la norma ISO 22301:2012.

- Realizar un Análisis de Impacto del Negocio (BIA) y un Análisis de Riesgo (primeras dos partes fundamentales del SGCN), según la metodología propuesta, para una empresa financiera que realiza actividades en la Región Arequipa (Camaná).

## 1.5. HIPÓTESIS

Con la aplicación de la metodología para la implementación de un Sistema de Gestión de Continuidad del Negocio propuesta; se logrará asegurar la Continuidad del Negocio y de los procesos críticos identificados de cualquier organización.

## 1.6. ANTECEDENTES DE LA INVESTIGACIÓN

No se ha encontrado una metodología clara y sistemática para la implementación de un sistema de gestión de continuidad del negocio; y que se base a la norma ISO/IEC 22301. Lo que existe son estudios e investigaciones donde se elaboran los Planes de Continuidad (un elemento de todo el sistema) a diferentes empresas. Dentro de estas investigaciones, existen metodologías ensayadas y exclusivas al desarrollo del Plan, pero no de todo el sistema. También existe el desarrollo de una tesis de la Universidad Austral de Chile, donde se elabora un modelo para la implementación de un Plan de Continuidad, de acuerdo a la realidad de ese país.

Se considera que el presente trabajo es original, debido a que recién en mayo del 2012, salió al mercado la norma ISO 22301:2012 “Seguridad de la Sociedad: Sistemas de Continuidad del Negocio-Requisitos” (Fuente Consultora Deloitte); y por su contenido, se considera que

cobrará mucha importancia y por la situación de nuestro país, generará mucha demanda por las organizaciones. Con la metodología propuesta se da una excelente alternativa para desarrollar el sistema y posteriormente, lograr la certificación.

## 1.7. TIPO DE INVESTIGACIÓN

Se considera que el presente trabajo de investigación es de carácter exploratorio, debido a que el fin es examinar un tema poco conocido, recogiendo toda la información sobre las recomendaciones y metodologías de los elementos del Sistema, integrándolos y obteniendo como resultado una metodología clara y sistémica, que pueda ser aplicada por cualquier tipo de empresa en el Perú. Además es de tipo experimental correlacional, relacionando las variables necesarias para conocer los efectos (aplicando la metodología en una empresa local para verificación de la misma).

## 1.8. ALCANCE

La metodología planteada, busca ser la base para el desarrollo del Sistema de Gestión de Continuidad del Negocio para cualquier tipo de empresa en el Perú, que incluye todas las actividades más importantes de la norma ISO/IEC 22301.

Su aplicación experimental incluye el desarrollo del Análisis de Impacto del Negocio (BIA) y el Análisis de Riesgo (elementos más importantes e iniciales dentro de todo el sistema); para la empresa financiera “Caja Municipal de Ahorro y Crédito ICA”. Por el tiempo y complejidad del

estudio, se toma en consideración sólo tres áreas (Créditos, Tesorería y Operaciones).

## 1.9. JUSTIFICACIÓN DE LA INVESTIGACIÓN

### 1.9.1. ASPECTO GENERAL:

El presente trabajo de investigación, permitirá a todas las empresas de Arequipa y del Perú tener como referencia una propuesta metodológica integrada, de acuerdo a la norma ISO/IEC 22301, para poder contar dentro de su organización con un sistema que asegure la continuidad de sus operaciones.

Debido a que nuestro País presenta una gran complejidad de eventos externos e internos que hacen que sus procesos más importantes se vean afectados; y por la reciente aparición en el mercado de la norma para la Gestión de la Continuidad, es que cobra una gran importancia el tema desarrollado. La razón por la cual actualmente son pocas las empresas que cuentan con un Sistema para la Continuidad de sus operaciones es que existe poca información y muy diversa sobre cómo implementarlo y sobre su contenido.

Con esta investigación se recopilará toda la información necesaria para tener el modelo compatible con cualquier organización; que sea claro y sencillo; muy sistematizado y que defina paso a paso los requerimientos para asegurar la continuidad operativa. Esto genera un gran aporte a las empresas que buscan la certificación, ya que la propuesta metodológica incluirá todas las actividades en orden y debidamente explicadas, que tienen en su contenido los

requerimientos más importantes de la norma; lo cual evita que se tenga que las empresas tengan que invertir tiempo revisando toda la norma y entendiéndola.

### 1.9.2. ASPECTOS ECONÓMICO:

La metodología propuesta tiene como fin principal el aspecto económico, debido a que implantando un Sistema de Gestión de Continuidad del Negocio, se identifican los procesos críticos de la organización; y esta selección se realiza evaluando el impacto económico de cada proceso y el impacto organizacional. Una vez identificados y cuantificados los procesos, se prioriza los planes de recuperación para estos y se evita las pérdidas más grandes que podría tener la empresa.

También existen consultoras como Deloitte, Ernest and Young, BSI Group; que ofrecen el servicio de implementar el sistema. Asimismo, existe software como el de Global Business Solutions (GBS) que desarrolla todo el contenido de la norma ISO/IEC 22301 en un sistema integrado con todas las áreas de la empresa; pero que tiene un costo económico muy elevado. La propuesta presentada busca reemplazar estas alternativas para lograr implementar el Sistema de Continuidad, ya que con el desarrollo de la metodología de una manera adecuada, se podría obtener el mismo resultado que con las consultoras o el software mencionado.

### 1.9.3. ASPECTO SOCIAL:

El presente trabajo de investigación, también busca masificar la acción en las empresas para la implementación del sistema, haciendo que logren entender la importancia de contar con planes que aseguren su funcionamiento continuo. Esto a su vez, se convierte en una importante fortaleza para las organizaciones, que las vuelve más competitivas y flexibles, preparadas para el cambio y que incrementa notoriamente su calidad de servicio. La consecuencia directa se ve reflejada en una mayor satisfacción del cliente al saber que puede contar con el servicio o producto que ofrece la empresa, a pesar de cualquier eventualidad.

## 1.10. VARIABLES

### 1.10.1. VARIABLE INDEPENDIENTE:

- Metodología para el SGCN propuesta.

### 1.10.2. VARIABLES DEPENDIENTES:

- Continuidad del negocio y de los procesos críticos identificados.

**Tabla 1 – Operacionalización de Variables**

| VARIABLE | TIPO | DEFINICIÓN CONCEPTUAL | DEFINICIÓN OPERACIONAL | INDICADORES | HERRAMIENTAS |
|---|---|---|---|---|---|
| Metodología del SGCN propuesta | INDEPENDIENTE | Conjunto de acciones, consideraciones y recomendaciones elaborados y sistematizados; con el fin de implementar un Sistema de Continuidad en cualquier tipo de organización y de acuerdo a la norma ISO 22301. | Integración de elementos, estándares internacionales, experiencias y actividades relacionadas a un SGCN. Revisión de documentos y registros considerados por la norma ISO 22301. | Alcance | Difusión y calificación por los portadores. |
| | | | | Extensión | Tener consideraciones, obligaciones y excepciones. |
| | | | | Flexibilidad | Desarrollo de la metodología en el campo de acción. |
| Continuidad del Negocio y de los procesos críticos | DEPENDIENTE | Lograr el aseguramiento de la funcionalidad de una organización, cumpliendo con los objetivos de cada proceso de negocio; ante eventos que afecten el normal funcionamiento de los mismos. | Aplicación de la metodología para lograr implementar las actividades que permitan contar con el sistema. | Impacto en el negocio | Evaluación de procesos críticos. |
| | | | | | Determinar recursos y aplicaciones. |
| | | | | | Determinar tiempos de recuperación. |
| | | | | Impacto de los riesgos | Evaluación de riesgos. |
| | | | | | Controles y medidas de acción. |

Fuente: Elaboración propia.

## 1.11. TÉCNICAS E INSTRUMENTOS

Para el proceso de recolección de información y verificación del presente trabajo, se estima aplicar las siguientes técnicas:

- DOCUMENTAL:

La técnica usada para la investigación es la documental. Para la elaboración de la metodología, la información primaria se obtendrá de la norma ISO/IEC 22301. Como fuentes de información secundaria se tiene libros, estadísticas, tesis de investigación y la información proporcionada por la red de internet.

- TÉCNICA DE CAMPO:

Para la recolección de los datos sobre los procesos, y su impacto operacional y económico (para desarrollar el BIA); así como asignación de responsabilidades y para los planes (para desarrollar los Planes de Continuidad); se utilizará básicamente estas técnicas de campo: Observación, encuestas, entrevistas y talleres.

## 1.12. CAMPO DE VERIFICACIÓN

Para la verificación de la propuesta metodológica, se tiene seleccionada la aplicación de los elementos iniciales y fundamentales (BIA y Análisis de Riesgos) a la empresa financiera “CMAC ICA”, que trabaja como una caja de ahorro y créditos; y según los contactos de la agencia Camaná, no cuenta con un Sistema de Gestión de Continuidad del Negocio. Se cuenta con el apoyo de un coordinador de créditos; y la aprobación informal del Administrador de la agencia.

Se seleccionó esta empresa como prueba, debido a que se cuenta con información privilegiada para facilitar la aplicación del BIA y el Análisis de Riesgo; y tiene mayor utilidad y urgencia el desarrollo del sistema, según el tipo de servicio que brinda esta organización.

## 1.13. CRONOGRAMA

**Tabla 2 – Cronograma de Actividades**

| ACTIVIDADES | ENERO | | FEBRERO | | MARZO | | ABRIL | |
|---|---|---|---|---|---|---|---|---|
| Aprobación del Plan de Tesis | ■ | | | | | | | |
| Recopilación Bibliográfica | ■ | | | | | | | |
| Elaboración de Fichas | | ■ | | | | | | |
| Desarrollo de la Metodología | | ■ | ■ | | | | | |
| Verificación de la Metodología | | | ■ | ■ | | | | |
| Evaluación de resultados | | | ■ | ■ | | | | |
| Comprobación de objetivos e hipótesis | | | | ■ | | | | |
| Conclusiones y recomendaciones | | | | | ■ | | | |
| Revisión y corrección del borrador | | | | | ■ | ■ | | |
| Redacción final | | | | | ■ | ■ | ■ | |
| Reproducción y encuadernación | | | | | | | ■ | |
| Presentación de ejemplares | | | | | | | ■ | ■ |

Fuente: Elaboración propia.

# CAPÍTULO II

# MARCO TEÓRICO

Se presentan los principales conceptos y conocimientos que se consideran necesarios para el desarrollo y entendimiento apropiado para el trabajo de investigación realizado.

## 2.1. ESQUEMA CONCEPTUAL

### 2.1.1. Amenaza:

Es una razón potencial de un incidente[1] que no es deseado, el cual puede causar un daño a un sistema u organización (ISO 27005)

NIST de los Estados Unidos de América (2008) lo define como : "*Cualquier circunstancia o hecho que pueda afectar negativamente a las operaciones de la organización, sus activos de información o individuos a través del acceso no autorizado, destrucción, acceso, modificación de la información, y/o negación de servicio. Además, la posibilidad de una amenaza de fuente de explotar con éxito una vulnerabilidad de la información del sistema en particular*"

[1] Es la interrupción no planeada de un servicio o la reducción en la calidad de un servicio (Hiles, 2007)

### 2.1.2. Análisis de Impacto del Negocio (BIA):

Por su significado en inglés (Business Impact Analysis), el BIA es una fase del Sistema de Gestión de Continuidad del Negocio (SGCN), que tiene como objetivo identificar procesos que tengan estrecha relación con la misión de una organización. Busca evaluar los impactos de la gestión comercial del negocio, si dichos procesos fuesen interrumpidos como resultado de un evento como un desastre. Los impactos financieros están referidos a pérdidas monetarias (ventas, penalidades o dinero dejado de percibir); mientras que los impactos operacionales representan pérdidas no monetarias que se relacionan con el giro de negocio como competitividad, nivel de servicio o daño a la confidencialidad. (Alberto G. Alexander, 2007)

### 2.1.3. Plan de Continuidad del Negocio (PCN):

Un Plan de Continuidad de Negocio está compuesto de varias fases que empiezan con una evaluación de los procesos que componen la organización. Este análisis servirá para priorizar qué procesos son críticos para la organización y establecer una política de recuperación ante un desastre. Por cada proceso se identifican los impactos potenciales que amenazan la organización, estableciendo un plan que permita continuar con la actividad empresarial en caso de una interrupción. (Laura del Pino, 2007).

### 2.1.4. Impacto:

El Business Continuity Institute (2010) lo define como un *"Evento que tiene la capacidad de provocar la pérdida de o la interrupción de las*

*operaciones, servicios o funciones de la organización, el cual, si no se administra, puede escalar y convertirse en una emergencia, crisis o desastre".* Su identificación y medición es relevante en el proceso de la Gestión y evaluación de Riesgos, que es el conjunto de tareas que permite analizar, tratar y evaluar los riesgos en las empresas. Cabe mencionar que la estimación del impacto es posible expresarla de forma cuantitativa, es decir estimando pérdidas económicas, o de forma cualitativa, asignando un valor dentro de una escala (p. e. alto, bajo, medio), también se recurre al análisis de grado de pérdida o impacto que causaría una detención en un activo de información mediante el ensayo de probabilidades de ocurrencia, ya que se utiliza para establecer si se invertirá en medidas para evitar dicha interrupción.

### 2.1.5. Gestión Integral de Riesgos:

En el artículo 3° de la Resolución SBS N° 37 – 2008, se precisa que "la Gestión Integral de Riesgos es un proceso, efectuado por el Directorio, la Gerencia y el personal aplicado en toda la organización y en el establecimiento de su estrategia, elaborado para tener identificados los eventos que pueden afectarla, gestionarlos de acuerdo a su nivel de riesgo y proveer una seguridad prudente en el logro de sus objetivos". (SBS 2008).

Cabe indicar que en la actualidad, se define a la Gestión de Continuidad del Negocio como un elemento adecuado de la Gestión de Riesgo operacional (SBS 2008) dando disposiciones más claras en cuanto al manejo y a este nuevo enfoque.

### 2.1.6. Gestión de la Continuidad del Negocio:

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 grupo de procesos holísticos que permiten tener identificadas las posibles amenazas, así como el impacto en las organizaciones.

### 2.1.7. ISO/IEC 22301:2012:

Norma internacional que detalla los requerimientos para establecer, implementar, operar, monitorear y mejorar un sistema de gestión que se encuentra documentado, para salvaguardar, reducir la probabilidad de ocurrencia, prepararse, proteger y recuperarse de incidentes nocivos cuando acontecen.

Los requisitos desarrollados en la norma son genéricos y se aplican a todas las empresas o parte de las mismas sin importar el tamaño ni su naturaleza. Además, las necesidades de cada organización deben estar enfocadas a un marco regulatorio, obligaciones organizacionales, productos y servicios, los procesos empleados, el

volumen, 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:

- Tener establecido, implementado, lograr mantener y tener mejora continua de un plan de gestión de continuidad de negocio.
- Asegurar la aprobación con las políticas determinadas de gestión de la continuidad del negocio.
- Lograr una certificación o registro de su Plan de Gestión de Continuidad de Negocio por una entidad externa.
- Determinar y declarar su conformidad con este estándar internacional.

Este estándar nos alcanza el llamado modelo PDCA de Deming “Plan – Do – Check - Act” (PDCA) para planificar, establecer, implementar, monitorear, revisar y mantener continuamente, incrementando la efectividad del Plan de Gestión de Continuidad del Negocio (SGCN). La ilustración 1 muestra cómo un SGCN toma las entradas y a través de acciones y procesos logra la los resultados esperados (ISO 2012).

**Ilustración 1 – Mejora Continua del Sistema de Continuidad**


Fuente: Blog de Consultores ISO/IEC 22301:2012 (27001 Academy, 2010).

## 2.2. BENEFICIOS DEL PCN Y RELACION CON LA COMPETITIVIDAD DE LAS ORGANIZACIONES

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

- **Ventaja competitiva frente a otras organizaciones:** el hecho de revelar que se realizan medidas para asegurar la continuidad de negocio mejora la imagen en el público de la organización y devuelve la confianza frente a socios, inversionistas, el mercado y proveedores.

- **Previene o minimiza las pérdidas de la organización en caso de desastres:** es apto de tener identificado de forma proactiva los

posibles daños e impactos que una paralización de sus actividades de los procesos puede provocar.

- **Asegurar que las actividades del negocio soporten y se recuperen ante interrupciones**: incrementando la disponibilidad de los productos y servicios preparados para el cliente.
- **Menor riesgo de sufrir sanciones económicas:** al acomodarse a requerimientos regulatorios definidos.
- **Asignación más eficiente de las inversiones en materia de seguridad:** con la aplicación del análisis de impacto, se logra priorizar las acciones críticas y establecer los esfuerzos y los presupuestos en las áreas más necesitadas (GASPAR, 2004).

## 2.3. PCN EN EL MUNDO

En un periodo donde es más importante usar mejor los recursos de los que dispone la empresa, es indispensable desarrollar ventajas competitivas que permitan satisfacer las exigencias del mercado. Una importante ventaja podría desarrollarse garantizando la disponibilidad de los servicios a los clientes, aún después de que ocurre una eventualidad. Un estudio realizado por el Emergency Management Forum en Estados Unidos dice lo siguiente (ITEAM, 2013):

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

Luego de ocurrido un evento de interrupción en una organización, se tiene como consecuencia dificultades financieras, además de daños intangibles como reducción de la productividad, estrés, recursos desviados, y en su conjunto, ocasiona un daño a la imagen de la empresa. En el entorno de la mala reputación de la organización, el nombre de los ejecutivos responsables es lo que se pone en riesgo. Hay que recordar que las empresas que sufren este tipo de incidentes son noticia al día siguiente, en muchos casos la prensa es la responsable de a los implicados. Además, adicionalmente, los directores corporativos pueden ser demandados por los daños ocasionados como consecuencia de interrupción del negocio.

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

- Para lograr una consultoría: Deloitte, KPMG, Risk México, Price Water House Coopers y AON.
- Como servicios de apoyo, como hardware, software, sitios alternos o centro de llamadas: Sungard, IBM, EMC, Symantec, Veritas, CITRIX y CISCO.
- En el tema de disciplina y comportamiento organizacional: Business Continuity Institute (BCI), Business Standar Institute (BSI), Disaster Recovery Institute Internacional (DRII), ISO 27002, ITIL, ISO 22301 y NFPA.

Una encuesta que se desarrolló por “Chartered Management Institute” sobre cómo se gestiona la continuidad de negocios a 1257 gerentes de

organizaciones del Reino Unido, arroja que tan sólo la mitad de sus empresas tiene desarrollado un Plan de Continuidad, considerando que el 94% de los encuestados consideran esta actividad como de una importancia elevada (WOODMAN, 2007).

## 2.4. EMPRESAS QUE HAN IMPLEMENTADO EL SGCN

### WAL-MART STORES INC.:

En Agosto del 2005 con el huracán Katrina, que cambió su categoría de tormenta tropical a huracán, Jason Jackson, que fue Director de Continuidad del Negocio de Wal-Mart cambio su ubicación al centro de comando de emergencias de Wal-Mart. Pasado 48 horas luego de ocurrido el huracán, este llegó a Florida, Jackson estaba reunido con un grupo de 50 gerentes y personal de soporte, antes de que el huracán tocara las tierras de México, Jackson dio la orden de que los almacenes de Wal-Mart dieran provisiones a áreas de almacenamiento designadas para tener la capacidad de proveer a las tiendas cuando fuera posible. Wal-Mart contaba con un sistema que podía actualizar instantáneamente los inventarios; pero la zona de Wal-Mart quedo sin señal. Como medida de contingencia se tenía establecida las vías telefónicas, donde Jackson atendió las llamadas de las tiendas para saber cuáles eran los requerimientos, para el siguiente martes, unidades de transporte de Wal-Mart fueron a suministrar generadores y toneladas de hielo seco a lo largo de las tiendas que se encontraban afectadas. Inicialmente 126 sucursales fueron cerrados por encontrarse directamente en la zona de impacto del huracán, a pesar de las pérdidas reportadas por las tiendas,

15 días después, todas a excepción de 15 tiendas, volvieron a abrir sus puertas (ZIMMERMAN, 2005).

**COMPAREX ESPAÑA S.A.:**

En febrero de 2005 se inició un incendio en el Edificio de Windsor, donde se encontraban ubicados los servidores principales, después de 6 horas toda la propiedad quedo devastado. Para esto, Comparex contaba con un plan de continuidad definido y que debido a las circunstancias, procedió con su activación. Dentro de las actividades propias de las estrategias se realizó: Backups de información, sitios alternos de trabajo para que los empleados puedan restablecer sus operaciones desde otra ubicación, teniendo acceso a aplicaciones críticas utilizando como recurso indispensable el internet, infraestructura que le permitió la comunicación de voz y datos entre los centros (MUR, 2013).

El Sistema que se definió, y la integración alcanzada, permitió a la organización lograr la recuperación de sus procesos la misma noche ocurrida el evento, se definieron los elementos tecnológicos (servidores, sistemas de almacenamiento, puestos de trabajo conectados a la red) que estaban disponibles y funcionando, así como los inactivos. Se recurrió a las copias de información que la organización tenía en resguardo en ciudades de Madrid y Barcelona, comprobando si podía realizarse la recuperación total al último día hábil de desarrollo de la actividad. Se realizó el alquiler de las ubicaciones alternas, dotándolas de equipo necesario que ya estaba definido en el plan, para trabajar y se

contactó a todos los clientes implicados para notificarles la situación de la compañía. El plan resulto un éxito para la compañía (MUR, 2013).

**BANKINTER:**

El 18 de julio de 2012, BSI tuvo como evento la entrega de su primer certificado a internacionalmente de la nueva norma ISO 22301:2012 de Continuidad de Negocio a la empresa Bankinter. El certificado avala que la empresa financiera mantiene activo y definido un Sistema de Gestión de Continuidad de Negocio conforme a los requisitos de la nueva norma. Este es el primer certificado ISO 22301 que fue emitido por BSI a nivel de sus actividades en todo el mundo. Además Bankinter pasa a ser la primera entidad financiera a nivel mundial certificada en ISO 22301. De acuerdo a los requisitos que contiene la norma, el certificado acredita el Sistema de Gestión de Continuidad de Negocio (SGCN) de Bankinter para los métodos de identificación, legitimación y firma de operaciones financieras y sus seguridades electrónicas a través de Internet, Teleproceso Operativo y la infraestructura de routing de Renta Variable para sus centros de Tres Cantos y Alcobendas en Madrid. (BSI GROUP, 2012).

## 2.5. ESTÁNDARES PARA LA ELABORACIÓN DE UN SISTEMA DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO

En esta parte, se presentan algunas prácticas y formas de desarrollo de los Sistemas que existen actualmente sobre Continuidad del Negocio desde diferentes orientaciones y entre los documentos que sirven de soporte para la elaboración del Plan de Continuidad de Negocio, se

tienen estándares que son reconocidos internacionalmente. Éstos son garantizados por instituciones reconocidas y que se dedican al desarrollo de actividades para asegurar la continuidad del negocio. En las siguientes páginas se evalúan las buenas prácticas y estándares encontrados.

En la Tabla Nº 2, se pueden observar los una información general de las instituciones y prácticas desarrolladas sobre el tema.

Como muestra la Tabla N º 2, las metodologías se han generado en distintas zonas geográficas, por lo cual es indispensable analizarlas en detalle para identificar los puntos de cada una que pueden aplicarse en Perú. Como corresponde, cada una se enfoca a un entorno diferente y a situaciones distintas, como aviso de crisis, tecnología, procesos de negocio y sitio alterno entre otras, debido a esto es significativo aprender de cada una de ellas, con la finalidad de identificar el tema en el que cada una se especializa y de esta forma, fortalecer la metodología que se diseñará para ser aplicada en nuestro país.

**Tabla 3 – Datos Generales de las metodologías de SGCN**

| ORGANIZACIÓN | ESTÁNDAR | ALCANCE | AÑO DE ACTUALIZACION | ORIGEN |
|---|---|---|---|---|
| BSI | BS 25999-1 BS 25999-2 | BCM (Business Continuity Management) | 2007 | Inglaterra |
| BSI | BS 25777 | ITDR (Information Technology Disaster Recovery) | 2008 | Inglaterra |
| BCI | Guía de las Buenas Prácticas | BCM identificando el ITDR como estrategia | 2008 | USA |
| ITIL | Gestión de la continuidad del servicio | Gestión de Servicios Informáticos | 2007 | Inglaterra |
| DRJ | Emergency Operation Center (EOC) | Centro alterno de operaciones para BCM como para ITDR | 2012 | USA |
| DRI DRJ | Prácticas Generalmente Aceptadas | BCM | 2007 | USA |
| National Fire Protection Association | NFPA 1600 | BCM | 2013 | USA |
| ISO | ISO 27002 | Seguridad de la información | 2005 | Ginebra (Suiza) |
| ISO | ISO 22301 | BCM | 2012 | Ginebra (Suiza) |

Fuente: Modelo integral de evaluación de un PCN, Estándares de elaboración, Guevara Arias (Chile, 2010).

### 2.5.1. BS 25999

La norma británica BS 25999 de la Institución Británica de Normas, toma la referencia del desarrollo de un PCN y amplía su trascendencia para incluir en su totalidad a la compañía. BS 25999 se divide en dos partes: BS 25999-1 y BS 25999-2. La BS 25999-1, o Código de Práctica tiene su publicación en diciembre de 2006 y es un documento normal que expone el propósito de la norma, es fundamentalmente un

documento que oriente y proporciona las recomendaciones prácticas para las el BCP. BS 25999-2, o la especificación, fue liberada en noviembre de 2007 y establece las exigencias para un Sistema de Gestión de la Continuidad (BCM). Esta es la parte de la norma que se certifica a través de una etapa de implementación, de auditoría y posterior certificación (PJR, 2013).

El estándar suministra una especie de parte introductoria a lo que es la Continuidad del Negocio, explicando la razón por la cual las empresas deben contar con un Plan de Continuidad de Negocio explicando cuáles son los beneficios que se logran con la implantación de éste.

Además explica las ventajas de contar con un Análisis de riesgos, un análisis de impacto y como estos asisten al Plan de Continuidad de Negocio. Las etapas que el estándar maneja, son identificadas como el ciclo de vida del BCP (PCN siglas en inglés Business Continuity Plan), el cual se puede distinguir en la Ilustración Nº 2.

**Ilustración 2 – Ciclo de Vida del Plan de Continuidad del Negocio**


Fuente: Norma Británica BS 25999-1, edición 2006.

Seguidamente, se explican con brevedad las etapas de este ciclo de vida (BS 25999-1: 2006):

- **Plan de Administración de Continuidad de Negocio:** Constituye la importancia de tener una administración del Plan de Continuidad de Negocio, en el que se lleve el seguimiento de cada una de las actividades que conforman el Plan y que permita identificar desde una forma general los puntos que falta especializar (BS 25999-1: 2006).

- **Entendiendo la organización:** Una actividad inicial y de mayor importancia para realizar el PCN es conocer y entender de forma minuciosa el negocio al que se ofrece la organización, para así conseguir como resultado un plan de continuidad óptimo. Es en

esta etapa dónde se lleva a cabo del desarrollo del Análisis de Impacto al Negocio (Business Impact Analysis, BIA por sus siglas en inglés), se determina todos los tiempos de recuperación: el Tiempo Objetivo de Recuperación (RTO) y el Punto Objetivo de Recuperación (RPO) (BS 25999-1: 2006).

- **Determinando la estrategia de Continuidad de Negocio:** Puede establecerse cualquier tipo de estrategia en función a la organización; como por ejemplo: Plan de Recuperación de Tecnología en caso de Catástrofe, sitios alternativos para la recuperación de tecnología y para la continuidad de las operaciones, destrezas para el trabajo desde casa, un sistema de comunicación interna y externa durante y después del incidente, respaldo de información en otro sitio, etc. (BS 25999-1: 2006).

- **Implementación de un programa de responsabilidades para la Continuidad de Negocio:** Reconocer y tener definido un equipo para la Continuidad de Negocio y cuáles son las tareas que se encuentran asignadas a cada uno de ellos, preventivas y de preparación, para estar aptos en cualquier momento ante una dificultad. Así, como las tareas que se deben realizar durante un evento de interrupción que sea manifestado. En esta etapa se identifica el equipo de Administración de Crisis y el equipo de Administración de Incidentes (BS 25999-1: 2006).

- **Pruebas y mantenimiento del Plan de Continuidad de Negocio:** Es realmente importante para el sistema poder realizar pruebas para tener un nivel de eficacia con la que puede asegurarse el

continuo funcionamiento del negocio ante la presencia de una posible interrupción. Además del proceso de mantenimiento del plan, es importante, para lograr instaurar un PCN actualizado y vigente, considerar que el negocio debe seguir operando y que se encuentra en constante cambio. En esta etapa se detalla la relevancia de experimentar los planes que se han perfeccionado para verificar la capacidad que posee y hallar mejoras que puedan ayudar a acrecentar el nivel de madurez del Plan de Continuidad de Negocio (BS 25999-1: 2006).

- **Desarrollando una cultura de Continuidad de Negocio:** Esta etapa busca desarrollar en todos los clientes internos de la empresa, la concienciación de que la organización puede tener en cualquier momento cierto suceso que afecte la operación normal de la empresa, ante lo cual se debe estar capacitados psicológica, tecnológica y técnicamente para poder dar continuidad al negocio con los recursos que cuenta la empresa, (BS 25999-1: 2006).

### 2.5.2. BS 25777

En muchas organizaciones, la realización de los procesos más importantes tiene como dependencia los servicios de información y tecnología de comunicaciones, definido en el BS 25777 como ICT (Information and Communications Technology) (BS 25777: 2008).

La finalidad del BS 25777 es soportar a las empresas a realizar una correcta estrategia para los servicios de información y tecnología de

comunicaciones. Los principios que componen el estándar son (BS 25777: 2008):

- **Protección:** Es necesario conocer las amenazas y vulnerabilidades mediante la evaluación de los sistemas de información, identificando con ello, los peligros que pueden disminuirse (BS 25777: 2008).
- **Detección:** Identificar los servicios que aguantan los procesos principales del negocio, para tenerlos como prioridad para su levantamiento (BS 25777: 2008).
- **Reacción:** Con la planeación de un programa relacionado a la continuidad, como el ICT, se logra la rápida reacción de la organización ante los incidentes, recortando así, el Downtime (BS 25777: 2008).
- **Recuperación:** Relacionado a las exigencias del negocio de las TI, y el desarrollo de los tiempos en que se necesita su recuperación, se puede concretar un plan de acción sobre las tecnologías que se recuperan inicialmente y las que se recuperarán a posterior (BS 25777: 2008).
- **Operación:** Operación es un principio que se enfoca a dar sustento a la operación contingente que la empresa despliegue después de la ocurrencia del suceso (BS 25777: 2008).
- **Regreso:** El ICT permite lograr la continuidad del negocio después de un incidente, pero es necesario plantear la mejor

estrategia para migrar la operación de la organización de regreso al Edificio principal (BS 25777: 2008).

El ICT debe contar con partes y elementos que para que pueda desenvolverse de la mejor manera, estos son (BS 25777: 2008):

- **Personal:** Son los que se encargan de la tarea diaria, y se tiene como personal importante los de TI y Comunicaciones. Ellos deben comenzar a desarrollar las destrezas para apoyar en caso de un escenario de contingencia. Una buena acción para lograr esto, es el desarrollo y práctica del ICT (BS 25777: 2008).
- **Localidades:** Es necesario reconocer el equipo indispensable para realizar la restauración de las tecnologías de información así como los lugares alternos que se utilizaran en un escenario de contingencia (BS 25777: 2008).
- **Tecnología:** Dentro de la tecnología pueden reconocerse algunos rubros como servidores, redes, servicios de voz, routert, información

El BS 25777: 2008, contiene buenas prácticas y desarrolla actividades enfocadas de buena manera para el área de TI, pues está totalmente detallado para no perder de vista ningún punto. Una gran ventaja es que se encuentra alineado y enfocado al BS 25999-1: 2007 de la misma institución, que está enfocado a los procesos del negocio, por tal motivo, este estándar, desarrolla un papel decisivo al momento de desarrollar los planes de contingencias tecnológicos, referentes al Plan de Continuidad Operacional.

### 2.5.3. ISO 27002

La norma ISO 27002 es un conjunto de buenas prácticas para el desarrollo de un sistema de gestión seguridad de información SGSI. La base de la norma fue inicialmente un documento divulgado por el gobierno del Reino Unido, que se convirtió en un estándar "adecuado" en el año 1995, cuando fue re-publicada por BSI según BS 7799. Fue hasta el año 2000 donde se volvió a publicar, en esta ocasión, por la ISO, como ISO 17799. Una nueva versión de ésta apareció en el año 2005, junto con una nueva publicación, la norma ISO 27001 (DIRECTORIO ISO 27000, 2013).

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

1) Política de Seguridad de la Información.

2) Organización de la Seguridad de la Información.

3) Gestión de Activos de Información.

4) Seguridad de los Recursos Humanos.

5) Seguridad Física y Ambiental.

6) Gestión de las Comunicaciones y Operaciones.

7) Control de Accesos.

8) Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.

9) Gestión de Incidentes en la Seguridad de la Información.

10) Gestión de Continuidad del Negocio.

11) Cumplimiento.

Para el presente trabajo de investigación, se considera de importancia en la norma la parte centrada en Gestión de la Continuidad de Negocio, en el cual se integran aspectos de seguridad de la información de la Gestión de la Continuidad de Negocio. Este dominio tiene el propósito de equilibrar la operación del negocio y salvaguardar los procesos críticos ante catástrofes y fallas menores en los sistemas de información. Con esto se asegura el restablecimiento oportuno.

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

**Incluir la seguridad de la información en el proceso de Gestión de Continuidad del Negocio.** Las actividades relacionadas a esta fase son (ISO 27002: 2005):

- Alcanzar los riesgos de la organización, identificar y priorizar, los procesos críticos.
- Asemejar los activos participantes en los procesos críticos.
- Entender el impacto que tendrían las interrupciones del Negocio.
- Evaluar la contratación de seguros adecuados.
- Evaluar la implementación de controles adicionales a la prevención.
- Identificar recursos financieros, organizacionales y técnicos.
- Tener asegurada la seguridad de los empleados en las instalaciones.
- Tener desarrollados y documentados los planes
- Realizar pruebas y actualizaciones a los planes.

- Asegurar la incorporación de la gestión de continuidad a los procesos de la organización. Asignar personal responsable.

**Elaboración del análisis de riesgo.** Basa su desarrollo en reconocer los sucesos que pueden producir una dificultad en los procesos del negocio, igual que su posibilidad de impacto. Para cumplir con el objetivo de esta sección se deben realizar las siguientes tareas (ISO 27002: 2005):

- Reconocer todos los eventos.
- Realizar una evaluación del riesgo determinando la probabilidad e impacto del evento.
- Desarrollar un plan basándose en los resultados del Análisis de Riesgos.
- Tener definida una estrategia.

**Desarrollar planes de continuidad del negocio incluyendo aspectos de seguridad de la información.** En esta etapa, se definen procedimientos de emergencia y pactos sobre las responsabilidades. Algunos otros puntos que se consideran en esta fase son (ISO 27002: 2005):

- Reconocimiento de pérdidas aceptables de información y productos.
- Desarrollo de procedimientos que puedan lograr la recuperación y reconstrucción de las operaciones del negocio, dependencias internas y externas.
- Documentación de procedimientos.

- Capacitación del personal del área de tecnologías de información para desenvolver la capacidad de realizar los procedimientos.
- Tener en el personal el desarrollo y mantenimiento de los planes para su conocimiento.

**Alinearse al marco referencial para la planeación de continuidad del negocio.** Se consideran las siguientes tareas para el desarrollo de esta fase (ISO 27002: 2005):

- Circunstancias para impulsar los planes y las tareas a ejecutar antes de la activación.
- Definición y detalle de las tareas que deben ejecutarse tras la ocurrencia de una ocurrencia.
- Procedimiento para asegurar un respaldo de información.
- Tener fechas de mantenimiento y actualización.
- Desarrollo de tareas para efectuar la capacitación.
- Definir las responsabilidades de las personas.
- Recursos críticos necesarios.

**Prueba, mantenimiento y actualización de los Planes de Continuidad del Negocio.** Es necesario desarrollar pruebas a los Planes de Continuidad con el fin de tener verificada su vigencia y su eficiencia dentro de la organización. Para este punto deben considerarse algunas actividades importantes (ISO 27002: 2005):

- Tener definidos escenarios.
- Simulacros de diferentes niveles con participación de empleados.

- Desarrollar pruebas de Recuperación en un lugar alterativo.
- Pruebas de servicios de proveedores en los sitios alternos.

El desarrollo de esta norma, y que se considera un estándar, está orientado en su mayoría a la información, por lo que puede ser de gran ayuda para el Plan de Continuidad de Negocio al momento de tomar en cuenta la continuidad de la seguridad que la información debe tener.

### 2.5.4. ISO 22301

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

- Definir de manera más concreta los objetivos, seguimiento del desempeño y de los indicadores.
- Mayor participación de la Dirección.
- Planificación y preparación más cuidadosas de recursos requeridos para el aseguramiento de la continuidad de negocio.

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

- **Contexto de la organización:** Determinar temas internos y externos que son relevantes para el propósito de la organización y que afectan su habilidad de alcanzar los resultados esperados de su SGCN. Identificar el alcance del SGCN, tomando en cuenta los objetivos estratégicos de la organización, sus productos y servicios claves, su tolerancia al riesgo y cualquier obligación reglamentaria, contractual o de sus partes interesadas, también forma parte de esta cláusula (ISO 22301: 2012).
- **Liderazgo:** La alta dirección debe demostrar un compromiso continuo con el SGCN, a través de su liderazgo y acciones. La dirección puede crear un ambiente en el cual distintos miembros del personal estén completamente involucrados y el sistema de gestión pueda funcionar de manera eficaz en sinergia con los objetivos de la organización. Una tarea clave es designar un coordinador/líder que se encargará de gestionar y supervisar el proceso de elaboración e implementación del plan de continuidad de negocio, e incluso, si la inversión lo permite y en función del tamaño de la organización y el alcance del plan, es recomendable asignar personal adicional y constituir un equipo de continuidad de negocio (ISO 22301: 2012).
- **Planificación:** Esta es una etapa crítica en la que se establecen objetivos estratégicos y principios para la orientación del SGCN en su totalidad. Los objetivos del SGCN

son una expresión del propósito de la organización para el tratamiento de los riesgos identificados y/o para cumplir con los requisitos de las necesidades de la organización (ISO 22301: 2012).

- **Soporte:** La gestión diaria de un sistema de gestión de la continuidad de negocio, se basa en el uso de recursos apropiados para cada actividad. Estos recursos incluyen personal competente en base a formaciones y servicios de soporte, toma de conciencia y comunicación pertinentes (y demostrables), esto debe ser apoyado por información documentada adecuadamente gestionada. Las comunicaciones, tanto internas como externas, deben ser consideradas en esta área, incluyendo su formato, contenido y el momento oportuno de estas comunicaciones. Los requisitos para la creación, actualización y control de la información documentada, también se especifican en esta cláusula (ISO 22301: 2012).
- **Evaluación del desempeño:** Una vez que el SGCN se ha implementado, la norma ISO 22301 requiere un permanente seguimiento del sistema, así como revisiones periódicas para mejorar su operación (ISO 22301: 2012).
- **Mejora:** La mejora continua puede ser definida como todas las acciones, realizadas a lo largo de la organización, para aumentar la eficacia (cumplir objetivos) y la eficiencia (proporción costo/beneficio óptima) de los procesos y controles

de seguridad para brindar más beneficios a la organización y a sus partes interesadas. Una organización puede mejorar continuamente la eficacia de su sistema de gestión a través del uso de la política de continuidad de negocio, los objetivos, los resultados de auditorías, el análisis de eventos controlados, los indicadores, las acciones correctivas y preventivas y la revisión por la dirección (ISO 22301: 2012).

En conclusión ISO 22301 no en gran medida diferente a la norma BS 25999 en la mayoría de los aspectos que se encuentran relacionados y ligados a la continuidad del negocio, como el análisis del impacto (BIA) y la estrategia o la planificación. Las principales diferencias se encuentran en la parte de gestión por parte de la norma ISO 22301, ya que se enfoca al desarrollo y comprensión de los requisitos, el establecimiento de los objetivos de manera más concreta y en la medición continua del desempeño. Por tal motivo, motiva una participación más elevada y una mejor comprensión por parte de la Gerencia, que, al mismo tiempo, contribuirá con la aceptación más generalizada de esta norma, como ISO 27001, ISO 9001 o ISO 14001.

# CAPÍTULO III

# DIAGNÓSTICO SITUACIONAL DE LAS EMPRESAS EN EL PERÚ Y AREQUIPA

En el presente capítulo, se realizará un diagnóstico situacional básico de los sectores productivos, y las empresas en el Perú y en Arequipa.

## 3.1. INTRODUCCIÓN

En la actualidad, se vienen presentando grandes cambios en los comportamientos de los sectores productivos de las empresas en el Perú y en Arequipa. Por tal motivo, se considera necesario conocer cómo se vienen dando y cuál es la tendencia.

Las cifras económicas globales y las estructuras económicas resultan de interés para el presente trabajo de investigación, debido a que la metodología propuesta tiene como aplicación directa todas estas organizaciones. La ejecución e implementación del Sistema de Continuidad del Negocio, indudablemente, requiere el uso de recursos financieros, humanos y tecnológicos; en un nivel que debe ser determinado por las necesidades y capacidades propias de cada empresa.

Los recursos tecnológicos tienen una importancia considerable; ya que en muchos casos son estos sistemas integrados que permiten el

funcionamiento y también la recuperación de procesos importantes en las organizaciones. Por esa razón, analizar como viene siendo usada la tecnología, y que capacidad de conocimiento tienen las empresas permitirá saber la facilidad que tendrán para implementar un SGCN.

Es necesario conocer si las empresas en Perú y especialmente en la ciudad de Arequipa, están en la capacidad y tienen la oportunidad para poder desarrollar la metodología y lograr los beneficios expuestos.

## 3.2. SECTORES PRODUCTIVOS EN AREQUIPA

### 3.2.1. SECTOR AGROPECUARIO

El sector agropecuario registró una caída de 2,2 por ciento, asociada al indicador negativo del sub-sector agrícola (-4.2 por ciento). El subsector agrícola, explica su contracción, en los menores niveles de producción de alfalfa (-4,0 por ciento), ajo (-63,3 por ciento), maíz chala (-15,0 por ciento), vid (-16,1 por ciento), entre los principales; por efecto de las menores cosechas zonales (factor clima).

La actividad pecuaria resultó semejante al período comparativo, entre los cultivos que mostraron un crecimiento se encuentran: carne de ave (1,4 por ciento), huevos (0,6 por ciento), además de carne de vacuno (2,3 por ciento), porcino (8,4 por ciento) y en menor medida de ovino (1,8 por ciento) y caprino (6,7 por ciento).

El avance de la presente campaña de siembras 2013/2014 mostró algunos desfases por el factor clima, determinando una superficie

acumulada de 36 785 hectáreas, con los principales cultivos, superficie inferior en 2,4 por ciento a igual período de la campaña anterior; resultado de las menores extensiones que reportaron los cultivos ají páprika (-78,0 por ciento), principalmente, además de alfalfa (-15,8 por ciento) y zapallo (-19,5 por ciento) y en menor medida de trigo (-13,2 por ciento) y vid (-100,0 por ciento), (BCR, pág. 5, 2014).

**Tabla 4 – Superficie Sembrada (en Hectáreas)**

| | Campaña agricola 2/ | | Variación | |
|---|---|---|---|---|
| | 2012/2013 | 2013/2014 | Absoluta | Porcentual |
| Ají páprika | 1 177 | 259 | - 918 | -78,0 |
| Ajo | 109 | 293 | 184 | 168,8 |
| Alfalfa | 3 877 | 3 263 | - 614 | -15,8 |
| Arroz | 19 839 | 19 995 | 156 | 0,8 |
| Arveja Grano verde | 654 | 795 | 141 | 21,6 |
| Caña de azúcar | 4 | 48 | 44 | 1016,3 |
| Cebolla | 2 978 | 2 703 | - 275 | -9,2 |
| Frijol grano seco | 101 | 162 | 61 | 60,4 |
| Maíz Chalero | 4 927 | 5 242 | 315 | 6,4 |
| Maíz choclo | 118 | 246 | 128 | 108,5 |
| Olivo | 0 | 1 | 1 | n.d. |
| Papa | 2 536 | 2 649 | 113 | 4,5 |
| Tomate | 303 | 310 | 7 | 2,3 |
| Trigo | 167 | 145 | - 22 | -13,2 |
| Vid | 71 | 0 | - 71 | -100,0 |
| Zapallo | 837 | 674 | - 163 | -19,5 |
| **Total** | **37 698** | **36 785** | **- 913** | **-2,4** |

Fuente: Gerencia regional de agricultura y riego – Arequipa. Elaboración: BCRP, sucursal Arequipa. Departamento de estudios económicos.

### 3.2.2. SECTOR PESCA

El valor del sector pesquero cayó 16,9 por ciento, debido a la nula actividad industrial.

La falta del recurso anchoveta en la zona fue determinante en la actividad pesquera, siendo esta vez, compensada, en cierta medida por la mayor extracción de especies marinas tanto de pescados como de mariscos, para la línea de consumo humano directo (82,4 por ciento), lo que dinamizó la línea de fresco (84,0 por ciento) y de congelado (70,1 por ciento), (BCR: pág. 6, 2014).

### 3.2.3. SECTOR MINERÍA

El valor de la actividad minera creció 9,7 por ciento, impulsado por los mayores volúmenes producidos de cobre (16,6 por ciento), además de plata (7,1 por ciento), plomo (2,0 por ciento), zinc (25,9 por ciento) y molibdeno (77,2 por ciento). (BCR: pág. 7, 2014).

**Tabla 5 – Variación % real respecto a similar periodo del año anterior**

| Mineral | Estructura Porcentual 2012 2/ | Enero | | | |
|---|---|---|---|---|---|
| | | 2013 | 2014 | Var.% | Contribución 3/ |
| Cobre (TMF) | 74,1 | 19 498 | 22 740 | 16,6 | 12,1 |
| Oro (KGF) | 16,9 | 1 144 | 898 | -21,5 | -3,6 |
| Plata (KGF) | 5,3 | 20 840 | 22 326 | 7,1 | 0,4 |
| Plomo (TMF) | 1,9 | 852 | 869 | 2,0 | 0,0 |
| Zinc (TMF) | 1,3 | 1 166 | 1 468 | 25,9 | 0,4 |
| Molibdeno (TMF) | 0,4 | 289 | 512 | 77,2 | 0,3 |
| **SECTOR MINERIA 2/** | **100,0** | | | **9,7** | **9,7** |

Fuente: Ministerio de Energía y Minas. Elaboración: BCRP, sucursal Arequipa, departamento de estudios económicos.

### 3.3. DEMANDA INTERNA DE AREQUIPA

El consumo final privado creció en 5,0%, en el primer trimestre de 2014, sustentado por los mayores ingresos de las familias como consecuencia del incremento en el empleo (1,9%), y la mejora en el ingreso promedio de los trabajadores (4,8%). El incremento del consumo se reflejó en el mayor gasto nominal de los hogares en alimentos y bebidas como: carne (8,2%); leche, queso y huevos (7,6%); frutas (12,5%); pescado (10,0%); y alimentos preparados consumidos dentro del hogar (18,5%), principalmente. (INEI: pág. 2 2014).

El gasto de consumo final del gobierno registró un crecimiento de 12,9%. A precios corrientes el gasto en remuneraciones y bienes y servicios se incrementó en 13,0% y 19,8% respectivamente.

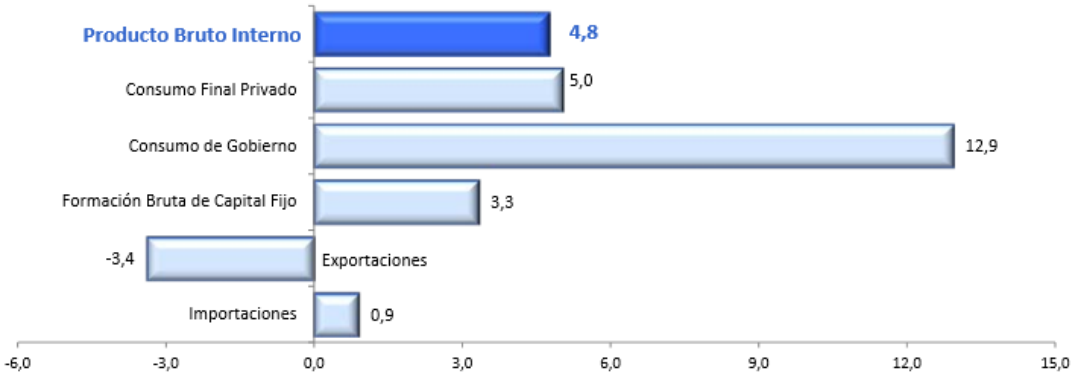
La inversión en capital fijo creció 3,3%, explicado por la mayor demanda de nuevas construcciones (5,3%) y adquisiciones de maquinaria y equipo (1,1%) principalmente de origen nacional que creció en 4,7%, las compras de maquinaria y equipo de origen importado se contrajeron en 0,6%.

Las exportaciones de bienes y servicios disminuyeron en 3,4% a precios constantes, principalmente debido a los menores envíos al exterior de nuestros productos tradicionales, principalmente mineros. El valor nominal de las exportaciones de mineral de oro, mineral de cobre y cobre refinado, disminuyó en 42,3%, 5,8% y 21%, respectivamente, la exportación de gas natural decreció en 36,3% y la gasolina bajó en 13,4%. Sin embargo, aumentaron las exportaciones de harina de recursos hidrobiológicos (154,6%), pescados y mariscos congelados y

refrigerados (44,5%), mineral de zinc (15,1%) y prendas de vestir textiles, excepto prendas de cuero y de piel (9,3%).

Las importaciones de bienes y servicios, a precios constantes, aumentaron en 0,9%, principalmente por las mayores compras de bienes de consumo. En el siguiente gráfico, se muestra el Producto Bruto Interno por componentes del gasto y la variación porcentual del índice de volumen físico respecto al mismo periodo del año anterior (año base 2007).

**Gráfica n° 1 – PBI por componentes del Gasto**




FUENTE: INEI, boletin trimestral, (Perú 2009).

## 3.4. INFORMACIÓN GENERAL DEL MERCADO DE AREQUIPA 2014

El PBI de Arequipa creció 11% en el 2013 y en el año 2014 se calculó un crecimiento de 9.2%.

Los sectores de la construcción y agricultura impulsaron el crecimiento económico de la región Arequipa. Para este año se espera la recuperación de la exportación en minería.

El crecimiento de la economía de Arequipa en el 2013 ha registrado tal nivel de dinamismo que habría llegado a duplicar el Producto Bruto Interno (PBI) del país, según datos del Instituto Peruano de Economía (IPE).

El Índice Compuesto de Actividad Económica (ICAE) para la región Arequipa, elaborado por el IPE, señala que la economía arequipeña creció 11.0% en el 2013 (su proyección para el PBI del Perú en el año pasado es de 5.1%).

Además, el reporte estima que para el 2014 la región siga creciendo a tasas altas de 9.2% (el estimado del IPE para la economía nacional es de 6% este año).

En la minería ha habido una desaceleración de producción de oro y cobre. (INSTITUTO PERUANO DE ECONOMIA. 2014).

### 3.4.1. PERSPECTIVAS

En cuanto a las perspectivas económicas para este año en Arequipa, su PBI también sería impulsado por el dinamismo del sector construcción y el moderado crecimiento de la agricultura, lo que redundará en mejores expectativas de generación de puestos de trabajo.

Principalmente se espera una recuperación de las exportaciones mineras, debido a que hay algunos proyectos relacionados al cobre que están en etapa de ampliación, y esto se apoya un poco con la recuperación del precio del cobre. Sin embargo, existen problemas

sociales con un proyecto de 1300 millones de dólares y 18 años de operaciones, que representa el proyecto minero más importante de la región Arequipa viene con problemas sociales debido a que los pobladores de la zona reclaman que se hará mal uso de sus recursos naturales. Esto podría generar el miedo a la inversión en la región.

## 3.5. DEMANDA GLOBAL

El Producto Bruto Interno (PBI) del primer trimestre de 2014 con nuevo año base 2007, muestra que la economía peruana registró un crecimiento de 4,8% respecto a similar periodo del año anterior, sustentado en la evolución favorable de las actividades de servicios (6,0%), trasformación (3,7%) y extractivas (3,5%).

Incidió en este resultado el dinamismo de la demanda interna que creció en 5,8%, debido al buen desempeño mostrado por el consumo final privado 5,0%, el consumo del gobierno 12,9% y la inversión en capital fijo 3,3%.

Las importaciones crecieron en 0,9% principalmente por las compras al exterior de bienes de consumo no duraderos, y en menor medida de bienes intermedios. (INEI pág. 1. 2014)

## 3.6. OFERTA GLOBAL

Las exportaciones de bienes y servicios disminuyeron en3,4%, reflejando principalmente, el menor dinamismo delas economías de nuestros principales socios comerciales como China que creció en el trimestre a un ritmo más lento que el mostrado hace año y medio,

incidiendo en las cotizaciones de nuestros principales productos tradicionales, y Estados Unidos cuya economía se estancó.

La oferta y demanda global de la economía se expandió en 3,9%, mostrando el menor ritmo registrado en el mismo periodo desde el año 2010.

El PBI desestacionalizado en el primer trimestre del 2014 creció en 0,3% respecto al trimestre inmediato anterior. En la siguiente tabla, se muestra la oferta y demanda global trimestral, con la variación porcentual del índice de volumen físico respecto al mismo periodo del año anterior. (Año base 2007). Nota: la estimación al trimestre de 2014 ha sido elaborada con información disponible al 15-05-2014.

**Tabla 6 – Variación % real respecto a similar periodo del año anterior**

| Oferta y Demanda Global | 2013/2012 | | | | | 2014/2013 |
|---|---|---|---|---|---|---|
| | I Trim. | II Trim. | III Trim. | IV Trim. | Año | I Trim. |
| **Producto Bruto Interno** | **4,5** | **6,3** | **5,3** | **6,9** | **5,8** | **4,8** |
| Extractivas | 0,8 | 3,6 | 4,1 | 8,1 | 4,1 | 3,5 |
| Transformación | 4,3 | 8,5 | 5,3 | 8,6 | 6,8 | 3,7 |
| Servicios | 5,7 | 6,4 | 6,0 | 6,4 | 6,1 | 6,0 |
| **Importaciones** | **7,4** | **4,5** | **-0,5** | **-2,2** | **2,1** | **0,9** |
| **Oferta y Demanda Global** | **5,2** | **5,9** | **3,9** | **4,8** | **4,9** | **3,9** |
| **Demanda Interna** | **10,7** | **7,3** | **5,0** | **6,4** | **7,2** | **5,8** |
| Consumo Final Privado | 5,0 | 5,3 | 5,1 | 5,9 | 5,3 | 5,0 |
| Consumo de Gobierno | 8,0 | 7,8 | 5,9 | 5,2 | 6,7 | 12,9 |
| Formación Bruta de Capital | 25,9 | 11,0 | 4,3 | 8,0 | 11,5 | 4,8 |
| Formación Bruta de Capital Fijo | 7,2 | 10,1 | 3,2 | 1,6 | 5,3 | 3,3 |
| **Exportaciones** | **-11,3** | **0,7** | **0,1** | **-1,1** | **-3,1** | **-3,4** |

Fuente: Base de datos del INEI, Informe Técnico PBI 2014.

## 3.7. ESTRUCTURA ECONÓMICA

### 3.7.1. INFORMACIÓN DEL MERCADO

Durante los tres primeros trimestres del año la economía habría crecido 2,8 por ciento, por debajo del 5,3 por ciento observado durante el mismo periodo de 2013.

El menor ritmo de crecimiento habría estado en gran parte asociado a los sectores no primarios, con una contribución de 1,9 puntos porcentuales a la desaceleración, con respecto al mismo periodo de 2013. El menor crecimiento de estos sectores se habría debido al empeoramiento de las condiciones externas (sobretodo el deterioro de los términos de intercambio) y las expectativas menos optimistas de los agentes económicos.

Adicionalmente, diversos choques de oferta habrían afectado a la economía, con mayor intensidad sobre los sectores primarios. Para los siguientes dos años, se prevé una mejora en las condiciones que impactaron negativamente en la evolución de algunos de los sectores primarios, lo que conjuntamente con la reversión esperada de las expectativas y las mayores exportaciones significaría un mayor impulso en la actividad económica.

La lenta recuperación de las economías desarrolladas, la desaceleración de las economías emergentes y el deterioro de los términos de intercambio en los últimos dos años, han sido los factores externos que han acentuado la dinámica de un ciclo económico débil. En el ámbito interno, la ocurrencia de una serie de factores de oferta

de carácter transitorio, junto a un menor dinamismo del gasto público afectó también negativamente las expectativas de los agentes económicos, y con ello el ritmo de crecimiento de la inversión privada. En este contexto, la demanda interna habría crecido 2,9 por ciento en los primeros nueve meses del año, resultado menor al registrado en el mismo periodo de 2013. Esta menor expansión es consistente con un menor gasto privado, que pasó de 6,6 por ciento en el periodo enero-setiembre de 2013 a 2,6 por ciento en el mismo periodo de 2014, y público, que habría crecido 4,6 por ciento en los primeros nueve meses del año respecto al 10,7 por ciento en el mismo periodo del año anterior. (BCR: pág. 33. 2014)

### 3.7.2. GASTO PÚBLICO

En el primer trimestre de 2014, el gasto de consumo final del gobierno a precios constantes de 2007, se incrementó en 12,9% respecto al mismo periodo del año anterior.

El gasto de consumo final del gobierno a precios corrientes, ascendió a 15 mil 771 millones de nuevos soles, lo que significó un crecimiento de 14,6%, respecto al mismo periodo del año anterior. Este nivel de gasto se explica por los incrementos de bienes y servicios (19,8%), y personal y obligaciones sociales (13,0%), (INEI pág. 2014)

Los sectores del Gobierno Nacional que presentaron una variación positiva en sus gastos de remuneraciones y bienes y servicios a valores corrientes fueron: Presidencia del Consejo de Ministros, Interior, Economía y Finanzas, Ministerio Público, Defensa y Poder

Judicial, Educación y Salud. El crecimiento en remuneraciones es explicado principalmente por el aumento de gastos en retribuciones y complementos en efectivo (13,6%), y contribuciones a la seguridad social (5,3%).

Los Gobiernos Regionales que incrementaron sus gastos en remuneraciones fueron: Ica, Amazonas, Huánuco, Piura, Tacna, Ucayali y Lima, principalmente. Asimismo, los gastos en bienes y servicios aumentaron, debido al mayor gasto en la asignación de los proyectos: camino departamental con mantenimiento vial; instituciones educativas con condiciones para el cumplimiento de horas lectivas normadas; niños con CRED (Control de Crecimiento y Desarrollo) completo según edad; niños con vacuna completa y atención en hospitalización.

### 3.7.3. EXPORTACIONES E IMPORTACIONES

En el primer trimestre de 2014, las exportaciones de bienes y servicios a precios constantes de 2007, registraron un decrecimiento de -3,4% respecto al mismo periodo del año anterior.

A precios corrientes, las exportaciones alcanzaron los 30 mil 957 millones de nuevos soles, registrando un decrecimiento de -1,1% respecto al primer trimestre del 2013, esta evolución negativa es resultado de la menor demanda externa por nuestros productos mineros, principalmente. (INEI pág. 6. 2014)

En el primer trimestre del año 2014, las importaciones de bienes y servicios a precios constantes de 2007, registraron un incremento de 0,9% respecto a similar periodo del año anterior.

El valor corriente de las importaciones de bienes y servicios ascendió a 34 mil 462 millones de nuevos soles, registrando un incremento de 9,7% respecto al primer trimestre del año anterior.

### 3.7.4. AHORRO E INVERSIÓN

La importancia del ahorro en la economía surge por el impacto de la elección inter temporal entre consumo presente y consumo futuro en el bienestar de los agentes y por la estrecha relación entre ahorro e inversión. La escasez de capital es reflejo de un déficit en cuenta corriente y es necesario aplicar políticas adecuadas para recuperar el nivel de ahorro y corregir el déficit (Bosworth, 1993). El sistema financiero en nuestro país ha experimentado una serie de cambios y un crecimiento considerable en los últimos años. Por ejemplo, en el 2006 los depósitos en la banca múltiple (conjunto de empresas bancarias privadas) fueron de 103538 millones de nuevos soles y hasta el 2012 estos depósitos han crecido en promedio 15.96%.

La dolarización es una de las características básicas del sistema financiero en el Perú. El fortalecimiento de la moneda nacional, gracias a políticas monetarias no discrecionales, ha incentivado a los usuarios a apostar por el ahorro en soles y generando una tendencia decreciente de la dolarización. En el 2001, el 74% de los depósitos totales era en moneda extranjera, luego de casi una década el

promedio de dolarización de los depósitos cayó más de 10%. Las tasas de interés pasivas del mercado reflejan este incentivo; en marzo de este año las tasas promedio para depósitos de ahorro y a plazo en soles superaban a las de moneda extranjera en 0.1% y 2.83% respectivamente.

La diferencia entre estos dos tipos de ahorro es que el primero permite depositar y retirar dinero cuando uno lo desee; por el contrario el depósito a plazo tiene el objetivo de generar intereses en un periodo de tiempo determinado y se dividen en plazo fijo, renovable e indefinido. Estos dos tipos de depósitos han experimentado una tendencia ascendente en la última década, el primero una tasa de crecimiento promedio (2006-2012) igual a 26.52% y los depósitos a plazo un 32.05%. Finalmente, aunque todavía son necesarias ciertas reformas para potencializar aún más el crecimiento del ahorro en nuestro sistema financiero es innegable que el usuario apuesta cada vez más por nuestra moneda nacional y por un mercado más formal. (IPE INSTITUTO PERUANO DE ECONOMIA. 2014)

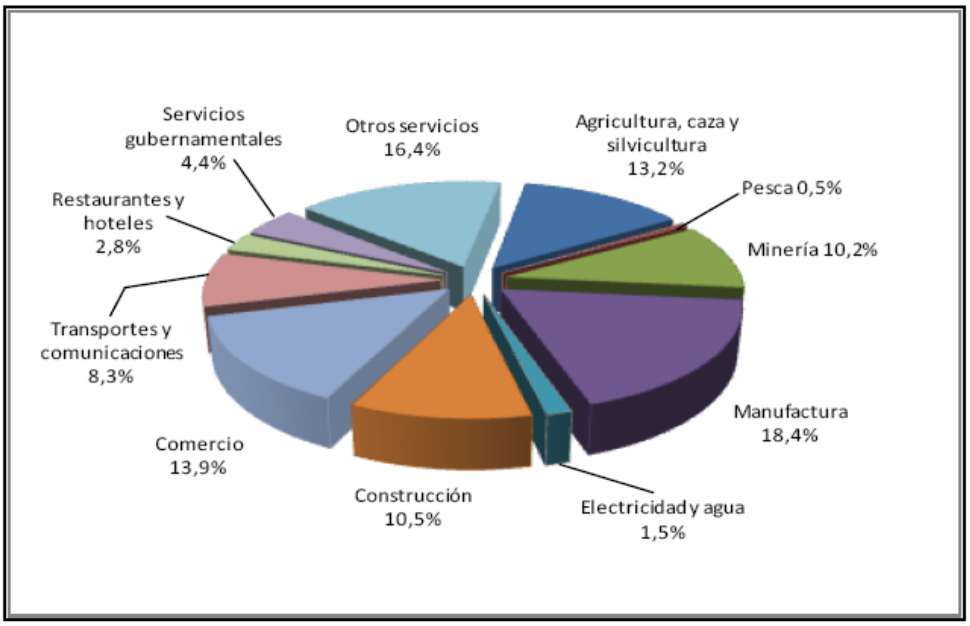
## 3.8. ECONOMÍA ACTUAL DEL MERCADO AREQUIPEÑO

Para el abogado arequipeño Mauricio Chabaneix, presidente de la Cámara de Comercio e Industria de Arequipa, fundada en 1887, un año antes que la Cámara de Comercio de Lima, mientras que la economía nacional se ha desacelerado, Arequipa creció 10,2% en 2013, el doble que el PBI del país, tres puntos más incluso que el crecimiento

económico de China en el mismo periodo. “Esperamos que el anuncio de mega obras de infraestructura, como el Gaseoducto Andino del Sur, los proyectos mineros y Majes-Siguas II, que ubicarán el crecimiento de Arequipa en un potencial máximo de 14,7% para 2014, obligue a las grandes empresas inmobiliarias a mirar Arequipa con más interés”. Chabaneix espera que el sector construcción siga liderando el dinamismo de la economía, tal como los últimos cinco años.

No obstante, este año, Arequipa, con una variedad de áreas productivas, así como una importante actividad exportadora, en la que destaca la exportación de productos mineros y agroindustriales, retrocedió al tercer lugar en el Índice de Competitividad Regional del Instituto Peruano de Economía (IPE), quedando desplazada por Moquegua. Según este ranking, Arequipa ocupa el segundo lugar en el pilar de salud e infraestructura, así como el tercero en entorno económico y mercado laboral. Pero retrocede al cuarto lugar en educación, así como el puesto 22 en calidad de las instituciones, debido a la percepción de corrupción, la falta de transparencia en la rendición de cuentas, la baja ejecución del presupuesto público y altos niveles de criminalidad y corrupción que se perciben. (CAMARA DE COMERCIO E INDUSTRIA AREQUIPÁ. 2014)

**Gráfica n° 2 – Estructura de la economía en Arequipa**




Fuente: INEI – Dirección Nacional de cuentas nacionales. Elaboración: GRTE – Observatorio Socio Económico laboral (OSEL) Arequipa

## 3.9. ANÁLISIS DE LA TECNOLOGÍA

Tecnología es la aplicación de un conjunto de conocimientos y habilidades para las cuales el hombre usa su razonamiento, con un claro objetivo: conseguir una solución que permita al ser humano desde resolver un problema determinado hasta el lograr satisfacer una necesidad en un ámbito concreto.

Nuestra vida cotidiana se desarrolla casi en todo momento con la participación de los diversos recursos tecnológicos. La presencia de la tecnología es tal y ha formado parte del desarrollo humano de manera tan estrecha que la hemos integrado en casi todos los aspectos de

nuestras vidas, hasta el punto de dejar de percatarnos de su presencia. En la actualidad, posiblemente las imágenes que de manera más inmediata acuden a nuestra mente al hablar de tecnología son las de los más recientes y espectaculares artificios electrónicos: computadoras, teléfonos celulares, dispositivos portátiles con conexión a Internet, etcétera. Hoy los avances tecnológicos son particularmente notables en el campo de la informática y las telecomunicaciones, tiempo atrás podíamos notarlos en la electrónica, la mecánica, la química, la biología y en distintas áreas de la ciencia, hoy podemos decir que son un elemento indispensable en la evolución del hombre y la sociedad. Hay que tener en cuenta que, debemos de hacer buen uso de la tecnología, ya que, abusar de ella podría traer consecuencias graves en general.

Sin duda alguna, la ciencia y la tecnología han tenido impacto en la sociedad, pues se han marcado tendencias, modas y sucesos trascendentes en diferentes países, con lo que ese ha marcado el rumbo de la historia y la influencia en las ideologías de los diferentes pueblos. Dicho impacto ha afectado en forma positiva y negativa en los acontecimientos sociales en el desarrollo y evolución de toda la humanidad.

Referente a los efectos positivos en nuestro entorno social, la ciencia ha tenido grandes logros como los avances médicos para la cura de enfermedades por medio del descubrimiento de vacunas y nuevos tratamientos, así como la investigación y desarrollo de nuevos medicamentos. En el campo de la industria y comercio se han creado nuevos modelos para optimizar los procesos productivos basados en la

planificación estratégica y nuevas técnicas de administración La tecnología ha aportado grandes beneficios a l ser humano, desde la invención de aparatos y dispositivos para la detección y diagnóstico de enfermedades, en la rama de la medicina, la creación y mejoramiento de herramientas o accesorios que son útiles para simplificar el trabajo en hogar, sobre todo después de incorporar la energía eléctrica como medio elemental para satisfacer necesidades.

Partiendo de dicha acepción nos encontraríamos con que dentro del "saco" de la tecnología se pueden incluir un amplio número de modalidades o disciplinas tales como la informática, la robótica, la domótica, la neumática, la electrónica, la urbótica o la inmótica, entre otras muchas más.

La tecnología está presente en todos los ámbitos de la vida cotidiana. De una forma u otra, casi todas las actividades que realizamos a lo largo del día implican la utilización de algún dispositivo tecnológico. No extinto a todo ello nos encontramos en la coyuntura del avance de la tecnología en lo referido al sistema de sistema de gestión de continuidad del negocio, cuyas fases integradas en la norma La norma ISO 22301, ayudan a ayudar a las organizaciones a minimizar el riesgo de este tipo de interrupciones, estas fases están ordenadas y contenidas en la norma señalada y orienta a la gestión adecuada de los recursos en forma casi integra para facilitar su desarrollo y contención ante riesgos no planeados.

Es de notar que esta norma es relativamente desconocida en la región dada su coyuntura y acceso. La norma ISO 22301 es casi desconocida en caso factual ha sido admitida tan solo en contadas organizaciones en el Perú, sin perder el espíritu de la norma de ser esta misma de carácter voluntaria conforma un aspecto en su desarrollo de tecnología contenida a su aplicación. Sin embargo, las empresas reguladas por la SBS se encuentran obligadas a tener actividades de continuidad del negocio; por una resolución que resuelve implementar el riesgo operacional en las empresas financieras (Ver Anexo 09); y que en su contenido se encuentra la continuidad del negocio. Asimismo, la SBS emitió una Circular donde establece requerimientos mínimos para la Continuidad del Negocio (Ver Anexo 10). La SBS realiza auditorías para verificar el cumplimiento de la resolución; y existen sanciones y multas en caso de incumplimiento.

# CAPÍTULO IV

# DESARROLLO DE LA METODOLOGÍA PARA LA IMPLEMENTACIÓN DE UN SGCN

En el siguiente capítulo, se presenta el desarrollo de la metodología que se propone para la implementación de un Sistema de Gestión de Continuidad del Negocio; que se realiza considerando como base los requerimientos de la norma ISO 22301:2012, y adicionando las fortalezas de normas que evalúan la misma función.

## 4.1. INTRODUCCIÓN

Dentro de las funciones de una compañía, se considera muy beneficioso evaluar las diferentes situaciones que podrían interrumpir los procesos más importantes; para contar con un plan alternativo que asegure la continuidad de las actividades y evite pérdidas de tiempo, dinero y prestigio.

Es por eso que los Planes de Continuidad, denominados planes de contingencia en sus orígenes, están asociados a grandes compañías, donde se exige el mínimo tiempo de reacción ante cualquier evento que interrumpa sus servicios. Pero la realidad es diferente, ya que se ha comprobado que cualquier compañía puede sufrir un incidente que afecte su continuidad; y dependiendo de la preparación y como se

maneje dicho problema, es que las consecuencias pueden ser más o menos graves.

Esta metodología busca definir las actividades necesarias para poder implementar un SGCN (cumpliendo con los requerimientos de la norma ISO 22301:2012); proporcionando plantillas y ejemplos que permitan a cualquier organización usar esta metodología para cumplir con la función de continuidad de las operaciones; evaluando que procesos son más críticos en impacto financiero y operacional, para evitar las pérdidas más considerables.

## 4.2. ALCANCE DE LA METODOLOGÍA

La presente metodología expone una secuencia de pasos detallados y secuenciales que buscan poder desarrollar un Sistema de Gestión de Continuidad del Negocio (SGCN), incluyendo los requerimientos de la norma ISO 22301:2012 “Seguridad de la Sociedad: Sistemas de Continuidad del Negocio – Requisitos”.

La metodología propuesta, puede ser aplicada a cualquier tipo de organización, y se puede desarrollar en una gran compañía, o en una pequeña empresa, aunque lógicamente el tiempo, esfuerzo y el presupuesto a emplear variaran sensiblemente de acuerdo al requerimiento particular de cada caso; y al nivel de necesidad y utilidad que se identifique que tiene el Sistema para con la organización.

## 4.3. OBJETIVOS DE LA METODOLOGÍA

La utilidad de la metodología se basa en el hecho de que existe poca información sobre la gestión de la continuidad del negocio y su gran importancia. Esta investigación se resume en un conjunto de actividades y tareas detalladas, que contiene todas las fortalezas de los diferentes métodos y recomendaciones de diferentes normas y estudios realizados sobre el tema. Se considera que los principales objetivos son:

- Difundir la gran importancia y utilidad del desarrollo de un Sistema de Gestión de Continuidad del Negocio para hacer frente a eventualidades que interrumpan las operaciones en una organización.
- Desarrollar la metodología completa sobre la Gestión de Continuidad del Negocio, donde se muestre detalladamente cada fase que compone el Plan.
- Definir de forma sencilla y clara, cada una de las actividades a desarrollar para las fases establecidas anteriormente.
- Presentar ejemplos y plantillas que ayuden a entender cómo se desarrollan las tareas y actividades de la metodología.

## 4.4. ANTECEDENTES

Debido a la gran competitividad entre las empresas que existe en la actualidad, los negocios operan a una velocidad muy alta; lo cual hace que un incidente de unas pocas horas de duración pueda tener un

impacto muy elevado en la imagen y resultados de la organización que lo sufra.

Esta situación hace que se cree la exigencia de que las organizaciones estén preparadas para afrontar múltiples amenazas que afecten su operatividad y como consecuencia, la continuidad del negocio. Diferentes eventos sísmicos como el terremoto de Pisco del año 2007, o los atentados terroristas que se sufría en el país, como por ejemplo el atentado de Miraflores de 1992 (daño 183 casas, 63 automóviles y 400 negocios); vienen a sumarse a sucesos que afectan a la comunidad y a las organizaciones. En especial en nuestro país, debido a que nos localizamos en el "Círculo de Fuego del Océano Pacífico", que concentra el 85% de la actividad sísmica mundial.

Sin embargo, en muchas ocasiones, no es necesario un desastre de dimensiones parecidas para poner en peligro no sólo la buena marcha de las operaciones, sino su supervivencia. Eventos menores como el corte de fluido eléctrico puede conducir a la inoperatividad e inutilización de elementos importantes que permitan cumplir con las funciones de la organización.

### 4.4.1. TIPOS DE INCIDENTES

No sólo debe considerarse para este estudio las catástrofes ambientales como incendios, o inundaciones que pueden causar grandes daños. Otros tipos de eventos pueden suscitarse, como los que se describen a continuación:

- Incidentes serios a los sistemas, como delitos cibernéticos, pérdida de información, robo de información, errores en los sistemas.
- Daños en servicios e infraestructura, falta de servicio eléctrico y de agua, fallos en las comunicaciones.
- Fallas en los equipos y en la maquinaria, incluyendo problemas en las fuentes de alimentación, en equipos críticos de la compañía.
- Daños deliberados como actos de terrorismo y sabotaje, guerras, robos, huelgas, manifestaciones, etc.

Todo evento que afecte a la empresa, tiene una repercusión diferente según el tipo de organización, su tamaño y su área de actividad.

En ocasiones, y como ya ha sucedido, estos accidentes pueden hasta lograr que se cierre la organización afectada. Se debe tomar en consideración las siguientes cifras:

- Un 43% de empresas, después de un accidente grave no podrán seguir operando, viéndose obligadas a cerrar.
- Un 80% de las mencionadas anteriormente, tendrán que hacerlo en menos de 13 meses.
- El 53% de clientes de las empresas que cerraron no recuperarán las pérdidas causadas por los daños derivados.
- Un 50% estarán obligadas a cerrar antes de cinco años pasado el desastre.

Se puede pensar que los daños inmediatos aparentemente son la pérdida de todos los beneficios por la interrupción de los procesos críticos de la organización y la parada de la actividad puntual. Sin embargo no son los únicos que se pueden identificar.

Otros efectos derivados y que pueden causar un daño considerable que es difícil de medir, son la pérdida de reputación con los clientes, o la pérdida de ventajas competitivas con otras organizaciones.

## 4.5. PLAN DE CONTINUIDAD DEL NEGOCIO

El Plan de Continuidad del Negocio (PCN), es el resultado de un estudio de una organización y diferentes elementos de la misma, que tiene como objetivo prepararla para continuar operando durante y después de un desastre. El PCN es el documento más importante del Sistema de Gestión de Continuidad del Negocio, ya que resume todas las fases y acciones necesarias para implementar el sistema. Este resultado, contiene procedimientos y lineamientos para lograr la recuperación y restablecimiento de procesos interrumpidos, incluidos los recursos empleados y afectados, para regresar al estado de operación normal, en un tiempo prudencial.

El desarrollo del Plan incluye varias fases, que tienen como base el estudio de los procesos que componen a la organización. En este estudio, se debe determinar la importancia de cada proceso para la organización, y priorizar cuales son críticos; para establecer una política de recuperación ante un desastre. Para cada proceso, se identifican los impactos potenciales.

El PCN tiene como diferencia a los planes de contingencia el alcance; ya que los PCN se orientan al mantenimiento del negocio de la organización, con lo que se prioriza las operaciones de negocio críticas; que son las que generan mayor impacto; y que son fundamentales para continuar correctamente con la operatividad integral de la empresa.

El Plan de Continuidad, debe lograr disminuir la cantidad y magnitud de decisiones que se tomen durante una situación de desastre y en un tiempo tan corto que los errores puedan resultar mayores. Este documento definirá, organizará, clasificara y documentará los riesgos, responsabilidades, políticas y procedimientos; así como algunos acuerdos y procedimientos que se definen con entidades internas y externas.

Se debe recurrir al Plan de Continuidad cuando existe una situación de emergencia; y donde las medidas de seguridad esenciales hayan fallado. Se considera las siguientes ventajas con la implementación de un PCN:

**Ventajas:**

- Define y califica los diferentes eventos que podrían generarse sobre la normal. operatividad de las operaciones en una organización; evaluando el impacto financiero, humano y de prestigio afectado.
- Permite conocer tiempos críticos para lograr la recuperación de los procesos y regresar a la situación normal, sin comprometer al negocio.

- Minimiza las pérdidas para la organización en caso de desastre.
- Evalúa los activos para priorizar su protección.
- Se convierte en una ventaja competitiva frente a la competencia.

## 4.6. ASPECTOS GENERALES DEL SGCN

Debido a que la presente metodología busca incluir los requerimientos de la norma ISO 22301:2012, deben considerarse algunos aspectos antes de desarrollar las actividades propias de Continuidad del Negocio.

Es una ventaja que la organización ya cuente con un planeamiento previo, que esté claramente definida la misión y visión, el contexto de la organización, sus objetivos estrategias y metas. Alguna de esta información es requerida para el desarrollo del SGCN, así que se detallará cuál debe incluirse y documentarse para cumplir con los requisitos de la norma.

### 4.6.1. DETERMINACIÓN DEL CONTEXTO DE LA ORGANIZACIÓN

Para tener definido claramente este aspecto, pueden desarrollarse varios documentos, por ejemplo un Procedimiento de identificación de Requerimientos, definir una Política de Continuidad del Negocio. El contexto también se define cuando se desarrolla el Análisis de Impacto del Negocio y en la Evaluación de Riesgos, que se detallará en posteriormente.

### 4.6.2. ALCANCE DEL SGCN Y EXCLUSIONES

Se debe documentar al inicio del proyecto de continuidad del negocio el alcance del sistema, definiendo claramente a que partes de la

organización se aplicarán los planes de continuidad, en base a las necesidades identificadas y pretensiones de la organización. También pueden excluirse del desarrollo del Sistema, algunas áreas muy particulares de la organización; de ser así, debe explicarse el motivo.

Estos aspectos pueden fusionarse con la Política de Continuidad del Negocio.

### 4.6.3. POLÍTICA Y OBJETIVOS

Este es el documento central en que la alta dirección debe indicar lo que quiere lograr con el SGCN y cómo lo controlarán. La alta dirección es la única responsable de la aprobación de este documento, ya que la demás documentación puede ser aprobada por administradores de nivel inferior.

Las organizaciones pequeñas y medianas por lo general incluyen aquí el alcance y objetivos del SGCN, mientras que otras más complejas, habitualmente, confeccionan documentos separados.

Es necesario definir claramente los objetivos del SGCN, que se establecen para todo el Sistema, no par actividades específicas.

### 4.6.4. CAPACITACIÓN Y CONCIENCIACIÓN

Debe desarrollarse planes de capacitación y concienciación sobre el SGCN. Esto debe ser desarrollado por la persona responsable de la continuidad del negocio y el área de recursos humanos. Es recomendable tener un registro de competencias del personal, y registrar los resultados.

### 4.6.5. COMUNICACIÓN CON LAS PARTES INTERESADAS

Se puede hacer de diferente tipo de formas, correo electrónico, postal, teléfono, etc. Es requerido por la norma documentar este tipo de comunicación; que puede hacerse de manera sencilla, guardando copias de los mensajes de correos, cartas, etc. Si es vía telefónica, puede hacerse y archivar una nota de acuerdo a reglas predefinidas.

### 4.6.6. PROCEDMIENTO PARA CONTROL DE DOCUMENTACIÓN

Debe hacerse un documento independiente, de 2 o 3 páginas, donde se tenga un procedimiento que identifique toda la documentación que se tiene y permita identificarla con facilidad. Si se tiene implementada alguna otra norma (ISO 9001, ISO 14001), puede utilizarse el mismo procedimiento.

### 4.6.7. CONTRATOS Y ACUERDOS DE NIVELES DE SERVICIO

Es crucial que sus proveedores y socios externos reaccionen de la misma manera cuando ocurre un incidente. Debe desarrollarse una plantilla con los requerimientos mínimos de continuidad del negocio que deben incluirse en cada contrato firmado.

### 4.6.8. PROCEDIMIENTO, PROGRAMA Y RESULTADO DE AUDITORÍA INTERNA

Habitualmente el procedimiento para auditoría interna es un procedimiento independiente que puede tener entre 2 y 3 páginas y que debe ser confeccionado antes de que comience la auditoría interna. En cuanto al procedimiento para control de documentos, un

procedimiento para auditoría interna puede ser utilizado para cualquier sistema de gestión.

Un programa de auditoría interna podría ser un simple documento de una página que describa cuándo se llevará a cabo cada auditoría y quién la realizará. Los resultados de la auditoría interna se documentan a través del informe de auditoría interna; este informe debe incluir todas las no conformidades y las observaciones.

Para poder desarrollar y controlar un programa de auditorías internas basadas en el sistema, se recomienda tomar en cuenta las siguientes consideraciones:

- Crear un Programa de auditorías internas basadas en las necesidades reales, la propia empresa debe establecer criterios, sin obligación de establecer plazos rígidos.
- Usar listas de chequeo de auditoría interna diseñadas exclusivamente para el sistema, que incluyan los requerimientos del sistema y de la norma.
- Llevar a cabo auditorías de los procesos en forma vertical, que no evalúan específicamente los procesos sino las áreas y departamentos.

Los proyectos relacionados con auditar el Sistema de Gestión de Continuidad de Negocio se realizan con el propósito de revisar la adecuada implantación y buen funcionamiento tanto de los controles de seguridad y procedimientos del Sistema de Gestión.

Según la norma, definimos que para realizar un estudio inicial del estado del sistema debemos realizar los siguientes pasos:

- Revisión del contexto.
- Revisión del liderazgo.
- Revisión del soporte.
- Revisión del BIA y análisis de riesgos.
- Revisión de las estrategias.
- Revisión de pruebas.
- Revisión de la evaluación del desempeño.
- Revisión de la mejora.

Como resultado, se debe preparar un informe de auditoría que considere:

- Establecerá un Plan de Auditoría
- Contexto de la organización.
- Liderazgo.
- Planificación.
- Soporte.
- Operación.
- Evaluación del desempeño.
- Mejora.
- Informe.
- Acciones correctivas.

Para evaluar estos aspectos, se puede realizar listas de chequeo, entrevistas, encuestas relacionadas al Sistema, por ejemplo, puede hacerse una Lista de Chequeo “Documentación del Sistema”, donde se evalúa si se cuenta con los formatos obligatorios (Ver Anexo 08).

### 4.6.9. RESULTADOS DE LA REVISIÓN POR PARTE DE DIRECCIÓN

Estos registros se presentan, normalmente, bajo la forma de actas de reunión y deben incluir todo el material tratado durante la reunión de la dirección, como también todas las decisiones que se tomaron. Estas actas pueden ser en papel o en formato digital.

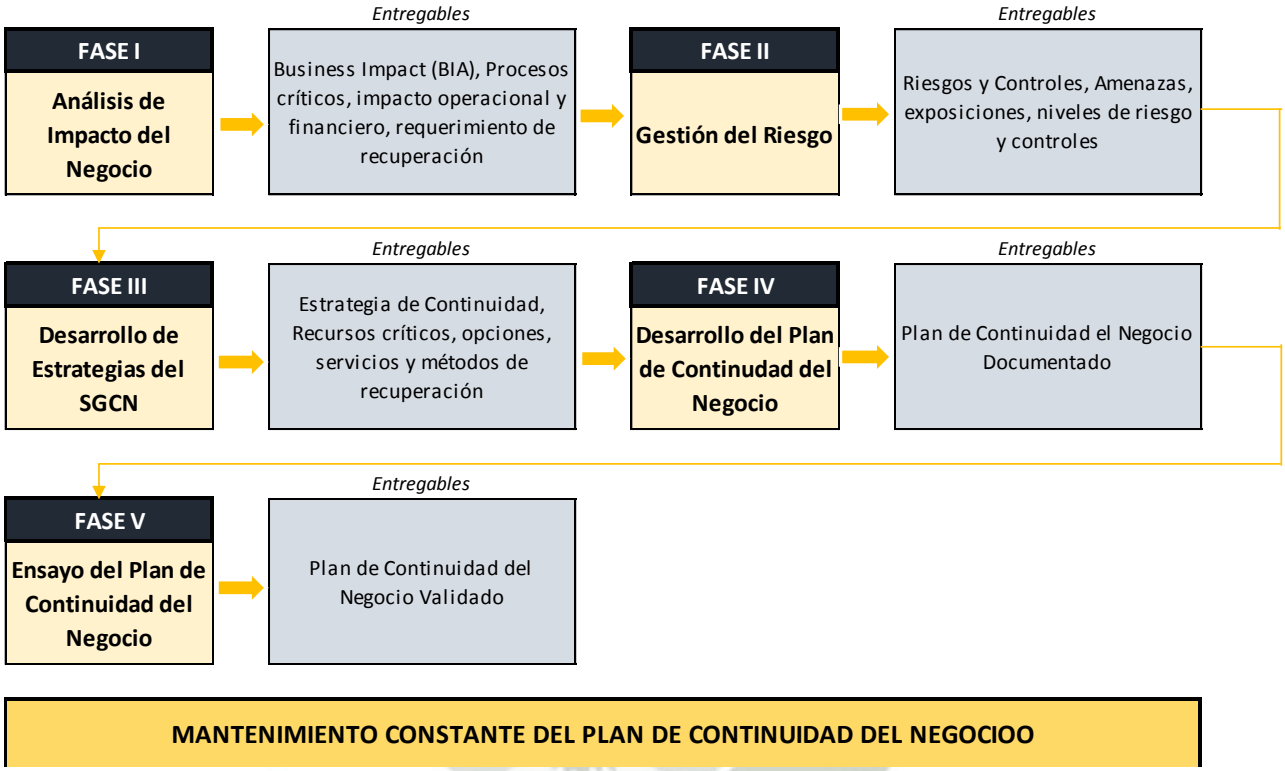
## 4.7. DESARROLLO DE LAS FASES Y ACTIVIDADES DEL SISTEMA DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO

Para desarrollar el Plan e implementar el Sistema de Continuidad del Negocio, es necesario empezar conociendo a la organización. Sus productos, servicios, objetivos empresariales, procesos, recursos, etc.

Como ejemplo, no es igual un Plan de Continuidad para una empresa que brinda un servicio de Internet que para una que fabrica zapatos. El objetivo, sin importar el rubro, es seguir dando atención a los clientes, actividades y mantener los procesos operativos. La diferencia entre los dos tipos de empresa es que se generarán diferentes prioridades de recuperación ante un incidente grave. Por eso es que la presente metodología se puede aplicar a cualquier tipo de organización; ya que se define las fases y actividades detalladas; el desarrollo de cada una, se puede adecuar a cualquier giro de negocio.

Como objetivo principal de un Plan de Continuidad se tiene el definir un mapa de acciones que reduzca la toma de decisiones, restaure servicios en el tiempo adecuado; minimizando costos y aumentando la efectividad. Podemos dividir un Plan de Continuidad de Negocio en estas Fases:

**Ilustración 3 – Fases del Sistema de Gestión de Continuidad del Negocio**




Fuente: Normas y estándares de continuidad estudiados. Elaboración Propia.

Es necesario, para la implementación del sistema; aplicar todas las fases mencionadas considerando todas las áreas de la organización. Con esto, se logra obtener información integrada y que tenga en su evaluación todos los aspectos que puedan generarse en cualquier sistema, proceso, recurso que tenga la empresa y que afecten a la continuidad del negocio.

Esta labor se vuelve complicada, por lo cual algunos pasos específicos (como el BIA, la evaluación de riesgos o la elaboración de los Planes de Continuidad) pueden desarrollarse por área para facilitar la recopilación de datos. Esta decisión depende del tipo de empresa y de que tan compleja sea su estructura.

La asignación de recursos para el desarrollo del SGCN, también varía en función al tamaño y tipo de organización. Generalmente se recomienda asignar la labor a un grupo seleccionado dentro de la organización, y que tenga representantes de cada área. Algunas organizaciones que tienen esta función como una obligación (Financieras), crean un área dentro de la empresa, el área de Continuidad del Negocio. Este órgano, se encarga de desarrollar el Sistema, de mantenerlo y actualizarlo. La forma de desarrollar todo el sistema depende del tamaño y tipo de organización, y de la necesidad inmediata y beneficios que se consideren por los responsables.

A continuación, se detalla una pequeña descripción de las Fases que se definieron para la metodología propuesta:

**Tabla 7– Descripción de las Fases del SGCN**

| FASE DEL SGCN | DESCRIPCIÓN |
|---|---|
| FASE I | Consiste en identificar procesos fundamentales y relacionados directamente con el giro de negocio (crítico). Se logra evaluar los impactos en la gestión comercial del negocio, en caso de verse interrumpidos. El entregable consiste en un informe describiendo las áreas de negocio críticas para el alcance de la misión de la organización. También requiere determinar cuantitativamente y cualitativamente los impactos económicos y operativos; así como |

| | |
|---|---|
| | la definición de tiempos adecuados para la recuperación de cada proceso. |
| FASE II | En la gestión del riesgo, se requiere una evaluación de amenazas de un evento, identificar las vulnerabilidades presentes, los potenciales impactos; para luego definir y aplicar controles necesarios para prevenir o reducir los riesgos. Para las empresas se puede determinar escenarios de amenazas para los procesos críticos. El entregable es el conjunto de amenazas potenciales evaluadas, con controles que sean específicos a cada situación. |
| FASE III | Busca valorar las alternativas y estrategias de respaldo en función a los resultados anteriores; para seleccionar la más adecuada. Busca corregir vulnerabilidades de los procesos críticos. El entregable es un informe con opciones viables para la recuperación de los procesos críticos, considerando la posibilidad y costo. Este trabajo se puede realizar por cada escenario de amenaza identificado. |
| FASE IV | Con una estrategia de respaldo, es necesario desarrollarla e implementarla. En esta fase se elaboran procedimientos y planes de actuación para las áreas y se organizan los equipos que intervienen. El entregable es un informa con los procedimientos y lineamientos para la recuperación. |
| FASE V | Tiene como objetivo conocer que realmente funciona el Plan y es efectivo. Se define una estrategia de pruebas y se ejecuta, para afinarlo y actualizarlo según los resultados. El entregable son registros llenados para demostrar su realización, así como las acciones correctivas para los ajustes necesarios. |
| MANTENIMIENTO | Busca conseguir un estado de constante preparación, para que las fases anteriores se ejecuten sin dificultad. |

Fuente: Diseño de un sistema de seguridad de información, Naturaleza del PCN, Alberto G. Alexander (2007).

Como se puede observar, el proceso del Sistema de Gestión de Continuidad del Negocio comienza con el BIA (base del análisis); seguido inmediatamente por la Gestión de Riesgo, el desarrollo de las

estrategias, el plan y el ensayo. Es un proceso como se mencionó secuencial, ya que los entregables de cada fase suministran la información requerida por la siguiente (se convierten en insumos). En lo que resta del capítulo, se describe cada una de las fases de la metodología propuesta.

**OTROS ENFOQUES AL PCN:**

Internacionalmente, existe otros enfoques relacionados a la continuidad del negocio, y que guardan cierta estrecha relación y a su vez diferencias con los Planes de Continuidad. A continuación, se describe estos enfoques:

- ***Distaster Recovery Planning (DRP):*** Enfocado a la recuperación de servicios de tecnología de información (TI) y sus recursos.
- ***Business Resumption PLanning (BRP):*** Se encuentra centralizado en la reanudación de procesos de la empresa que se encuentran alterados sólo por una falla en aplicaciones de TI. Utiliza principalmente procedimientos relacionados con el área que se esté trabajando.
- ***Continuity of Operations Planning (COOP):*** Busca recuperar funciones estratégicas de una empresa que se desarrollen dentro de las instalaciones coorporativas.
- ***Contingency Planning (CP):*** Está centrado en poder recuperar servicios y recursos de TI, pasado un evento de dimensiones mayores o interrupción menor. Se aplica específicamente a un

evento y describe procedimientos y lineamientos, estableciendo responsabilidades en áreas internas y alternas.

- ***Emergency Response Planning:*** Tiene como objetivo salvaguardar a los empleados, clientes, público, el ambiente y los activos de la empresa. Lo principal es pasar de un estado de crisis a un estado de control lo más pronto posible.

Todos estos enfoques tienen algo en común, tienen un alcance estrecho y específico. Están centrados en la protección de aspectos específicos de la empresa, no haciendo una evaluación integran e ignorado áreas críticas. Con el SGCN, se logra un enfoque de planeación integrado, que permita proteger a toda la organización y que priorice aquellas que son más vulnerables.

El PCN viene a ser un marco conceptual, que puede integrar el alcance y objetivo de todos los enfoques descritos.

## 4.8. FASE I: ANALISIS DE IMPACTO DEL NEGOCIO (BIA)

El análisis de impacto del negocio, conocido como BIA por sus siglas en inglés (Business Impact Analysis) corresponde a la primera fase del proceso del SGCN. Analiza los impactos financieros y operacionales de un desastre en la organización, sus áreas y sus procesos.

El BIA requiere un análisis bajo dos enfoques, cualitativo y cuantitativo; ya que se necesita para la evaluación financiera (cuantitativo) estudiar las pérdidas monetarias, como pueden ser ventas no realizadas, gastos

adicionales de personal y maquinaria, penalidades contractuales, etc.; que se ocasionan en caso de una interrupción en los procesos. El otro enfoque se desarrolla en la evaluación operacional, que se refiere a daños no monetarios que pueda tener la organización, donde podemos encontrar por ejemplo problemas que afecten la calidad de atención al cliente, el nivel de competitividad o generar daño a la reputación del negocio.

Este análisis, es indispensable para posteriormente definir una estrategia que tenga como objetivo dar continuidad a los procesos críticos de una organización, y posteriormente al resto si es posible.

Para establecer el nivel de criticidad de cada operación, se debe tomar en cuenta cuan dependiente de ella es la organización. En el caso de valoración económica, corresponde cuantificar las pérdidas monetarias involucradas.

En esencia, el BIA detalla la siguiente información:

- Funciones y procesos organizacionales, jerarquizando y priorizando los mismos, para hacerles arreglos específicos en los PCN. Se recomienda no ignorar los procesos que no son considerados críticos, se puede preparar Planes de Recuperación para estos.
- Calcular las consecuencias operacionales y financieras que un evento, que ocasione la interrupción de los procesos, tendría en la organización.

- Estimar y definir los tiempos de recuperación, dad una alteración de procesos clave de la empresa.
- Establecer cuáles son los recursos indispensables para el normal funcionamiento y para un estado de activación del PCN.

El BIA se concluye con un informe que recoge la información más importante del desarrollo de esta fase. Se incluye funciones y procesos críticos, información básica de tiempos de recuperación y recursos requeridos.

### 4.8.1. FORMAS RECOMENDADAS PARA RECOLECCIÓN DE INFORMACIÓN

La recolección de la información, la calidad y veracidad de la misma, representa un punto sumamente importante para poder desarrollar el BIA. Se requiere tener información de las distintas áreas de la compañía, lo cual vuelve esta labor en retadora y compleja. Debe evaluarse, según el tamaño de la empresa, cual es el tiempo que se dedicará a cada técnica de recolección de información. Asimismo, decidir cuál usar para cada requerimiento del BIA, evaluando flexibilidad, tiempo y costo. También entender las necesidades de cada área con el personal y recursos que tienen para establecer un cronograma de actividades que no afecte el normal funcionamiento de la empresa.

A continuación, se presentan tres métodos recomendados y que pueden ser aplicados en cualquier empresa:

**Tabla 8 – Formas de Recolección de Información del BIA**

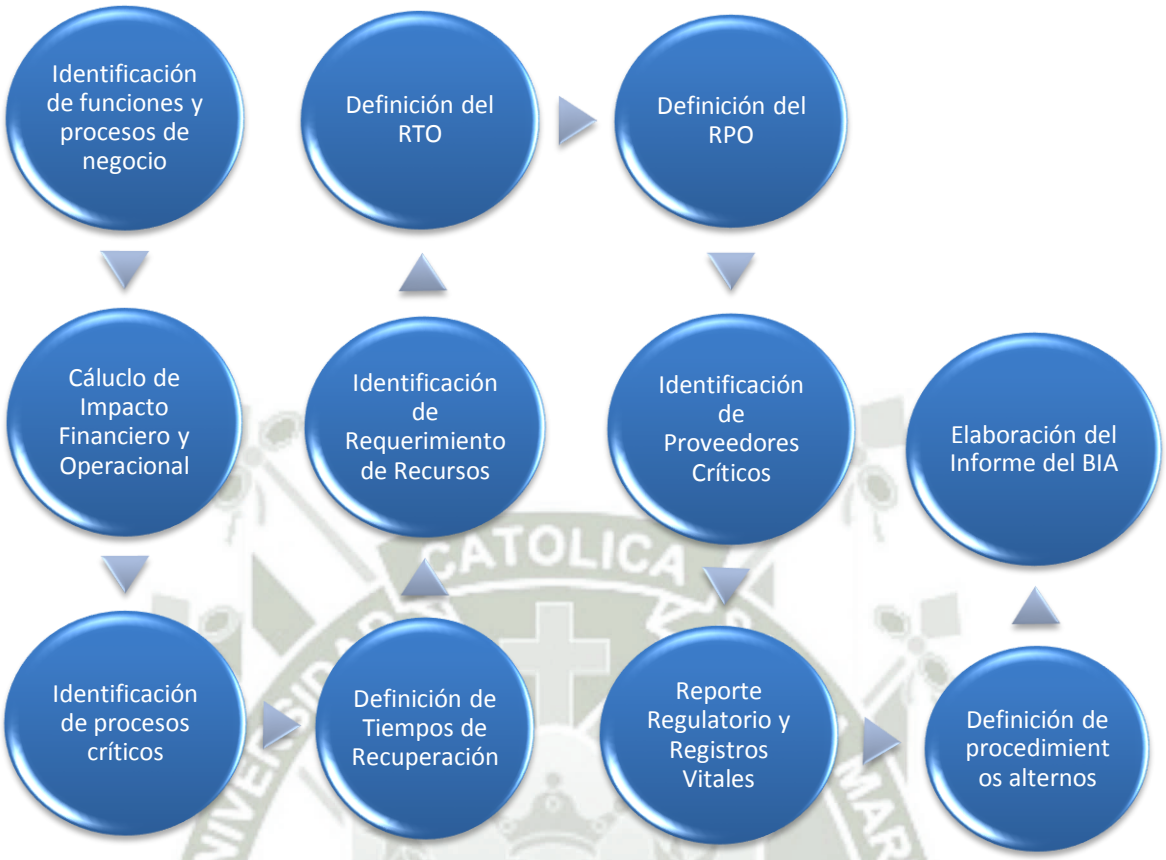
| ENCUESTA | ENTREVISTA | TALLERES |
|---|---|---|
| Conjunto de preguntas enviadas a todas las áreas de la organización. Flexibilidad para el llenado, pero posible falta de precisión y confiabilidad. | Recolección personal confeccionando preguntas para cada sesión, de acuerdo a intereses particulares. Interacción directa minimiza mala interpretación. Por el tiempo invertido puede ser muy costoso. | Grupo de personas trabajando de manera dinámica, y que permite clarificar al punto máximo la información recolectada. |

Fuente: Business Continuity: Best Practices, Técnicas de estudio. Hiles (2004).

### 4.8.2. PROCESO METODOLÓGICO DEL BIA

Para facilitar el entendimiento y desarrollo del BIA, la presente metodología expone una secuencia de pasos interactivos que tienen como objetivo identificar impactos de una interrupción y definir recursos y tiempos de recuperación. En la siguiente ilustración, se muestra los pasos que se definieron para el desarrollo metodológico del BIA:

**Ilustración 4 – Proceso Metodológico del BIA**




Fuente: Normas y estándares de continuidad estudiados. Elaboración Propia.

Como se puede observar, la propuesta para poder realizar un análisis de impacto del negocio (BIA), considera una secuencia de pasos interactivos y relacionados entre sí. A continuación, se hará una descripción de cada actividad con un ejemplo de referencia.

La propuesta es un procedimiento secuencial, cada actividad será necesaria para poder realizar la siguiente.

#### 4.8.2.1. PRIMER ETAPA: IDENTIFICACIÓN DE FUNCIONES Y PROCESOS DE NEGOCIO

Como primer paso para elaborar el BIA, se debe identificar todas las funciones y procesos de negocio que se tengan en la organización. De acuerdo a la estructura de la organización, pueden encontrarse diferentes niveles de funciones y procesos; como ejemplo básico se puede definir esta etapa así:

**Tabla 9 – Funciones del Negocio y Procesos**

| FUNCIONES DEL NEGOCIO | PROCESOS |
|---|---|
| Ventas | Gerencia de órdenes |
| | Informe datos de ventas |
| Marketing | Promoción de productos |
| | Mantenimiento de catálogo |
| Servicio al cliente | Manejo problemas del cliente |
| | Proceso de órdenes |
| Despacho | Empaque de productos |
| | Envío de productos |

Fuente: Diseño de un sistema de seguridad de información, Análisis de Impacto. Alberto G. Alexander (2007).

El propósito de esta actividad es tener identificadas todas las funciones y procesos que apoyan el cumplimiento de la misión, metas y objetivos donde se encuentre el alcance del Sistema. Esta información puede estar contenida en un Mapa de Procesos que tenga la organización; y si no es el caso, es necesario identificarlos. Para todo recaudamiento de información se puede usar cualquier de las formas de recolección de información expuestas anteriormente.

Para completar la información, en la identificación de los procesos, se puede también listar:

- **Estacionalidad Crítica:** Define cada cuanto tiempo el proceso es totalmente necesario que se realice, o con qué frecuencia se realiza regularmente
- **Tiempo máximo de espera:** Cálculo inicial de cuánto tiempo puede paralizarse el proceso sin generar un impacto significativo en el negocio
- **Responsable del proceso:** Identifica directamente a una persona responsable de la ejecución del proceso.
- **Procedimiento alterno:** Identifica la existencia o no de algún procedimiento alterno que ya esté definido en caso de no poder operar normalmente.

#### 4.8.2.2. SEGUNDA ETAPA: EVALUACIÓN DE IMPACTOS FINANCIEROS Y OPERACIONALES

Como siguiente etapa, es necesario evaluar y cuantificar los impactos que puede tener una interrupción en el negocio; definiendo dos perspectivas (financiera y operacional).

**IMPACTOS FINANCIEROS:**

Es necesario cuantificar la magnitud de un impacto que genera la interrupción de un proceso. La medición se realiza por cada proceso identificado.

Para poder realizar esta evaluación, se puede utilizar algún sistema de costeo que tenga la organización; evaluar todas las actividades y recursos que se generan a partir de una operación; las ganancias posibles y reales dejadas de percibir a partir de la interrupción del proceso; o prorratear y distribuir cada operación en función a un porcentaje evaluado y sacado de algún ítem del estado de ganancias y pérdidas. Cada organización particular debe encontrar la mejor manera de cuantificar el impacto financiero.

Luego de haber identificado este valor, se debe establecer una escala de severidad, basada en el valor de pérdida monetaria. Se recomienda utilizar una escala como la siguiente:

- Nivel de Severidad 1: Sin Impacto
- Nivel de Severidad 2: Impacto Bajo
- Nivel de Severidad 3: Impacto Medio
- Nivel de Severidad 4: Impacto Medio Alto
- Nivel de Severidad 5: Impacto Alto

Para definir de qué valor a qué valor se considera un nivel de severidad determinado, se debe establecer la escala en función al tamaño de la empresa; ya que una organización pequeña es más sensible a pérdidas monetarias más bajas comparadas a una gran organización que maneja diferentes flujos económicos.

En la siguiente tabla, se tiene una ilustración de los niveles de severidad de los impactos financieros:

**Tabla 10 – Ilustración Impacto Financiero y Nivel Severidad**

| Función del negocio | Proceso del negocio | Magnitud de pérdida financiera (diaria) | Nivel de Severidad |
|---|---|---|---|
| Ventas | Generación órdenes | S/. 700,000 | 5 |
| | Informes datos ventas | S/. 1100 | 1 |
| Marketing | Promoción productos | S/. 4,000 | 2 |
| | Mantenimiento catálogo | S/. 5,000 | 2 |
| Servicio al cliente | Manejo problemas clientes | S/. 5,000 | 2 |
| | Procesamiento órdenes | S/. 500,000 | 4 |
| Despacho | Empaque producto | S/. 15,000 | 3 |
| | Envío producto | S/. 20,000 | 3 |

Fuente: Elaboración propia.

Los valores son estimados y se definen en base a un estudio y análisis de los responsables y expertos. Se cuantifica para cada proceso un monto en caso de interrupción, por ejemplo para el proceso: Informe datos ventas, se puede considerar costos de incumplimiento, de mal control y manejo de las estrategias de ventas que puede llevar a reflejarse en pérdidas.

**IMPACTOS OPERACIONALES:**

Se evalúa el daño generado por una interrupción por aspectos no cuantificables, aspectos de las operaciones del negocio. Para su medición, se puede usar un esquema de jerarquización cualitativo.

Para una evaluación general, se consideran estos puntos como necesarios en cualquier organización:

- Eficiencia operativa, cliente interno.
- Daños a su reputación e imagen.
- Daño al público o cliente externo.

Para definir una escala de evaluación, se puede usar la misma del impacto financiero (Del 1 al 5); para cada proceso y en considerando los puntos mencionados anteriormente.

En la siguiente tabla se ilustra los impactos operacionales:

**Tabla 11 – Ilustración Impacto Operacional**

| Función del negocio | Proceso del negocio | Jerarquización de impactos operacionales | | |
|---|---|---|---|---|
| | | Cliente interno | Reputación e imagen | Cliente externo |
| Ventas | Generación órdenes | 3 | 3 | 5 |
| | Informes datos ventas | 4 | 2 | 2 |
| Marketing | Promoción productos | 2 | 4 | 4 |
| | Mantenimiento catálogo | 2 | 4 | 3 |
| Servicio al cliente | Manejo problemas clientes | 2 | 3 | 5 |
| | Procesamiento órdenes | 1 | 3 | 3 |
| Despacho | Empaque producto | 2 | 4 | 3 |
| | Envío producto | 4 | 3 | 4 |

Fuente: Elaboración propia.

#### 4.8.2.3. TERCERA ETAPA: IDENTIFICACIÓN DE PROCESOS CRÍTICOS

Utilizando los requerimientos anteriormente usados, se debe definir de los procesos evaluados, cuales se consideran críticos en caso de una

interrupción del negocio; ya que estos serán los objetos de estudio en lo que continua del desarrollo del SGCN. Es importante que para la selección de los procesos críticos, se consideren ambos aspectos.

Se puede definir, según la metodología propuesta, que se realice una suma de todas las evaluaciones:

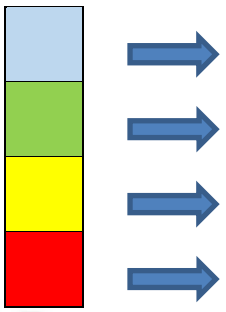
**Tabla 12 – Tabla Ponderación Para Procesos Críticos**

| Función del negocio | Proceso del negocio | Aspectos Evaluados | | | | |
|---|---|---|---|---|---|---|
| | | Cliente interno | Reputación e imagen | Cliente externo | Severidad Financiera | SUMA |
| Ventas | Generación órdenes | 3 | 3 | 5 | 5 | **16** |
| | Informes datos ventas | 4 | 2 | 2 | 1 | **9** |
| Marketing | Promoción productos | 2 | 4 | 4 | 2 | **12** |
| | Mantenimiento catálogo | 2 | 4 | 3 | 2 | **11** |
| Servicio al cliente | Manejo Prob. Cliente | 2 | 3 | 5 | 2 | **12** |
| | Procesamiento órdenes | 1 | 3 | 3 | 4 | **11** |
| Despacho | Empaque producto | 2 | 4 | 3 | 3 | **12** |
| | Envío producto | 4 | 3 | 4 | 3 | **14** |

Fuente: Elaboración propia.

Como se puede observar en la tabla, simplemente se suman todas las evaluaciones y se obtiene un total por cada proceso evaluado. Para definir cuáles vendrían a definirse como los procesos críticos, se realiza esta comparación:

**Ilustración 5 – Escala de Comparacion Para Criticidad Alta**



| CONSIDERACIÓN | SUMA TOTAL |
|---|---|
| **CRITICIDAD MINIMA** | **0 a 3** |
| **CRITICIDAD BAJA** | **4 a 8** |
| **CRITICIDAD MEDIA** | **9 a 13** |
| **CRITICIDAD ALTA** | **14-20** |

Fuente: Elaboración propia.

Como el aspecto financiero tiene una importancia igual o mayor para la mayoría de casos en las empresas, también se realizará la selección de Procesos Críticos en base a este aspecto. Por tal motivo, todos los procesos que contengan una evaluación de 4 o 5 en su Impacto Financiero; se considerarán como Procesos Críticos también.

En resumen, todos los procesos que tengan una Suma de 14 a 20 en su total; o los que tengan 4 o 5 en su Impacto financiero, se considerarán Procesos Críticos, y serán objeto de evaluación para lo que resta del SGCN. Para el ejemplo tenemos:

**Tabla 13 – Jerarquización de Procesos Críticos**

| PROCESOS CRÍTICOS | ASPECTOS EVALUADOS | | | | |
|---|---|---|---|---|---|
| | Cliente interno | Reputación e imagen | Cliente externo | Severidad Financiera | SUMA |
| Generación órdenes | 3 | 3 | 5 | 5 | 16 |
| Envío producto | 4 | 3 | 4 | 3 | 14 |
| Procesamiento órdenes | 1 | 3 | 3 | 4 | 11 |

Fuente: Elaboración propia.

El resultado final es el listado de Proceso Críticos del Negocio, que pueden estar jerarquizados por su importancia. Se resalta en rojo el aspecto por el cual se consideró que es crítico.

Este proceso de evaluación puede variar en función al tipo y necesidades de la empresa. Se puede asignar diferentes escalas, dando mayor importancia al aspecto financiero u operacional.

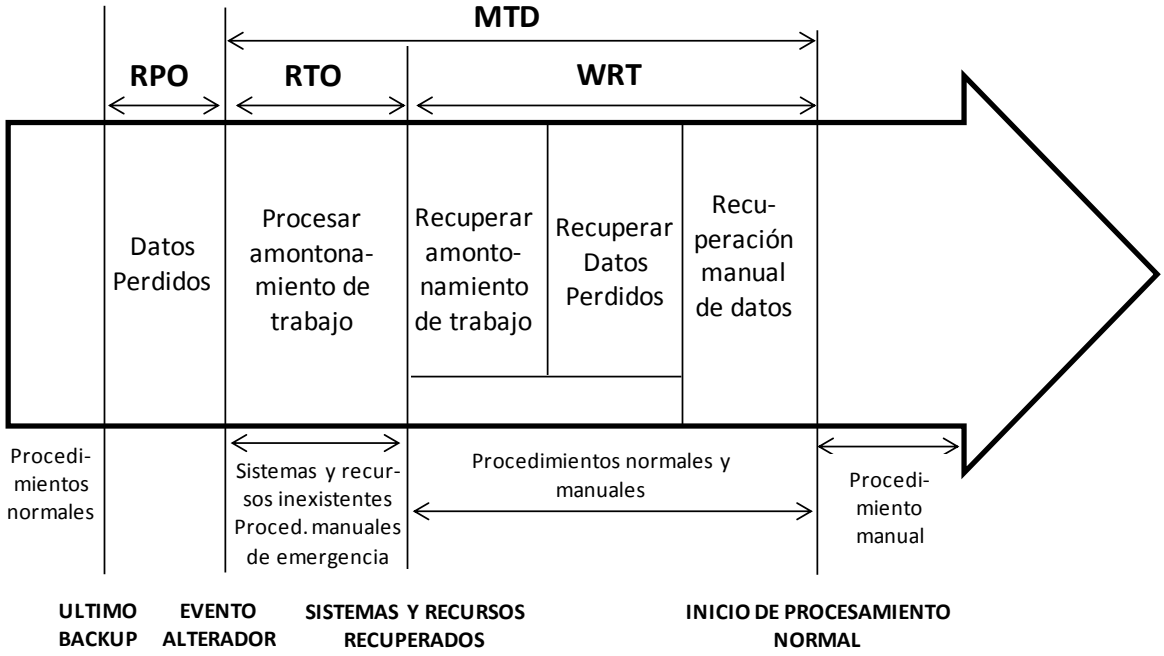
#### 4.8.2.4. CUARTA ETAPA: DEFINICIÓN DE TIEMPOS DE RECUPERACIÓN

Una vez que se ha logrado identificar que procesos son más importantes para la organización, se debe determinar los tiempos en los cuales se tolera, se acepta y se permite la recuperación en caso de una interrupción. Definirlo y entenderlos es un requisito importante para el BIA.

El acumulado de pérdidas suele ir creciendo linealmente a medida que pasan los días y las actividades están interrumpidas. No obstante, a partir de un momento que denominaremos Período Máximo de Interrupción, las pérdidas sufren un aumento significativo y las funciones no podrían ser reasumidas.

Existen varias definiciones y diferentes menciones para los tiempos de recuperación; los que usaremos y que se consideran necesarios son los siguientes:

**Ilustración 6 – Tiempo de Recuperación de un Desastre**




Fuente: Diseño de un sistema de seguridad de información, Análisis de Impacto (BIA). Alberto G. Alexander (2007).

A continuación, se explicará cada término de los Tiempos de Recuperación mencionados:

- **Maximum Tolerable Downtime (MTD):** Representa el periodo máximo de inactividad de un proceso, que puede tolerar la

organización; sin entrar en una crisis financiera y operacional. Dado este valor y las evaluaciones de impacto, se puede establecer una prioridad de recuperación; o una escala ya definida, por ejemplo:

**Tabla 14 – Jerarquización de Procesos Críticos**

| MTD | Prioridad de Recuperación |
|---|---|
| *24 Horas* | 1 |
| *1 a 2 días* | 2 |
| *3 a 5 días* | 3 |
| *6 a más días* | 4 |

Fuente: Elaboración propia.

Definiendo el MTD para cada Proceso Crítico se puede obtener una priorización para la recuperación de procesos; como se muestra en la siguiente tabla, siguiendo con el ejemplo:

**Tabla 15 – Jerarquización de Procesos Críticos**

| PROCESOS CRÍTICOS | MTD | PRIORIDAD |
|---|---|---|
| Generación órdenes | 12 horas | 1 |
| Envío producto | 4 días | 3 |
| Procedimientos órdenes | 2 días | 2 |

Fuente: Elaboración propia.

- **Recovery Point Objective (RPO):** Este tiempo se define como la tolerancia que se puede asignar referida a la pérdida de datos; que se mide con la elaboración del último respaldo (backup) de información y el posible evento de interrupción.

- **Recovery Time Objective (RTO):** Se refiere específicamente a la recuperación de recursos, como sistemas de computación, equipos internos, edificaciones, ambientes e infraestructura. Indica el tiempo que se dispone para lograr la recuperación de estos elementos.

- **Work Return Time (WRT):** Se define como el tiempo entre la recuperación del sistema, y la vuelta total a la normalidad del proceso. Se realiza la búsqueda de todos los datos y las operaciones necesarias para la restauración total.

La suma del RTO y el WRT, serán iguales o menores que las del MTD. En esta etapa, sólo se define el MTD para cada proceso y ayuda a lograr una priorización de recuperación.

#### 4.8.2.5. QUINTA ETAPA: IDENTIFICACIÓN DE REQUERIMIENTOS DE RECURSOS

Dentro de la recuperación de procesos para el mantenimiento de las operaciones, un sistema de tecnología de información o una aplicación puede considerarse muy importante. En esta etapa, debe

identificarse sistemas y aplicaciones que son necesarios para la recuperación de un proceso.

**Tabla 16 – Sistemas de TI y aplicaciones**

| PROCESOS CRÍTICOS | Sistemas de IT críticos y aplicaciones |
|---|---|
| Generación órdenes | Sistema de información al cliente |
| | Sistema entrada de orden |
| | Aplicaciones e-mail |
| | Aplicación EDI |
| Envío producto | Despacho y flete |
| | Sistema de gestión |
| | Sistema entrada de orden |
| Procesamiento órdenes | Sistema entrada ordenes |
| | Gestión sistema inventario |
| | Sistema cobranzas clientes |

Fuente Elaboración propia.

**RECURSO HUMANO:**

Dentro de los recursos necesarios para una interrupción, en algunos procesos si es requerido contar con personal. Mientras mayor sea el tiempo de interrupción, más recursos se deberán gestionar; por tal motivo, para este u otros aspectos, puede hacerse una evaluación considerando diferentes tiempos de paralización (2, 4, 8, 24, 48 horas, 5 días, etc.)

**RECURSOS NO CRÍTICOS DE TECNOLOGÍA DE INFORMACIÓN:**

Se debe evaluar todos aquellos recursos que no son de tecnología de información y que son requeridos. También se recomienda definirlos

por tiempos, ya que la cantidad si es más variable en función a esta condición.

#### 4.8.2.6. SEXTA ETAPA: DETERMINACIÓN DEL RECOVERY TIME OBJECTIVE

Como ya se explicó, el RTO está relacionado con la recuperación de recursos, tanto de TI, como otros que también tengan participación en el proceso. Es el tiempo entre el desastre y la recuperación de recursos transformados. En esta etapa también se debe definir el WRT, que es el tiempo total que se necesita para completar el trabajo interrumpido para regresar al estado de normalidad.

Para esta etapa se debe definir este tiempo por cada sistema y aplicación crítica identificada anteriormente; como se muestra en el siguiente ejemplo:

**Tabla 17 – Sistemas de TI y aplicaciones**

| PROCESOS CRÍTICOS | Sistemas de IT críticos y aplicaciones | RTO | WRT |
|---|---|---|---|
| Generación órdenes | Sistema de información al cliente | 10 h | 2 h |
| | Sistema entrada de orden | 4 h | 8 h |
| | Aplicaciones e-mail | 10 h | 2 h |
| | Aplicación EDI | 9 h | 3 h |

Fuente: Elaboración propia.

#### 4.8.2.7. SÉPTIMA ETAPA: DETERMINACIÓN DEL RECOVERY POINT OBJECTIVE

En el desarrollo del análisis de impacto, también debe determinarse el RPO por cada aplicación. Una manera adecuada de hacerlo es respondiendo a la siguiente pregunta: ¿Cuál es la tolerancia máxima del tiempo que los datos pueden estar perdidos sin afectar el desempeño del sistema?

#### 4.8.2.8. OCTAVA ETAPA: IDENTIFICACIÓN DE PROVEEDORES CRÍTICOS

Es necesario identificar para cada proceso crítico, si existe participación externa; listando los proveedores que intervienen en el desarrollo del proceso y que son realmente importantes para que se lleve a cabo. Debe determinarse en este análisis varios aspectos:

- Nombre de la empresa proveedora.
- Tipo de servicio provisto.
- Si cuentan con un PCN.
- Persona de contacto con el proveedor.
- Datos del proveedor (teléfono, correo, etc.)

#### 4.8.2.9. NOVENA ETAPA: REPORTES REGULATORIOS Y REGISTROS VITALES

**REPORTES REGULATORIOS:**

Para poder asegurar la continuidad de las operaciones, es necesario identificar dentro de la organización, todas aquellas obligaciones que

tiene la empresa con entidades reguladoras, para poder evitar incumplimientos normativos y multas que se generarían en caso de que un evento imposibilite preparar y entregar estos reportes en el tiempo adecuado.

Se requiere la siguiente información:

- Nombre del reporte.
- Entidad a la que se envía.
- Frecuencia.
- Complejidad.
- Tiempo máximo de demora de entrega.

**REGISTROS VITALES:**

Se hace un listado de toda aquella documentación e información importante que se maneje dentro del proceso crítico. Se debe recabar la siguiente información:

- Tipo de Registro (archivo, certificado, contrato, cinta de respaldo, etc.)
- Nombre del Registro Vital.
- Fuente y ubicación.
- Determinar si cuenta con respaldo.
- Ubicación alterna.

#### 4.8.2.10. DÉCIMA ETAPA: IDENTIFICACIÓN DE PROCEDIMIENTOS ALTERNOS

Los procedimientos alternos permiten que los procesos críticos puedan continuar si se presentara una interrupción. La idea es buscar métodos alternos, usualmente operaciones manuales temporales; e identificar aquellos que ya estén establecidos.

#### 4.8.2.11. DÉCIMO PRIMERA ETAPA: INFORME DEL BIA

Para formalizar el proceso del BIA y lograr el requerimiento de comunicación en toda la organización y participación de la alta dirección; se resume todo el desarrollo del análisis de impacto en un informe que se recomienda debe tener los siguientes puntos definidos con claridad:

- Lista de procesos críticos
- Lista de tiempos MTD y su jerarquización
- Lista jerarquizada de sistemas y aplicaciones
- Lista jerarquizada de recursos ajenos a tecnología de información
- Lista de tiempos RTO
- Lista de tiempos RPO
- Lista de procedimientos alternos

## 4.9. FASE II: GESTIÓN DEL RIESGO

Para completar y lograr implementar un SGCN, es importante entender que el desarrollo no debe estar enfocado solamente en la recuperación de instalaciones frente a un incidente, sino contemplar las acciones preventivas correspondientes.

Para este fin, en todo PCN, se debe calcular el riesgo, identificando amenazas que afecten las operaciones; las vulnerabilidades y el grado de exposición. Con esta evaluación, se proponen controles para minimizar el daño del impacto en un desastre.

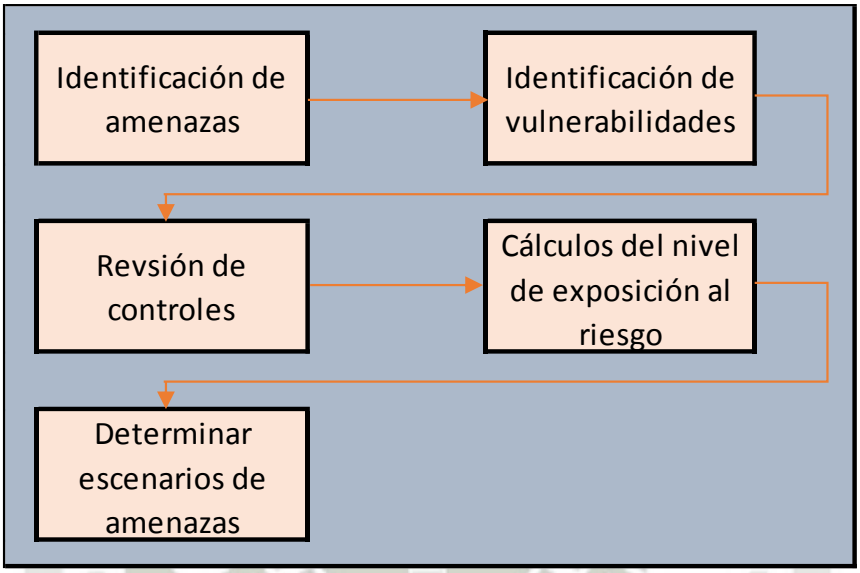
En la metodología propuesta, para la gestión del riesgo, se busca determinar escenarios de amenazas que puedan presentar los procesos críticos; que se usarán con el fin de evaluar estrategias de continuidad y para elaborar posteriormente un plan de reanudación de operaciones.

La gestión de riesgo es una actividad requerida no solo por el SGCN, sino por diferentes actividades y funciones de la organización; y existen diversas organizaciones internacionales que lo regulan (Ver Anexo N° 01).

### 4.9.1. METODOLOGÍA DEL CÁLCULO DEL RIESGO

En la siguiente ilustración, se muestra la metodología que se establece para gestionar el riesgo en la empresa:

**Ilustración 7 – Metodología del Cálculo del Riesgo**




Fuente: Normas y estándares sobre análisis de riesgos estudiados. Elaboración Propia.

#### 4.9.1.1. IDENTIFICACIÓN DE AMENAZAS:

Una amenaza puede definirse como un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus servicios.

A la hora de analizar los riesgos hay que evaluar las distintas amenazas que pueden provenir considerando las fuentes. Dentro de todas se incluyen los agresores malintencionados, las amenazas no intencionadas y los desastres naturales.

La siguiente ilustración clasifica las distintas amenazas y que están relacionadas con la gestión de continuidad del negocio:

**Ilustración 8 – Tipos de Amenazas**


Fuente: Guía de desarrollo de un PCN, Evaluación de Riesgos. Laura del Pino (España, 2007).

Dependiendo de la organización y el proceso analizado, serán aplicables distintos tipos de amenazas. Las amenazas tendrán una ***probabilidad de ocurrencia*** que dependerá de la existencia de una vulnerabilidad que pueda ser explotada, para materializarse en un incidente; y que puede ser calculada.

Se deben identificar todas las amenazas, (ver Anexo N°02) ligadas a continuidad del negocio y evaluar su nivel de riesgo. Para eso se propone la siguiente matriz de riesgo:

**PROBABILIDAD DE RIESGO:**

**Tabla 18 – Probabilidad de Riesgo**

| Probabilidad | Descripción |
|---|---|
| Improbable | No se registra en los últimos 10 años |
| No frecuente | Se presenta una vez de seis a diez años |
| Moderada | Se presenta una vez de dos a cinco años |
| Frecuente | Se presenta una vez al año |
| Muy Frecuente | Se presenta una o más veces en el semestre |

Fuente: Elaboración propia.

**IMPACTO/CONSECUENCIA:**

**Tabla 19 – Impacto de Riesgo**

| Impacto | Descripción |
|---|---|
| No significativo | Tiene un efecto nulo o muy pequeño en la operación. |
| Menor | Afecta parcialmente la operación. Paraliza servicios que no afectan directamente al cliente. |
| Moderado | Operativamente es sostenible, Dificulta o retrasa la operación. Paraliza parcialmente los servicios críticos a clientes. |
| Mayor | Paraliza la atención de servicios críticos a clientes. Pérdida potencial de clientes |
| Catastrófico | Paraliza toda la operación del negocio. |

Fuente: Elaboración propia.

Para poder calcular el nivel de riesgo de cada amenaza, se identifica en que probabilidad puede incidir; y que impacto puede causar. Combinando las dos anotaciones se define el nivel de riesgo.

**NIVEL DE RIESGO:**

**Ilustración 9 – Matriz Nivel de Riesgo**

| | | IMPACTO | | | | |
|---|---|---|---|---|---|---|
| | | No Sign. | Menor | Moderado | Mayor | Catastrófico |
| PROBABILIDAD | Muy Frecuente | A | A | E | E | E |
| | Frecuente | M | A | A | E | E |
| | Moderada | B | M | A | E | E |
| | No frecuente | B | B | M | A | E |
| | Improbable | B | B | M | A | A |

Fuente: Elaboración propia.

Nota: Leyenda: E: Extremo, A: Alto, M: Medio, B: Bajo.

Mediante esta evaluación, ya se puede tomar decisiones sobre el tratamiento de riesgo. Decidir cuáles amenazas se reducirán con controles, cuáles se aceptarán y cuáles se transferirán (aseguradora).

#### 4.9.1.2. IDENTIFICACIÓN DE VULNERABILIDADES:

Las vulnerabilidades son debilidades que pueden ser explotadas para convertir una amenaza en un riesgo real que puede causar daños graves en una compañía. Las vulnerabilidades en sí mismas no causan daño alguno, sino que es una condición o un conjunto de condiciones que pueden permitir a una amenaza afectar a un activo. En el Anexo N°03 se recogen algunos ejemplos de vulnerabilidades.

Para identificar las vulnerabilidades que pueden afectar a una compañía debemos responder a la pregunta: ¿Cómo puede ocurrir una amenaza?

Se termina con un listado de vulnerabilidades, por cada amenaza, que se consideren importantes.

#### 4.9.1.3. REVISIÓN DE CONTROLES ACTUALES:

En esta etapa, se debe evaluar las distintas salvaguardas existentes en la empresa; y que se encuentran funcionando correctamente. Un control en el cual se confía en su eficacia, pero en la práctica no opera bien, es una fuente de posibles vulnerabilidades y aumenta la probabilidad de que las amenazas penetren y hagan daño.

Como resultado se tiene un listado de controles, su estado de funcionamiento, y algunos pequeños controles ligados a las amenazas que puedan instaurarse. (Ver Anexo N°04).

#### 4.9.1.4. CÁLCULO DEL NIVEL DE EXPOSICIÓN AL RIESGO:

En esta actividad, se determina el nivel de exposición. Es otra perspectiva para la evaluación de riesgos que se basa en precisar el grado de severidad de cada potencial amenaza y su cobertura.

El grado de severidad está relacionado al impacto que puede tener una amenaza; y la cobertura se define como el grado de protección y medidas preventivas que tiene la empresa frente a una amenaza en particular.

El grado de severidad se va a definir por cinco puntos:

- MB = Muy baja (0)
- B = Baja (10)
- M = Moderada (40)
- A = Alta (70)
- MA = Muy alta (100)

La exposición al riesgo es calculado con la siguiente fórmula:

$$Exposición\ al\ riesgo = Severidad \times (100\% - \%Cobertura)$$

Para poder identificar todas las amenazas y poder compararlas, se recomienda completarlas en el siguiente cuadro, que permite entender de mejor forma la evaluación realizada.

**Tabla 20 – Nivel de Exposición al Riesgo**

| POTENCIALES AMENAZAS | SEVERIDAD | | | | | COBERTURA | | | | | | EXPOSICION AL RIESGO |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | MB | B | M | A | N/A | 0-19% | 20-39% | 40-59% | 60-79% | 80-99% | 100% | |
| | | | | | | | | | | | | |

Fuente: Elaboración propia.

Como se puede observar en el ejemplo, se asigna el valor al grado de severidad y se ubica la cobertura dentro de los rangos de la tabla; y para la aplicación de la fórmula, se escoge el valor menor del rango definido.

Habiendo definido la exposición del riesgo, se debe empezar a crear escenarios particulares de amenazas que la empresa pudiera tener y que causen daño a las operaciones de la empresa.

#### 4.9.1.5. ESTABLECER ESCENARIOS DE AMENAZAS:

Se elaboran escenarios particulares de riesgos que pudieran presentarse en la organización y se clasifican por niveles y conjuntos que sean probables de presentarse. En la siguiente ilustración, se identifica como ejemplo para una empresa en particular, escenarios de amenazas que se ha evaluado que pueden presentarse. Cada empresa organiza particularmente sus escenarios en base al análisis de cálculo de exposición al riesgo; y la experiencia propia de la empresa.

**Ilustración 10 – Ejemplo escenarios de amenazas**

| |
|---|
| NIVEL 1 |
| • Amenaza para la continuidad de uno o más procesos debido a la pérdida de un recurso único pero crítico en una instalación |
| NIVEL 2 |
| • Amenazas para la continuidad de muchos procesos, por un evento que evita el acceso a una instalación; pero sin daño a recursos críticos |
| NIVEL 3 |
| • Amenaza para la continuidad de varios procesos, por un evento que destruye recursos críticos en una de las instalaciones |
| NIVEL 4 |
| • Amenaza para la continuidad de varios procesos por evento que destruye totalmente una instalación y sus recursos |
| NIVEL 5 |
| • Amenaza para muchos procesos, con pérdidas de instalaciones criticas y pérdida del equipo gerencial. |

Fuente: Diseño de un sistema de seguridad de información, Gestión del Riesgo. Alberto G. Alexander (2007).

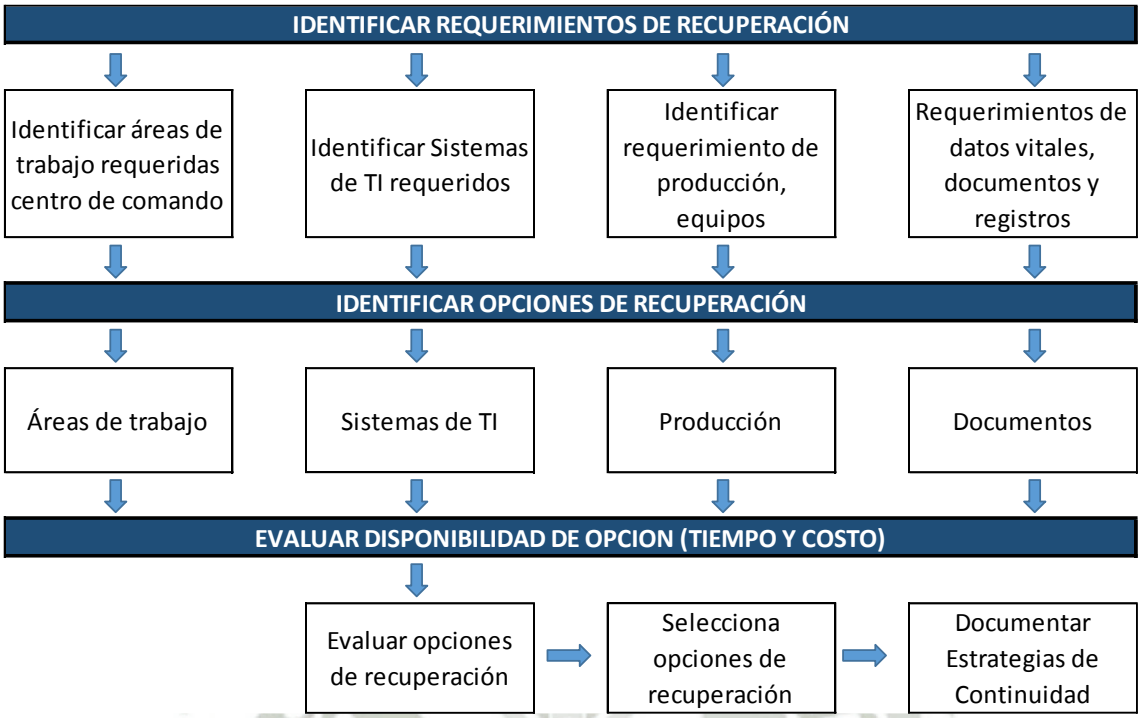
La gestión del riesgo es una parte muy importante del SGCN. Con los escenarios definidos que pueden afectar las operaciones; la empresa es más capaz de invertir el tiempo necesario para jerarquizar sus riesgos. Esta evaluación se basa en sustentar qué operaciones se interrumpirán, dado el grado de seriedad de las amenazas. Como principal objetivo se tiene el de entender a un nivel bastante elevado, que cosas podrían salir mal, y establecer los controles para fortalecer vulnerabilidades y minimizar las posibilidades de que un desastre cause un daño mayor.

## 4.10. FASE III: ESTRATEGIAS DE RESPALDO

En esta fase se deben elegir los métodos alternativos para usarse en el caso de que ocurra un incidente que provoque una interrupción en la empresa. El método seleccionado deberá garantizar la restauración de los procesos afectados en los tiempos determinados por el Análisis de Impacto.

En la siguiente Ilustración, se define las fases y actividades que se recomiendan en la metodología para definir las estrategias de respaldo. Hay que recalcar que toda la información se basa en el BIA.

**Ilustración 11 – Desarrollo Estrategia de Continuidad**




Fuente: Diseño de un sistema de seguridad de información, Estrategias del PCN. Alberto G. Alexander (2007).

- **FASE A: Requerimientos de Recuperación:**

  En esta primera parte, se hace una recolección y organización de información que se obtuvo en el Análisis de Impacto (BIA). Como se puede observar, se identifica áreas de trabajo principales, sistemas de tecnología de información requeridos y que se usarán, requerimientos de producción y equipos que esté relacionados a los requerimientos de información vital y de registros y documentos importantes. Todos estos aspectos son importantes atenderlos para la ejecución de la estrategia de continuidad.

- **FASE B: Opciones de Recuperación:**

  En esta fase, se busca identificar posibles opciones como soluciones a los requerimientos de recuperación. Es decir, se evalúa la disponibilidad y facilidad para la adquisición de los requerimientos mencionados anteriormente. Se hace una evaluación y se menciona específicamente cuáles son estos elementos que van a ser usados y se menciona una lista con aquellos que sean de utilidad.

- **FASE C: Evaluación de Disponibilidad de Tiempo:**

  Se realiza un descarte, eliminando todas aquellas opciones que no cumplan con los tiempos de recuperación que se han definido en el BIA. Estos tiempos vendrían a representar el primer criterio de selección para las estrategias, ya que se considera el más importante.

- **FASE D: Evaluación de Costos:**

  Una vez descartadas las opciones que no cumplan con el tiempo requerido, se hace una evaluación de costos a todas las alternativas que quedaron; para poder seleccionar las más viables y eficaces. Este segundo criterio de selección es más flexible; ya que depende del presupuesto de la empresa y la complejidad de su sistema.

## 4.11. FASE IV: DESARROLLO DEL PLAN DE CONTINUIDAD DEL NEGOCIO

A partir de esta parte, se desarrollará el Plan de Continuidad, que representa el documento que resume todas las actividades anteriores. Es una forma de lograr la comunicación con todas las partes de la

empresa; ya que se presenta en una estructura flexible y que puede ser dirigida a todas las áreas relacionadas al SGCN. Es el resultado de cómo se encuentra actualmente el SGCN. En el plan se define principalmente:

- El personal y la organización del mismo para el Plan.
- Definición de responsabilidades y funciones.
- Relaciones jerárquicas y dependencias de los equipos.
- La definición de los procedimientos de alerta y actuación frente a eventos que logren activar el Plan.
- Actividades a desarrollar ante eventualidades.
- Actividades para la vuelta a la normalidad.

### 4.11.1. LOS EQUIPOS DE TRABAJO

Los equipos designados de emergencia están representados por el personal clave necesario en la activación y desarrollo del Plan de Continuidad. Cada equipo tiene unas funciones y procedimientos que tendrán que desarrollar en las distintas fases del Plan.

La forma en que se organicen y el tamaño del grupo, depende del tipo de estrategia de recuperación, y de la empresa. Asimismo, una persona puede representar a varios grupos, siempre y cuando se cuide que no existan incompatibilidades en las tareas. A continuación se hace un listado de algunos grupos que pueden integrarse para el SGCN:

#### 4.11.1.1. EQUIPO DIRECTOR O COMITÉ DE CRISIS

La principal función del comité es reducir el riesgo y la incertidumbre en la dirección de la situación. Es el encargado de la toma de decisiones en momentos críticos, además de hacer de enlace con la dirección de la compañía, manteniéndoles informados de la situación regularmente.

Las principales tareas y responsabilidades de este comité son:

- Evaluación de la situación.
- Activación del Plan.
- Iniciar con la notificación de los incidentes.
- Supervisión del proceso de recuperación, con relación a los tiempos estimados de recuperación.

#### 4.11.1.2. EQUIPO DE RECUPERACIÓN

Este equipo es el encargado de establecer los lugares físicos requeridos para lograr la recuperación. Esto tiene incluido todos los servidores, PC's, comunicaciones de voz y datos y cualquier otro componente obligatorio para la restauración de un servicio. Se debe considerar las prioridades y la disponibilidad de recursos.

#### 4.11.1.3. EQUIPO LOGÍSTICO

Este equipo, está encargado de lo que se relaciona con las necesidades de abastecimiento logístico, en el contexto de una situación de activación del plan; dentro de las tareas establecidas tenemos:

- Transporte de material y personas (si es necesario) al lugar de recuperación.
- Suministros de oficina.
- Servicios alimentarios.
- Reservas de hotel (en caso de requerirse).
- Contacto directo con proveedores

Esta unidad debe organizarse conjuntamente con los otros, para asegurar que todas las necesidades logísticas sean cubiertas.

#### 4.11.1.4. EQUIPO DE RELACIONES Y ATENCIÓN AL CLIENTE

Se encarga de lograr la canalización de la información que se relaciona con fuera de la empresa; en un solo punto para se tenga una sola fuente de referencia para el SGCN. Sus funciones principales son:

- Desarrollo de comunicados con la prensa (en caso de ser necesario).
- Notificación con los clientes.
- Información a los clientes del estado de alerta y de la información que se solicite al respecto.

#### 4.11.1.5. EQUIPOS DE LAS UNIDADES DE NEGOCIO

Esta unidad estará conformada por personal que tiene a su cargo aplicaciones críticas; y que son los responsables de hacer las pruebas de funcionamiento para verificar la operatividad de los sistemas y comenzar a andar. Cada equipo deberá configurar las diferentes pruebas que deberán realizar para los sistemas.

La composición de cada uno de los equipos no es obligatoria; debe evaluarse el tipo de organización y decidir si se incluyen todos, o se adiciona alguno más que pueda considerarse.

### 4.11.2. PROCEDIMIENTOS DEL PLAN

Cuando ya se tienen bien definidos los equipos de trabajo y sus funciones principales, es necesario desarrollar los procedimientos que van a seguir, y su actuación en cada una de las fases de activación del Plan de Continuidad. Se puede establecer, en general, que existen las siguientes fases y que se deben desarrollar de la siguiente manera:

**Ilustración 12 – Actividades del Plan de Continuidad**


Fuente: Guía de desarrollo de un PCN, Estrategias de Respaldo, Laura del Pino (España, 2007).

#### 4.11.2.1. FASE DE ALERTA Y OPERACIÓN EN CONTINUDAD

La Fase de Alerta precisa las actividades a desarrollarse inicialmente ante las primeras etapas de un acontecimiento que involucre la pérdida parcial o total de uno o varios servicios críticos. Dividiremos esta fase en tres partes:

**NOTIFICACIÓN:**

Debido a que no es viable confeccionar un Plan de Alerta que dé capacidad a todos los casos que implican de suponer que cualquier persona pueda dar aviso de un incidente, vamos a suponer que el encargado que manifiesta la contingencia será un empleado o cualquier otra persona cercana al sitio donde ocurre el incidente. Como parte del Plan de Continuidad se debe instaurar un programa de concienciación, en el que se informe debidamente al personal de cómo proceder ante estos casos y a quién comunicar lo ocurrido.

**Tabla 21 – Ejemplo Fase de Notificación**

| | EVENTO | ACCIÓN |
|---|---|---|
| 1 | Situación de contingencia/incidente detectado por algún empleado de la compañía. (Fuego, inundación, virus, etc.). | Aviso inmediato con el máximo detalle posible al Responsable de Personal de turno o a Seguridad. |
| 2 | El responsable de turno o de seguridad conoce que ha sucedido una contingencia. | Aviso a la persona de contacto del Comité de Crisis. Aviso a los equipos de emergencia (si procede). |

Fuente: Guía desarrollo de un PCN, Desarrollo de un PCN. Laura del Pino (2007).

**EVALUACIÓN:**

Cuando algún responsable del Comité de Crisis es contactado e informado del incidente, se debe realizar la evaluación de la situación actual con el fin de recopilar la mayor información posible. El Comité comunicará a los responsables de los diferentes grupos de trabajo lo acontecido y del escenario en ese momento para que permanezcan en situación de espera, hasta que se tome la decisión de disparar el Plan o iniciar otro tipo de estrategia.

**Tabla 22 – Ejemplo Fase de Evaluación**

| | EVENTO | ACCIÓN |
|---|---|---|
| 3 | Conocimiento por algún miembro del Comité del incidente ocurrido. | El equipo del Comité se reunirá en un lugar acordado previamente y evaluará la situación. Este Comité deberá tomar la decisión de activar o no el Plan de Continuidad. Se debe informar a los siguientes responsables: Responsable de Seguridad, Comité de Dirección, Relaciones Públicas, Equipo de Recuperación. |

Fuente: Guía desarrollo de un PCN, Desarrollo de un PCN. Laura del Pino (2007).

**EJECUCIÓN DEL PLAN:**

Cuando el Comité ya tomó la decisión de poner en marcha el Plan de Continuidad, debe de iniciarse el árbol de llamadas (En el Anexo N°05 se incluye un ejemplo de un árbol de llamadas) para comunicar a los encargados y partes de cada equipo el escenario suscitado ante el inicio de las actividades del Plan para comenzar los procedimientos de actuación de cada uno de ellos. Deberá informarse también al Comité de Dirección.

**Tabla 23 – Ejemplo Fase de Ejecución**

| | EVENTO | ACCIÓN |
|---|---|---|
| 4 | Consideración por parte del Comité de Crisis y ejecución del Plan. | Iniciar el árbol de llamadas. |
| 5 | Paso a la Fase de Transición. | Informar al Comité de Dirección. |

Fuente: Guía desarrollo de un PCN, Desarrollo de un PCN. Laura del Pino (2007).

#### 4.11.2.2. FASE DE TRANSICIÓN

La Fase de Transición es la fase anterior a la de recuperación de los sistemas. Es indispensable que en esta fase se logre una conexión entre los diferentes equipos y equipos de logística, ya que son éstos los encargados de que todo esté disponible para comenzar la recuperación en el menor tiempo posible.

Podemos dividir la fase de transición en dos partes principalmente:

- **Procedimientos de concentración y traslado de personas y equipos:**

  Dependiendo de la estrategia elegida, es que este procedimiento varía. Una vez avisados los equipos y puesto en marcha el Plan, deberá determinarse un centro de reunión. Además del traslado de personas al centro de recuperación (si es necesario) hay que realizar una importante labor de coordinación para el traslado de todo el material necesario para

poner en marcha el centro de recuperación (cintas de backup, material de oficina, documentación).

- **Procedimientos de puesta en marcha del centro de recuperación:**

  Después que se ha logrado concentrar a los equipos responsables y material necesario para comenzar con la estrategia de recuperación, hay que poner en marcha este centro, estableciendo la infraestructura necesaria, tanto de software como de comunicaciones, etc.

#### 4.11.2.3. FASE DE RESTAURACIÓN

En este punto, ya se tienen desarrolladas las bases que permitirán la restauración. Por tal motivo, se debe proceder a la carga de datos y a la restauración de los servicios críticos. Este proceso y el anterior suele precisar los mayores esfuerzos e intervenciones para cumplir con los plazos fijados.

Podemos dividir esta fase en dos:

- **Procedimientos de Restauración:**

  Acciones específicas que buscan lograr la restauración de los servicios críticos.

- **Procedimientos de soporte y gestión:**

  Los sistemas necesitan ser comprobados en funcionamiento normal; por lo que se debe realizar un mantenimiento sobre los

mismos y protegerlos, para lograr la reanudación a las mejores condiciones.

#### 4.11.2.4. FASE DE RETORNO A LA NORMALIDAD

Cuando los procesos críticos ya están levantados y funcionan normalmente y realizada la contingencia, deben considerarse algunas acciones necesarias adicionales para lograr el retorno completo a la normalidad. Para esto, se deben considerar los siguientes procedimientos:

- **Análisis del impacto:**

  Es una evaluación diferente a la del BIA. Se debe cuantificar los equipos e instalaciones dañadas, para definir como retornar a la normalidad.

- **Procedimientos de vuelta a la normalidad:**

  Una vez determinado el impacto deben establecerse los mecanismos que en la medida de lo posible lleven a recuperar la normalidad total de funcionamiento. Estas acciones incluyen las necesidades de compra de nuevos equipos, mobiliario, material, etc.

#### 4.11.2.5. GENERACIÓN DE INFORMES Y EVALUACIÓN

Cuando ya se lograr el total retorno a la normalidad de todas las operaciones, cada equipo deberá realizar un informe de las acciones

que se han realizado, y como se relacionan a los objetivos planteados en el SGCN; el cumplimiento con los tiempos y dificultados en el camino.

Toda esta información servirá para valorar si el Plan ha funcionado según lo planeado, así como conocer los posibles fallos, y en su caso, tenerlos en cuenta para la adecuación del mismo y lograr el mantenimiento constante.

## 4.12. FASE V: ENSAYO DEL PLAN DE CONTINUIDAD

El Plan de Continuidad no se considerará válido hasta que no se haya superado satisfactoriamente el Plan de Pruebas que asegure la viabilidad de las soluciones adoptadas.

### 4.12.1. TIPOS DE PRUEBAS

Se consideran estas características como necesarias para el desarrollo de las pruebas:

**Realismo:** Mientras escenarios más reales se reproduzcan, las pruebas brindan mayor utilidad. Es importante generar escenarios que proporcionen un nivel de realismo adecuado y que mejoren el resultado de las pruebas.

**Exposición Mínima:** El diseño de las pruebas, debe lograr que no se genere un impacto verdadero en la organización, es decir, que si se programa una prueba que suponga una parada de los sistemas de información, debe realizarse una ventana de tiempo que impacte lo menos posible para el negocio.

En algunos casos puede resultar complicado realizar una prueba completa del Plan de Continuidad de Negocio. Por ello, es necesario desarrollar un programa de pruebas planificado para garantizar que todos los aspectos de los planes y personal se han ensayado durante un período de tiempo.

### 4.12.2. EJERCICIOS TÉCNICOS

Este tipo de ejercicio requerirá la ejecución de procedimientos de notificación y operativos, el uso de equipos de hardware, software y posibles centros y métodos alternativos para asegurar un rendimiento adecuado. Ejemplos de elementos verificados durante un ejercicio de simulación son:

- Procedimientos de emergencia.
- Métodos alternativos.
- Líneas de telecomunicaciones de backup.
- Procedimientos de notificación Vendedores / Clientes.
- Capacidad y rendimiento del hardware.
- Portabilidad del software.
- Accesibilidad al centro de respaldo.
- Movilización de los equipos de trabajo.
- Recuperación de ficheros y documentación almacenados en lugar externo.
- Recuperación de datos.

## 4.13. MANTENIMIENTO DEL PLAN DE CONTINUIDAD

Una vez que se tiene todo el sistema definido y que se ha logrado ensayar y comprobar su funcionamiento, el mantenimiento se convierte en una actividad crítica.

Existen diversos cambios internos y externos que son comunes. Muchos de estos requieren de una evaluación para considerar si pueden lograr invalidad el Plan de Continuidad.

El objetivo principal del mantenimiento es asegurar que el PCN se mantenga operativo en cualquier circunstancia; y listo para ejecutarse.

Debe establecerse una política de mantenimiento que haga una evaluación según un tiempo determinado para actualizar el Plan y todo el Sistema de Continuidad del Negocio.

## 4.14. CONCLUSIONES DE LA METODOLOGÍA

- La presente metodología genera una base para la implementación de un SGCN, que se adecua a la norma ISO 22301:2012, incluyendo los requisitos y recomendaciones y que puede acercar a la empresa a lograr una certificación.
- La metodología se adapta a cualquier tipo de organización; ya que los aspectos generales son los mismos. Existen algunos puntos donde puede existir variación en el desarrollo; por dependencia del tamaño y presupuesto de la empresa; pero se encuentra especificado en la metodología.

- Un Plan de Continuidad es una manera de controlar el destino de la empresa, y permite una evaluación y diagnóstico del funcionamiento integral.
- En mercados globalizados, el tener instaurado un PCN ha empezado a convertirse en una exigencia a las empresas que demuestran ser confiables con sus clientes.

# CAPÍTULO V

# DESARROLLO DEL BIA Y ANÁLISIS DE RIESGO A EMPRESA FINANCIERA "CMAC ICA" SEGÚN LA METODOLOGÍA PROPUESTA

## 5.1. INTRODUCCIÓN

Con el fin de poder comprobar el desarrollo de la metodología para su fin, que es establecer y mantener un SGCN; es que en el presente capítulo se desarrollará un Análisis de Impacto del Negocio (BIA), y un Análisis de Riesgo, para la empresa financiera "Caja Municipal de Ahorro y Crédito ICA".

La selección de la empresa en mención, se justifica porque se cuenta con información privilegiada sobre las operaciones de la financiera, y el apoyo de un coordinador de créditos; que consiguió la aprobación informal por el Administrador de la agencia Camaná para brindar esa información y colaborar con el desarrollo de las dos primeras fases según la metodología del capítulo anterior; y que son la base de todo el Sistema.

Al finalizar la propuesta, se enviará a la empresa para que la evalúen y estudien la posibilidad de complementarla, fortalecerla e implementarla en su organización.

## 5.2. LIMITACIONES

Debido a que el desarrollo de todo el Sistema de Continuidad es una actividad compleja y que requiere asignar diversos tipos de recursos y tiempo, es que para la verificación de la metodología sólo se desarrollará las dos primeras fases y que son las más importantes (BIA y Análisis de Riesgos).

Además, el fin del presente trabajo de investigación no es el desarrollo del Sistema para una empresa específica, sino el desarrollo de la metodología. Se considera, que para poder dar una inicial demostración de la aplicación de la metodología, el desarrollo de esas dos primeras fases es suficiente.

Existen limitaciones por parte de la empresa en mención. No se asignó personal específico que apoye esta labor, y la información brindada también es limitada. Para los análisis y especificaciones que requiere la metodología, se hará, en medida de lo posible, la intervención de personal experimentado para cada actividad y que acerque el contenido a la realidad.

Por la complejidad de la organización y el tiempo disponible, se realizará la evaluación a las áreas más importantes de la empresa y que se relacionan con la operatividad; se selecciona tres: operaciones, créditos y tesorería.

## 5.3. INFORMACIÓN INICIAL DE LA EMPRESA

Como se explica en la metodología, para cumplir con los requisitos de la norma ISO 22301:2012, existen aspectos generales que son importantes. La participación y comunicación por la alta dirección; la comunicación de los objetivos del SGCN, y la alineación de su contenido con la estrategia de la organización. Por tal motivo, antes de iniciar las actividades propias definidas, se debe conocer la siguiente información:

### 5.3.1. DATOS GENERALES

La Caja Municipal de Ica es una empresa financiera de derecho público que goza de autonomía económica, financiera y administrativa, desarrolla sus actividades basándose en sus principios: Democratización y descentralización del crédito, así como fomentar e incentivar una cultura de ahorro. Igualmente está autorizada a ofrecer el servicio de créditos pignoraticios y desarrollar otros servicios financieros.

Actualmente tiene el nombre de Caja Municipal de Ahorro y Crédito de Ica S.A. (CMAC ICA S.A.). La CMAC Ica, queda constituida en diciembre de 1987. El 18 de octubre de 1989 la Superintendencia de Banca y Seguros y AFP´s, autoriza el inicio de sus operaciones, lo cual se cumple el 21 de Octubre del mismo año.

### 5.3.2. VISIÓN

“Ser una empresa líder en calidad de servicio y rentabilidad”.

### 5.3.3. MISIÓN

"Brindar soluciones financieras de calidad que promuevan el éxito de los emprendedores del Perú".

## 5.4. CONSIDERACIONES PARA EL DESARROLLO

Para poder presentar el contenido del Análisis de Impacto del Negocio (BIA) y el Análisis de Riesgo, se presentará la información en este capítulo en forma de informe. Las tablas y desarrollo completo se anexarán.

Las evaluaciones que requieren un conocimiento del sistema y operatividad de la empresa, se consultaron con expertos y responsables de los procedimientos específicos. Existen aspectos que debido a la lejanía, y falta de tiempo y asignación de personal para esta labor, no se pueden desarrollar adecuadamente.

El fin de este capítulo no es tener un BIA y un Análisis de Riesgo totalmente validado; sino comprobar la aplicación de la metodología y generar una aproximación de su desarrollo para brindársela a la empresa y que pueda completarlo y fortalecerlo, teniendo la metodología también como guía.

## 5.5. PERSPECTIVA SOBRE EL DESARROLLO:

En este ítem, se busca explicar el papel que juega el desarrollo de la metodología y la influencia del iniciador de este pequeño proyecto, para poder llevarse a cabo y tener los resultados que beneficien a ambas

partes (empresa CMAC ICA y al desarrollador de la tesis para lograr su aplicación).

En inicio, el desarrollo de estas actividades se gestiona, como ya se mencionó, con un Coordinador de Créditos que lleva trabajando 10 años en la institución.

Para poder lograr la aprobación del trabajo, se expone abiertamente (vía telefónica y electrónica) el tema de Continuidad del Negocio, que ya es conocido por la empresa financiera; y se manifiesta que con el presente trabajo de investigación, es posible implementar todo el sistema de manera gradual y adecuándose a las necesidades propias que tiene la organización. Se presenta el modelo planteado de la metodología, siendo de gran interés para la organización ya que las financieras tienen una obligación de cumplimiento de actividades de Continuidad del Negocio reguladas por la SBS; y la CMAC Ica no contaba con una metodología definida.

La empresa si manejaba las siguientes actividades e implementaciones ligadas a la continuidad del negocio:

- Mapa de Procesos por áreas.
- Lista de funciones y procesos de negocio.
- Planes de contingencia para ciertos procesos, pero que fueron elegidos sin un estudio previo y justificado.
- Lista de sistemas y aplicaciones críticas.
- Análisis de riesgos de seguridad de información, pero no de continuidad del negocio.

Es así, que la empresa maneja un grupo de observaciones, resultado de la última auditoría realizada por la SBS, ya que su sistema no cuenta con las acciones básicas para asegurar la continuidad de las operaciones. Por tal motivo es que se logró la aprobación e interés de la CMAC Ica por contar y aplicar la metodología de este trabajo de investigación.

Los talleres se gestionaron con acuerdo del área de Seguridad de Información, y con apoyo del Coordinador, para completar la información que se presentará en el resto del capítulo.

El papel que tengo, es de facilitador de las actividades que se deben desarrollar, y de cómo se deben presentar de acuerdo a todo el estudio realizado; y de acuerdo a la experiencia que presento, habiendo ya implementado un Sistema de Gestión de Continuidad en una empresa como funciones propias del puesto de trabajo; organizando y participando en los talleres y desarrollando todas las actividades propiamente dichas. Toda la experiencia adquirida también se trasladó al producto final, la metodología que está hecha considerando varios aspectos que sólo se pueden ver en la práctica. También mi objetivo es transmitir la metodología para que pueda ejecutarse y sea de utilidad para empresas que reconozcan la necesidad de contar con un SGCN.

Al final se obtuvo el resultado que se presenta, que está enfocado al interés de verificar la facilidad de aplicación, comprensión, contenido y flexibilidad de la metodología; y sirve como iniciativa de la empresa para desarrollar todas las actividades de la metodología y cubrir las necesidades que consideren importantes.

## 5.6. INVERSION Y COSTO DE UN SISTEMA DE CONTINUIDAD

El desarrollo e implementación de la metodología para implementar un Sistema de Gestión de Continuidad del Negocio representa un gasto debido a que requiere el uso de recursos financieros y empresariales.

La inversión total requerida es muy variable, que depende de un gran componente de variables que engloben la situación empresarial y la necesidad reconocida que concientice la empresa con el sistema. A continuación se listan las variables consideradas como las más importantes:

- Tamaño de la organización
- Estructura de la organización
- Cantidad de funciones y procesos críticos del negocio
- Tipo de industria de la compañía
- Funciones actuales relacionadas a la continuidad del negocio y su correcto desarrollo
- Tiempo del personal requerido
- Deseo de lograr la certificación
- Recursos adicionales utilizados

Es necesario evaluar si la organización ya cuenta con funciones de continuidad, y si se han realizado de la manera correcta. También es indispensable definir hasta que etapa se quiere completar el sistema; si se quiere implementar algunas actividades o lograr la certificación y mantener el sistema.

En todo caso, se pueden identificar básicamente dos grupos de costo:

**Costos de implementación:**

Conjunto de herramientas requeridas por el sistema. Son todos los elementos del Sistema de Continuidad que están detallados en la metodología. Existen varias opciones para gestionarlos y poder desarrollarlos; y el gasto está influenciado directamente con las variables expuestas anteriormente. Se detallan algunas de las formas de llevarlos a cabo y cotizaciones promedio:

- Desarrollarlo total por propia cuenta, en gran medida la metodología apoya el entendimiento de la norma y como desarrollar cada paso requerido. Requiere básicamente el uso de tiempo de personal, en la implementación los recursos necesarios para los planes de continuidad y según los resultados; sistemas, aplicaciones, infraestructura, procedimientos que sean necesarios adicionar.
- Apoyo de un asesor: Existen personas expertas entendidas del tema que apoyan el desarrollo del sistema. En conjunto con los recursos de la empresa implementan el sistema. El costo depende del tiempo que demore la empresa en certificarse. En promedio puede costar $1000 al mes.
- Venta de software especializado: Existen empresas consultoras que diseñan software que busca implementar un sistema de continuidad. Por ejemplo tenemos a BSI Group, Ernest and Young, Ingertec, Global Suite. El software incluye todos los

procesos de la norma ISO 22301; que se integran a cada área de la organización para que aporten al desarrollo del sistema. Para entender el costo, se hizo una cotización a la empresa Global Suite, que ofrece el software Business Continuity. El software tiene un costo de $50000 sin incluir IGV.

**Costos de la auditoría de certificación:**

Según el tamaño, el número de sitios y el tipo de industria de la compañía es que se calcula el costo de la auditoría. Es necesario elegir a la empresa certificadora más adecuada en función a esas variables. En promedio las auditorías y la certificación pueden costar entre $5000 y $10000.

Para el desarrollo de las etapas implementadas en este capítulo, se utilizó principalmente el tiempo de las personas en los talleres realizados, y del desarrollador de la tesis, para la organización, procesamiento y presentación de la información.

El costo e inversión requerido es muy variable, a continuación se presenta un costo aproximado para la Implantación de la Norma ISO 22301 en la CMAC Ica, que se obtuvo de un auto presupuesto de la empresa Ingertec, consultora de sistemas de gestión. Las variables que utilizan son tipo de negocios, alcance del negocio, país, número de oficinas, número de trabajadores. El auto presupuesto según la consultora dio un costo de 23716 euros para las condiciones de la CMAC Ica.

## 5.7. INFORME DE ANÁLISIS DE IMPACTO DEL NEGOCIO (BIA)

### 5.7.1. OBJETIVOS DEL ANÁLISIS DE IMPACTO

El Análisis de Impacto al Negocio (BIA), tiene como objetivo el identificar los impactos resultantes de escenarios de discontinuidad y desastre que pueden afectar a la organización.

### 5.7.2. ALCANCE

El Alcance del BIA está enmarcado en realizar el análisis a las áreas funcionales de la organización CMAC Ica (créditos, tesorería y operaciones). Con el estudio se logrará:

- Identificar los procesos críticos y los componentes que soportan al negocio.
- Identificar los componentes mínimos necesarios para mantener la operatividad de las áreas críticas identificadas a operar desde un centro de negocio alterno.
- Los procesos de análisis son aquellos procesos críticos para el negocio y que requieren continuidad frente a eventos de contingencia.

### 5.7.3. METODOLOGÍA APLICADA

Para el desarrollo del BIA, se aplicará la metodología para la implementación de un SGCN, basada en la norma ISO/IEC 22301, que corresponde a una tesis desarrollada en la UCSM de Arequipa.

### 5.7.4. PROCESOS DEFINIDOS Y PROCESOS CRÍTICOS

Según el Mapa de Procesos que maneja la empresa y que pudo ser proporcionado, se identificó todos los procesos de todas las áreas de la organización (Ver Anexo N° 06). Por el tiempo disponible, solo se realiza el estudio en base a los procesos de tres áreas (Créditos, Operaciones y Tesorería). Una vez identificados, se hace la evaluación financiera y operacional; de donde se obtuvo los siguientes resultados:

**Tabla 24 – Resultado evaluación procesos CMAC ICA**

| Procesos del área | CRITICIDAD |
|---|---|
| **OP-Movimientos en cuentas de operaciones de ahorro** | ALTA |
| OP-Ingreso de expedientes | ALTA |
| OP-Desembolso de Créditos | ALTA |
| **OP-Cobranzas de créditos** | ALTA |
| TS-apertura y registro de cuentas. | ALTA |
| TS-Emisión diaria de Reporte de tesorería | ALTA |
| TS-Remesas de Efectivo de Bancos | ALTA |
| TS-Habilitaciones de efectivo a ventanillas | ALTA |
| TS-Control de Encaje | ALTA |
| OP-Promoción | MEDIA |
| **OP-Inicio de cajero** | ALTA |
| OP-apertura de cuentas (ahorro, DPF y CTS) | ALTA |
| OP-cancelaciones de cuentas de ahorro | ALTA |
| **OP-Operaciones Inter cajas** | MEDIA |
| OP-Servicio de Cobranza APAFAS | ALTA |
| OP-cierre de operaciones | ALTA |
| TS-Pago a proveedores | MEDIA |
| TS-Abono de planilla y liquidaciones | MEDIA |
| TS-Transferencias bancarias | MEDIA |
| TS-Corresponsalía Banco de la Nación | ALTA |

| | |
|---|---|
| TS-Habilitaciones de efectivo a agencias | MEDIA |
| TS-Custodia de Valores | MEDIA |
| CR-Promoción de Crédito | BAJA |
| CR-Solicitud de Crédito | BAJA |
| CR-Evaluación de Crédito | BAJA |
| CR-Aprobación de Crédito | BAJA |
| CR-Desembolso de Crédito | BAJA |
| CR-Seguimiento y Recuperación de Crédito | BAJA |

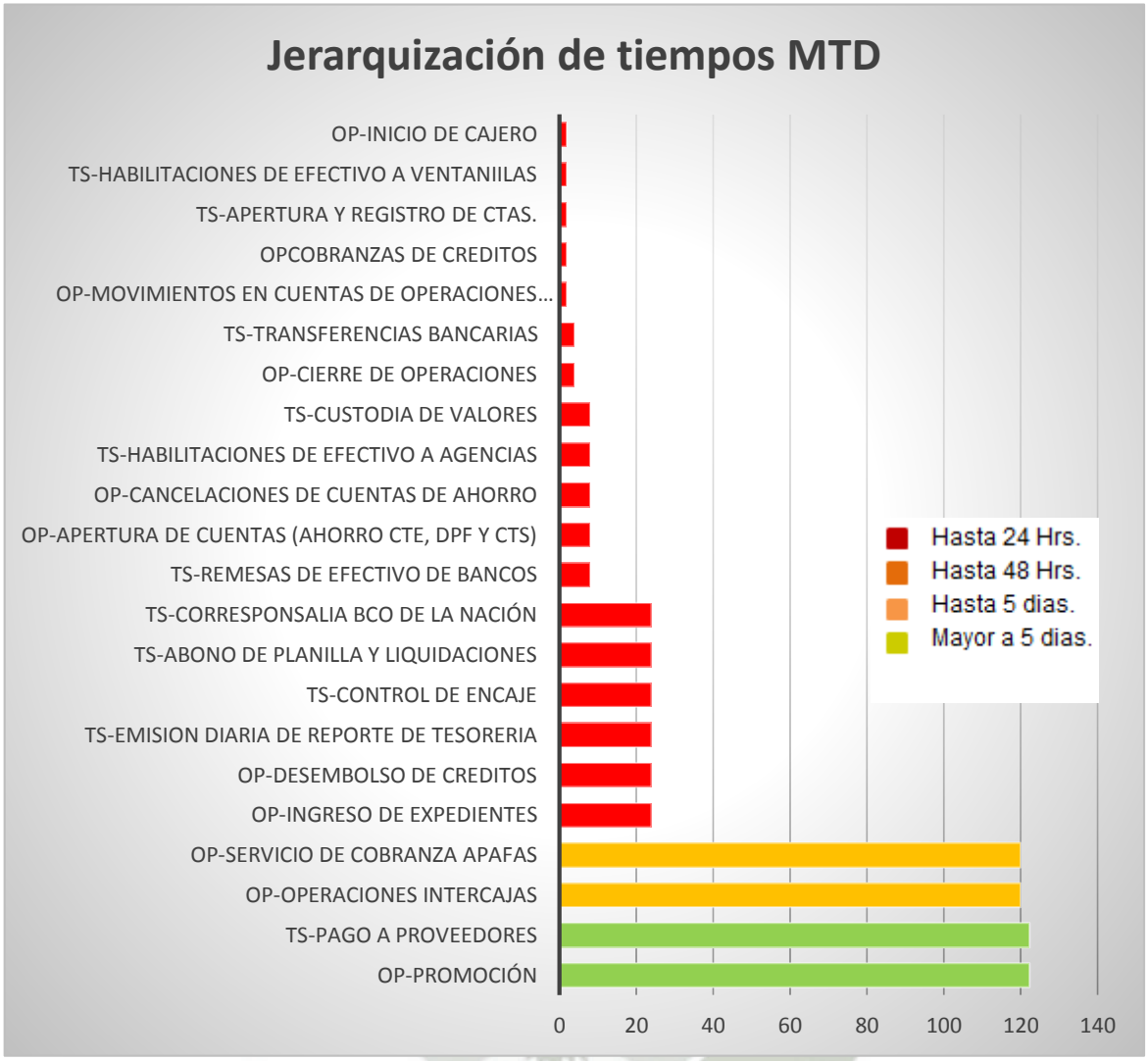
Fuente: Taller de Análisis de Impacto, CMAC ICA. Elaboración propia.

### 5.7.5. LISTA DE TIEMPOS MTD Y SU JERARQUIZACIÓN

Se presenta el reporte de la evaluación de tiempo MTD (tiempo que puede paralizarse el proceso sin que genere un impacto significativo) por cada proceso crítico y medio identificado. Se obtuvo los datos mediante la participación de los responsables conocedores de cada proceso. Recolectada la información, se realiza una jerarquización, priorizando los que tienen menor tiempo. Se consideran para atención inmediata los de color rojo.

Se establece el orden y jerarquización de menor a mayor, debido a que los tiempos más pequeños son los que requieren una atención con mayor urgencia. Se agrupó a todos aquellos que son menores a 24 horas, considerándolos como de prioridad alta.

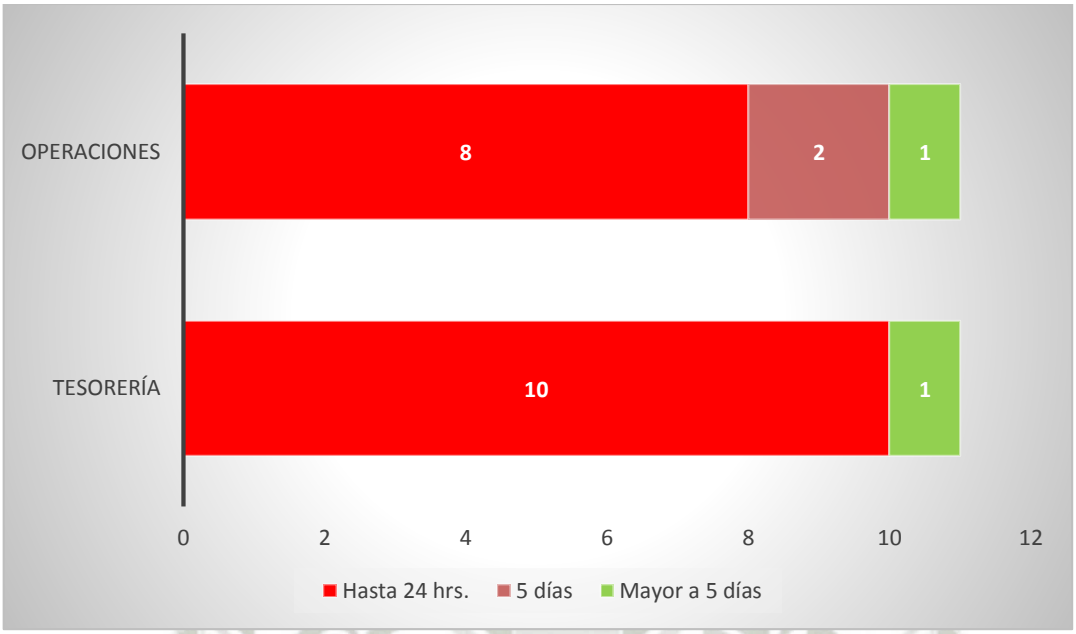
**Gráfica n° 3 – Jerarquización tiempos MTD**




Fuente: Taller de Análisis de Impacto, CMAC ICA. Elaboración propia.

A continuación, se muestra un gráfico que expresa la cantidad de procesos que tienen determinado MTD por áreas dentro de la organización.

**Gráfica n° 4 – Cantidad procesos según MTD por área**




Fuente: Elaboración Propia.

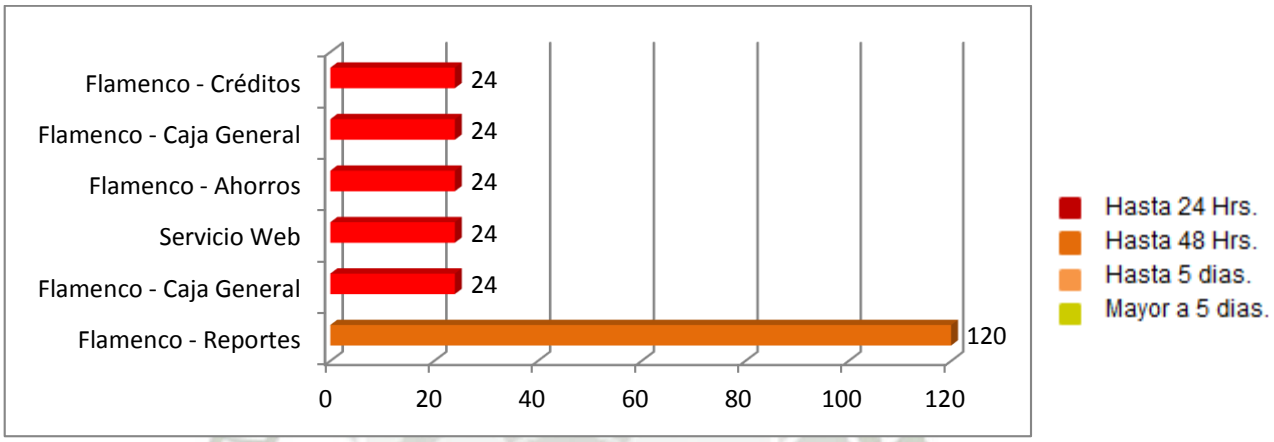
### 5.7.6. SISTEMAS Y APLICACIONES

De un total de 20 aplicaciones que figuran en la relación de aplicaciones proporcionada por la empresa (Ver Anexo N°07), las áreas involucradas en el alcance del BIA identificaron y analizaron un total 06 aplicaciones que representan el 30% de las indicadas en dicha relación. El 70% restante deberá ser analizado por la empresa en una etapa posterior, como parte de la aplicación del BIA a las demás áreas y subprocesos no considerados en el alcance del proyecto actual.

Primero, se establece, según cada proceso evaluado; el sistema y/o aplicación que es fundamental en su desarrollo. Dentro de la lista de todos los sistemas verificados, se debe evaluar también cual es el

tiempo crítico para el levantamiento de cada uno en caso de una interrupción. A continuación, se presenta el gráfico que nos indica estos valores para las 6 principales aplicaciones consideradas:

**Gráfica n° 5 – Tiempo de Demora Máxima levantamiento del sistema**




Fuente: Elaboración propia.

A continuación, se muestra la relación directa entre procesos y aplicaciones. Esta información se recogió con un mini taller informal con colaboración del contacto de la empresa. Se consultó a los encargados del área de Seguridad de la Información, Tecnología de Información, Administrador de la agencia Camaná, de la CMAC Ica.

**Tabla 25 – Aplicaciones y Sistemas de TI**

| Proceso | Servicio TI / Aplicación |
|---|---|
| **OP-Inicio de cajero** | Flamenco - Ahorros |
| OP-movimientos en cuentas de operaciones de ahorro | Flamenco - Ahorros |
| OP-Ingreso de expedientes | Flamenco - Créditos |
| **OP-Desembolso de Créditos** | Flamenco - Créditos |
| OP-Cobranzas de créditos | Flamenco - Créditos |
| TS-apertura y registro de cuentas. | Flamenco - Caja General |
| TS-Emisión diaria de Reporte de tesorería | Flamenco - Caja General |
| OP-apertura de cuentas (ahorro, DPF y CTS) | Flamenco - Ahorros |
| OP-cancelaciones de cuentas de ahorro | Flamenco - Ahorros |
| **OP-Operaciones Inter cajas** | Flamenco - Ahorros |
| OP-Servicio de Cobranza APAFAS | Flamenco - Ahorros |
| OP-cierre de operaciones | Flamenco - Ahorros |
| TS-Pago a proveedores | Flamenco - Caja General |
| TS-Abono de planilla y liquidaciones | Flamenco - Planillas |
| TS-Control de Encaje | Flamenco - Caja General |
| TS-Transferencias bancarias | Servicio Web |
| TS-Habilitaciones de efectivo a ventanillas | Flamenco - Caja General |

Fuente: Taller Análisis de Impacto, CMAC ICA. Elaboración propia.

### 5.7.7. RECURSOS ADICIONALES REQUERIDOS

#### 5.7.7.1. PUESTOS DE TRABAJO REQUERIDOS POR PERIODO

Recursos que no sean de Tecnología de información son indispensables. Se empezará analizando el factor humano, personal requerido por cada proceso evaluado. Esta información también se obtuvo en el taller.

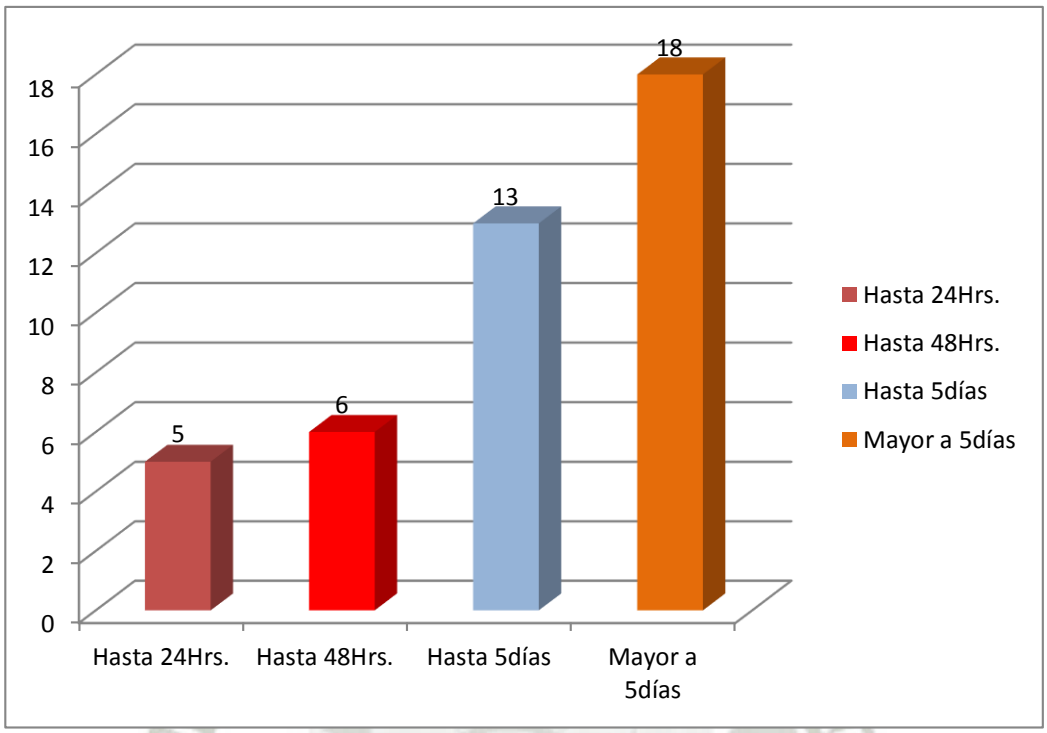
**Tabla 26 – Puestos de Trabajo Requeridos por Periodo**

| Proceso | Hasta 2Hrs. | Hasta 4Hrs. | Hasta 8Hrs. | Hasta 24Hrs. | Hasta 48Hrs. | Hasta 5días | Mayor 5días |
|---|---|---|---|---|---|---|---|
| **OP-Movimientos en cuentas de operaciones de ahorro** | 1 | 1 | 2 | 2 | 4 | 4 | 4 |
| OP-Ingreso de expedientes | | | | 1 | 1 | 1 | 1 |
| OP-Desembolso de Créditos | | | | 1 | 1 | 1 | 1 |
| **OP-Cobranzas de créditos** | 1 | 1 | 2 | 2 | 4 | 4 | 4 |
| TS-apertura y registro de cuentas. | 1 | 1 | 2 | 2 | 4 | 4 | 4 |
| TS-Emisión diaria de Reporte de tesorería | | | | 1 | 1 | 1 | 1 |
| TS-Remesas de Efectivo de Bancos | | | 1 | 1 | 1 | 1 | 1 |
| TS-Habilitaciones de efectivo a ventanillas | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| TS-Control de Encaje | | | | 1 | 1 | 1 | 1 |
| OP-Promoción | | | | | | | 1 |
| **OP-Inicio de cajero** | 1 | 1 | 2 | 2 | 4 | 4 | 4 |
| OP-apertura de cuentas (ahorro, DPF y CTS) | | | 2 | 2 | 4 | 4 | 4 |
| OP-cancelaciones de cuentas de ahorro | | | 2 | 2 | 4 | 4 | 4 |
| **OP-Operaciones Inter cajas** | | | | | | 1 | 1 |
| OP-Servicio de Cobranza APAFAS | | | | | | 1 | 1 |
| OP-cierre de operaciones | | 1 | 2 | 3 | 4 | 4 | 4 |
| TS-Pago a proveedores | | | | 1 | 1 | 1 | 2 |
| TS-Abono de planilla y liquidaciones | | | | 1 | 1 | 1 | 2 |
| TS-Transferencias bancarias | | 1 | 1 | 1 | 1 | 1 | 2 |
| TS-Corresponsalía Banco de la Nación | | | | 1 | 1 | 1 | 2 |
| TS-Habilitaciones de efectivo a agencias | | | 1 | 1 | 1 | 1 | 2 |
| TS-Custodia de Valores | | | 1 | 1 | 1 | 1 | 2 |

Fuente: Taller Análisis de Impacto, CMAC ICA. Elaboración propia.

Existe algún personal que puede duplicar funciones y en caso de la caída de varios procesos, colaborar con tareas de más de un proceso caído. En el siguiente gráfico, se muestra la cantidad máxima de personas que deberían necesitarse en caso de la caída total de todos los procesos.

**Gráfica n° 6 – Puestos de Trabajo Totales por Periodo**




Fuente: Elaboración propia.

### 5.7.7.2. RECURSOS ADICIONALES

Se lista y enumera recursos adicionales secundarios que son necesarios para poder levantar el proceso. Toda esta información se obtuvo en conjunto en el mini taller realizado.

**Tabla 27 – Recursos Adicionales**

| | 24Hrs. | 48Hrs. | 5días | TOTAL > 05días |
|---|---|---|---|---|
| ESCRITORIO | 5 | 6 | 13 | 18 |
| PC | 5 | 6 | 13 | 18 |
| UPS | 5 | 6 | 13 | 18 |
| IMPRESORAS | 2 | 2 | 2 | 3 |
| TELF. CELULAR | 5 | 6 | 13 | 18 |
| TELF. ESTAND | 2 | 2 | 3 | 3 |
| KIT DE ESCRITORIO | 5 | 6 | 13 | 18 |
| FOTOCOPIADORA | 1 | 2 | 2 | 3 |
| USB | 2 | 3 | 3 | 7 |
| FAX | 1 | 2 | 2 | 2 |
| INTERNET/NAV | 5 | 6 | 13 | 18 |
| CORREO INTER | 5 | 6 | 13 | 18 |
| CARPT COMPAR | 3 | 3 | 3 | 3 |
| Cajas de Seguridad | 1 | 1 | 1 | 1 |
| Sumadora | 2 | 3 | 4 | 4 |
| SELLO FECHADOR 2910/P02 TRODAT | 4 | 4 | 4 | 4 |
| TAMPON REDONDO AZUL PEQUEÑO (1500 HUELLAS) | 1 | 1 | 1 | 1 |
| TAMPON 2K ARTESCO AZUL | 4 | 4 | 4 | 4 |
| Cajas metálicas | 4 | 4 | 4 | 4 |
| Pagares | 1 | 1 | 1 | 1 |
| Contratos | 1 | 1 | 1 | 1 |
| Chequeras/Ordenes de pago | 1 | 1 | 1 | 1 |
| Certificados de Depósitos | 1 | 1 | 1 | 1 |
| Hojas Resumen | 1 | 1 | 1 | 1 |

Fuente: Taller de Análisis de Impacto CMAC ICA. Elaboración propia.

### 5.7.8. REPORTES REGULATORIOS

Se presentan los reportes regulatorios que son importantes para la organización, para considerarlos en caso de una interrupción.

**Tabla 28 – Reportes Regulatorios**

| ENTDAD REGULATORIA | NOMBRE DEL REPORTE | COMPLEJIDAD DEL REPORTE | ÁREA QUE EMITE EL REPORTE | DEMORA MÁXIMA |
|---|---|---|---|---|
| Banco Central de Reserva | Encaje Diario | Fácil | Tesorería | Hasta 24Hrs. |
| Banco Central de Reserva | Encaje Definitivo | Difícil | Tesorería | Hasta 24Hrs. |
| Superintendencia de Banca y Seguros | Encaje Definitivo | Difícil | Tesorería | Hasta 24Hrs. |
| Banco Central de Reserva | Numerario falso | Fácil | Tesorería | Hasta 24Hrs. |
| Banco Central de Reserva | Anexo N 6 Tasas | Difícil | Operaciones | Hasta 24Hrs. |
| Superintendencia de Banca y Seguros | Adeudados | Fácil | Tesorería | Hasta 24Hrs. |
| Fondo de Seguros y Depósitos | FSD | Difícil | Operaciones | Hasta 24Hrs. |

Fuente: Taller de Análisis de Impacto, CMAC ICA. Elaboración propia.

### 5.7.9. LISTA DE TIEMPOS RTO

Se tiene que identificar el tiempo RTO para cada proceso, y jerarquizarlo según el requisito de la metodología usada. Se presenta la tabla a continuación:

**Tabla 29 – Lista Jerarquizada según RTO**

| Proceso | RTO |
|---|---|
| **OP-Inicio de cajero** | Hasta 2Hrs. |
| OP-Movimientos en cuentas de operaciones de ahorro | Hasta 2Hrs. |
| OP-Cobranzas de créditos | Hasta 2Hrs. |
| TS-apertura y registro de cuentas. | Hasta 2Hrs. |
| TS-Emisión diaria de Reporte de tesorería | Hasta 2Hrs. |
| OP-apertura de cuentas (ahorro, DPF y CTS) | Hasta 2Hrs. |
| TS-Habilitaciones de efectivo a ventanillas | Hasta 2Hrs. |
| OP-cancelaciones de cuentas de ahorro | Hasta 4Hrs. |
| OP-cierre de operaciones | Hasta 4Hrs. |
| **OP-Operaciones Inter cajas** | Hasta 5días |

| | |
|---|---|
| OP-Servicio de Cobranza APAFAS | Hasta 5días |
| OP-Ingreso de expedientes | Hasta 8Hrs. |
| **OP-Desembolso de Créditos** | Hasta 8Hrs. |
| TS-Transferencias bancarias | Hasta 8Hrs. |
| TS-Pago a proveedores | Hasta 24Hrs. |
| TS-Abono de planilla y liquidaciones | Hasta 24Hrs. |
| TS-Control de Encaje | Hasta 24Hrs. |

Fuente: Taller de Análisis de Impacto, CMAC ICA. Elaboración propia.

### 5.7.10. LISTA DE TIEMPOS RPO

Según la funcionalidad de la empresa, de los procesos que se tienen; y para evitar la complejidad organizacional; la empresa define que la pérdida tolerable de datos debe ser igual para todos los procesos. Se realizan copias de información por cada periodo de un día (24 horas) para todos los procesos estudiados.

### 5.7.11. PROCEDIMIENTOS ALTERNOS

Se consideran los siguientes procedimientos alternos según cada proceso:

**Tabla 30 – Procedimientos Alternos**

| PROCESO | PROCEDIMIENTO ALTERNO |
|---|---|
| **OP-movimientos en cuentas de operaciones de ahorro** | No se cuenta con plan alterno |
| OP-Ingreso de expedientes | No se cuenta con plan alterno |
| OP-Desembolso de Créditos | Se trabajara con formatos manuales |
| **OP-Cobranzas de créditos** | Se trabajara con formatos manuales |
| **TS-apertura y registro de cuentas.** | Se trabajara con formatos manuales |
| TS-Emisión diaria de Reporte de tesorería | Se trabajara con formatos manuales |
| TS-Remesas de Efectivo de Bancos | Se trabajara con cartas ordenes |
| **TS-Habilitaciones de efectivo a ventanillas** | Se trabajara con formatos manuales |
| TS-Control de Encaje | Cuento con plantilla manual |
| OP-Promoción | |
| **OP-Inicio de cajero** | Se trabajara con formatos manuales |
| OP-apertura de cuentas (ahorro, DPF y CTS) | Se trabajara con formatos manuales |
| OP-cancelaciones de cuentas de ahorro | Se trabajara con formatos manuales |
| **OP-Operaciones Inter cajas** | |
| OP-Servicio de Cobranza APAFAS | Se trabajara con formatos manuales |
| OP-cierre de operaciones | Se trabajara con formatos manuales |
| TS-Pago a proveedores | Se trabajara con formatos manuales |
| TS-Abono de planilla y liquidaciones | Se trabajara con formatos manuales |
| TS-Transferencias bancarias | Se trabajara con cartas ordenes |
| TS-Corresponsalía Banco de la Nación | Se trabajara con formatos manuales |
| TS-Habilitaciones de efectivo a agencias | Se trabajara con formatos manuales |
| TS-Custodia de Valores | Se trabajara con formatos manuales |

Fuente: Taller de Análisis de Impacto, CMAC ICA. Elaboración propia.

### 5.7.12. CONCLUSIONES

- La identificación de las áreas críticas del negocio, se llevó a cabo teniendo en cuenta su participación en el Core de la empresa (corazón del negocio). La identificación de sus procesos es vitales para contribuir con la misión, metas y objetivos donde se encuentra el alcance del Plan de Continuidad del Negocio.
- Se logró identificar los procesos más representativos para la empresa y conocer los tiempos críticos para poder medir el impacto de una interrupción. Toda la información es de utilidad para conocimiento y establecimiento de estrategias que permitan evitar pérdidas.
- El BIA se realizó en base a la metodología de la tesis de implementación de un SGCN en base a la norma ISO 22301.
- El desarrollo completo se encuentra documentado, en este contenido sólo se encuentra el informe final.

## 5.8. INFORME DE ANÁLISIS DE RIESGOS

### 5.8.1. OBJETIVO DEL ANÁLISIS DE RIESGOS

La identificación y evaluación de controles preventivos según el nivel de riesgos en la Continuidad de Negocios considera como objetivo principal el prevenir la ocurrencia de un incidente que pueda ocasionar un desastre.

El presente Informe Análisis de Riesgo (RA por sus siglas en inglés) aplicado según la perspectiva de Continuidad de Negocios, a las instalaciones del edificio de la CMAC Ica Camaná; tiene por objetivo presentar los resultados obtenidos y las correspondientes recomendaciones orientadas a mitigar los riesgos identificados.

### 5.8.2. ALCANCE

En primera instancia se consideró realizar el Análisis de Riesgo teniendo en cuenta las áreas críticas del negocio, como son Créditos, Operaciones y Tesorería; considerando como edificio principal a las Agencias y Oficinas Especiales que tiene la CMAC en las localidades de Ica. Se consideran condiciones y aspectos de estas ubicaciones; pero la información principal se obtiene de la Agencia Camaná.

### 5.8.3. METODOLOGÍA APLICADA

Para el desarrollo del Análisis de Riesgos, se aplicará la metodología para la implementación de un SGCN, basada en la norma ISO/IEC 22301, que corresponde a una tesis desarrollada en la UCSM de Arequipa.

### 5.8.4. COMPONENTES CRÍTICOS DE EVALUACIÓN

Los componentes del Negocio evaluados para el edificio de la Oficina de la CMAC ICA Camaná, son:

- **Empleados -** Indisponibilidad de los colaboradores de CMAC Ica
- **Infraestructura -** Indisponibilidad del ambiente físico.

- **Recursos -** Indisponibilidad de los recursos necesarios para la operación, tales como PC, impresora, fax, dinero en efectivo, entre otros.
- **Registros Vitales –** Indisponibilidad de información del cliente, registro de las operaciones activas y pasivas, pagares, contratos, expedientes de créditos, entre otros.
- **Sistemas Informáticos –** Indisponibilidad de los sistemas de la CMAC, tales como Flamenco, Intranet, etc.
- **Clientes -** Indisponibilidad de los clientes de la CMAC Ica
- **Proveedores Externos**
- **Comunidad en General**

### 5.8.5. IDENTIFICACIÓN DE AMENAZAS

Para la identificación de amenazas, se revisó el historial de todas las eventualidades y problemas que se habían suscitado en las instalaciones del edificio. Además, en el mini taller realizado para el BIA, también se llevaron a cabo actividades para el desarrollo del Análisis de Riesgos. Dentro de las amenazas identificadas que pueden afectar las operaciones y la continuidad del negocio, se encontraron las siguientes:

**Tabla 31 – Amenazas Identificadas CMAC Ica**

| Clasificación | Tipo de Amenaza |
|---|---|
| Naturales | Pandemia |
| | Terremoto, Sismo |
| | Maremoto |
| Antrópicas | Incendio |
| | Disturbios sociales |
| | Inundaciones y Aniegos |
| | Ataque terrorista |
| | Secuestro |
| | Toma de local con rehenes |
| | Fraude robo falsificación |
| | Daño en la Reputación |
| | Explosión |
| | Accidentes aéreos |
| Tecnológicas | Falla red comunicaciones |
| | Falla servicio eléctrico |
| | Sabotaje Tecnológico |
| | Falla Internet, correo electrónico |
| | Falla en aplicaciones |

Fuente: Taller de Análisis de Riesgos, CMAC ICA. Elaboración propia.

### 5.8.6. IDENTIFICACIÓN DE CONTROLES

Los controles hacen posible la mitigación de posibles daños y son identificados según cada componente que se ve afectado según la amenaza evaluada.

Las áreas críticas, así como oficinas y agencias remotas han identificado los controles de acuerdo a los tipos de amenazas que consideran se presentarían y que podrían generar la suspensión de las operaciones, las mismas que se detallarán al final del Análisis.

### 5.8.7. EVALUACIÓN DE RIESGOS

El nivel de riesgo de una amenaza se calcula considerando el nivel de riesgo mayor de cada uno de los componentes evaluados.

Para la identificación del nivel de riesgo se ha considerado la siguiente matriz:

**Ilustración 13 – Matriz para Medición de Nivel de Riesgo CMAC Ica**

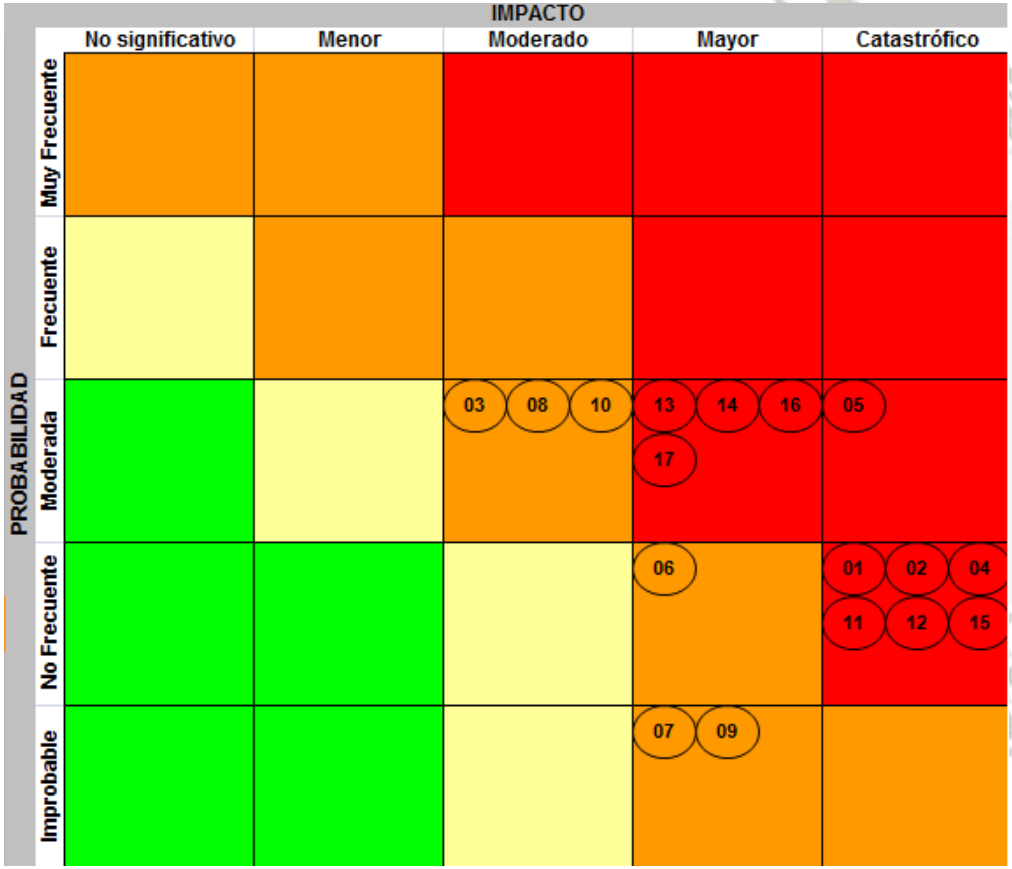
| Probabilidad ⇩ | Impacto | | | | |
|---|---|---|---|---|---|
| | No Significativo (1) | Menor (2) | Moderado (3) | Mayor (4) | Catastrófico (5) |
| Muy Frecuente (5) | Alto | Alto | Extremo | Extremo | Extremo |
| Frecuente (4) | Moderado | Alto | Alto | Extremo | Extremo |
| Moderado (3) | Bajo | Moderado | Alto | Extremo | Extremo |
| No frecuente (2) | Bajo | Bajo | Moderado | Alto | Extremo |
| Improbable (1) | Bajo | Bajo | Moderado | Alto | Alto |

Fuente: Metodología Implementación SGCN, Fase II Gestión del Riesgo, (Arequipa, 2015).

El nivel de riesgo de cada una de las amenazas identificadas para la continuidad del negocio en el edificio de la Oficina de la CMAC Ica Camaná, desde el punto de vista de las áreas críticas, conforme a sus componentes o activos expuestos, fueron los siguientes:

## RESULTADOS PARA EDIFICIO CMAC ICA CAMANA

### Gráfica n° 7 – Resultado Medición de Riesgo CMAC Ica

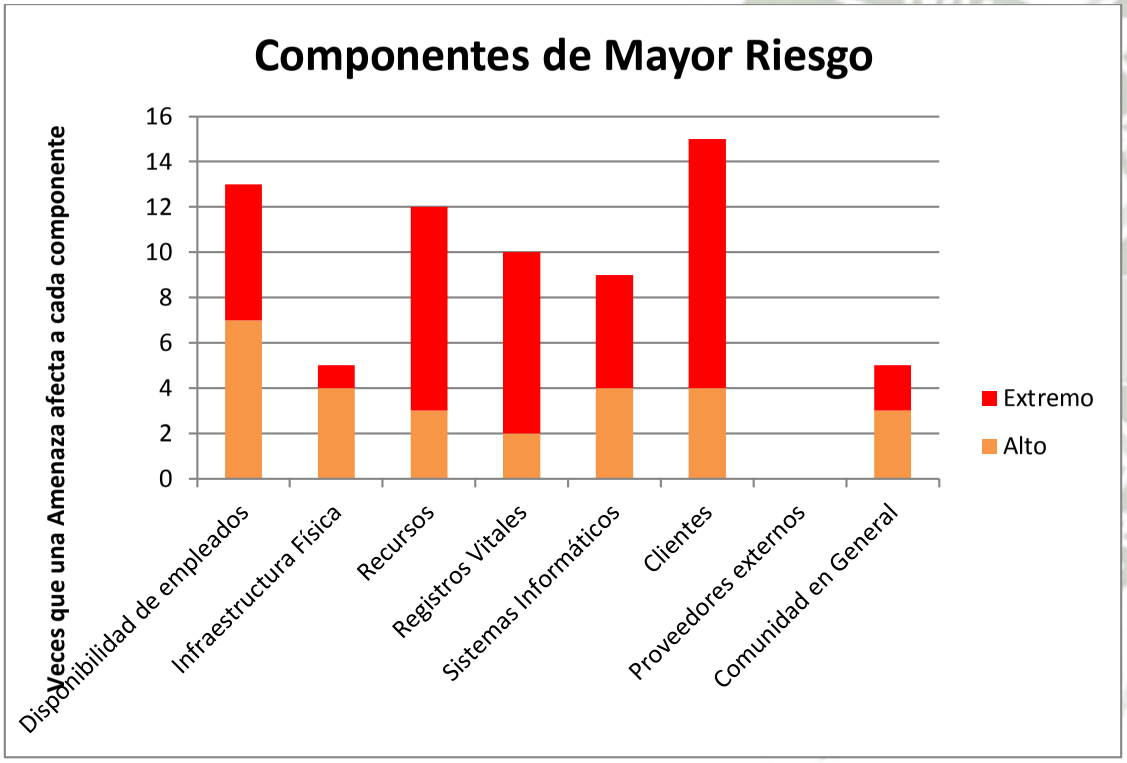



| | Evento | Nivel de Riesgo |
|---|---|---|
| ER01 | Pandemia | Extremo |
| ER02 | Terremoto | Extremo |
| ER03 | Inundaciones y Aniegos | Alto |
| ER04 | Maremoto | Extremo |
| ER05 | Incendio | Extremo |
| ER06 | Manifestac. y Disturb. Sociales | Alto |
| ER07 | Ataque Terrorista | Alto |
| ER08 | Secuestro | Alto |
| ER09 | Toma de local con rehenes | Alto |
| ER10 | Fraude Robo Falsificación | Alto |
| ER11 | Explosión | Extremo |
| ER12 | Accidentes aéreos | Extremo |
| ER13 | Falla de Red de Comunicaciones | Extremo |
| ER14 | Falla energía eléctrica | Extremo |
| ER15 | Sabotaje tecnológico | Extremo |
| ER16 | Falla de internet Correo | Extremo |
| ER17 | Fallo en las aplicaciones | Extremo |

Fuente: Elaboración propia.

Se evaluó también, cuáles componentes del negocio pudieran resultar afectados como consecuencia de la ocurrencia de cada amenaza, obteniendo la siguiente gráfica.

**Gráfica n° 8 – Componentes de negocio y riesgos asociados**




Veces que un componente clave del negocio presenta un nivel de riesgo Extremo

Veces que un componente clave del negocio presenta un nivel de riesgo Alto

| Activos | Extremos | Altos |
|---|---|---|
| Disponibilidad de empleados | 7 | 6 |
| Infraestructura Física | 4 | 1 |
| Recursos | 3 | 9 |
| Registros Vitales | 2 | 8 |
| Sistemas Informáticos | 4 | 5 |
| Clientes | 4 | 11 |
| Proveedores externos | 0 | 0 |
| Comunidad en General | 3 | 2 |

Fuente: Elaboración propia.

Como se puede observar, de los 07 eventos de riesgo evaluados para la CMAC Ica, se identificó que:

Existen 11 eventos de riesgo considerados significativos, pues sus niveles de riesgo se ubican como Riesgo Extremo, los cuales son los siguientes:

- Paralización de los procesos y/o servicios del Edificio CMAC analizado, debido a posibles daños a la salud de los trabajadores a causa de una PANDEMIA.
- Paralización de los procesos y/o servicios del Edificio CMAC analizado, debido a posibles daños en la infraestructura, el centro de cómputo (debido a destrucción de los equipos, deterioro de la sala), centro de control de seguridad, áreas administrativas y al personal, a causa de un TERREMOTO.
- Paralización de los procesos y/o servicios del Edificio CMAC, debido a posibles daños en la infraestructura, el centro de cómputo (debido a destrucción de los equipos, deterioro de la sala), centro de control de seguridad, áreas administrativas y al personal, a causa de un MAREMOTO.
- Paralización de los procesos y/o servicios de la CMAC debido a posibles daños de los recursos (escritorio, documentos, muebles, computadoras, etc.) de la empresa y en el personal de trabajo a causa de un INCENDIO.
- Paralización de los procesos y/o servicios de la CMAC debido a posibles daños de los recursos (escritorio, documentos,

muebles, computadoras, etc.) de la empresa y en el personal de trabajo a causa de una EXPLOSION.

- Paralización de los procesos y/o servicios del Edificio CMAC analizado, debido a posibles daños en la infraestructura, el centro de cómputo (debido a destrucción de los equipos, deterioro de la sala), centro de control de seguridad (destrucción de los equipos de monitoreo integral de Seguridad), y central telefónica, a causa de un ACCIDENTE AEREO.
- Paralización de los procesos y/o servicios del Edificio CMAC analizado, debido a posible daño a la infraestructura de telecomunicaciones (interrupción del servicio de voz (telefonía) y/o datos, cualquier problema físico que detenga las operaciones de los equipos de comunicación o afecte el medio de transmisión) a causa de una FALLA EN LA RED DE COMUNICACIONES.
- Paralización de los procesos y/o servicios de la CMAC debido a interrupciones en los equipos y Centro de Computo que impidan el movimiento, flujo de dinero o tramites que originen una perdida monetaria a causa de una FALLA EN LA ENERGÍA ELECTICA.
- Paralización de los procesos y/o servicios del Edificio CMAC analizado, debido a fuga o perdida de información vital, que afecten los procesos críticos de la financiera, a causa de un acto de SABOTAJE.

- Paralización de los procesos y/o servicios del Edificio CMAC analizado, debido a posible daño a la infraestructura de telecomunicaciones (interrupción del servicio de voz, datos, cualquier problema físico que detenga las operaciones de los equipos de comunicación o afecte el medio de transmisión) a causa de FALLAS DE INTERNET, CORREO ELECTRONICO.
- Paralización de los procesos y/o servicios de la CMAC debido a interrupciones en las aplicaciones con los clientes y Centros de Computo que impidan el movimiento, flujo de dinero o tramites que originen una perdida monetaria a causa de una FALLAS EN LAS APLICACIONES.

Existen 06 eventos de riesgo que a pesar de los controles existentes son considerados con nivel de riesgo alto, los cuales se indican a continuación:

- Paralización de los procesos y/o servicios de la CMAC debido a posibles daños de los recursos (escritorio, documentos, muebles, computadoras, etc.) de la empresa y en el personal de trabajo a causa de una INUNDACIÓN y ANIEGOS.
- Paralización de los procesos y/o servicios del Edificio CMAC analizado, debido a posibles daños a la integridad de los trabajadores a causa de MANIFESTACIONES y DISTURBIOS SOCIALES.

- Paralización de los procesos y/o servicios del Edificio CMAC analizado, debido a posibles daños a la infraestructura y a la integridad de los trabajadores a causa de un ATAQUE TERRORISTA.
- Paralización de los procesos y/o servicios del Edificio CMAC analizado, debido a posibles pérdidas de ejecutivos y/o personal clave que participa en los procesos críticos del negocio a causa de un SECUESTRO.
- Paralización de los procesos y/o servicios del Edificio CMAC analizado, debido a presencia de personas con actitud hostil, peligrosa y con fines ilegales que pueden atentar a la integridad de los trabajadores a causa de TOMA DEL LOCAL CON REHENES.
- Paralización de los procesos y/o servicios del Edificio CMAC analizado, debido a fuga o perdida de información vital, perdida de activos críticos, que afecten los procesos críticos de la financiera, a causa de FRAUDE, ROBO o FALSIFICACIÓN.

### 5.8.8. REVISIÓN DE CONTROLES EN ESCENARIOS DE AMENAZAS

Luego de efectuar la Evaluación de Riesgos y Controles es necesario tomar en cuenta las siguientes recomendaciones; que podrían considerarse como controles propuestos en determinados escenarios de amenazas descritos anteriormente para explicación de cada riesgo.

**Tabla 32 – Controles en escenarios de amenazas**

| CODIGO | AMENAZA | CONTROLES |
|---|---|---|
| **NIVEL DE RIESGO EXTREMO** | | |
| ER01 | Pandemia | Reglamento de Seguridad |
| | | Taller de capacitación sobre el uso adecuado de los instrumentos de primeros auxilios |
| | | Campaña de vacunación |
| | | Implementación de servicios por internet(acceso remoto) |
| ER02 | Terremoto | Taller de capacitación sobre el uso adecuado de los instrumentos de primeros auxilios |
| | | Evaluación de la Infraestructura |
| | | Implementación de plan de emergencia |
| | | Conformación de Brigadas de Emergencia |
| | | Identificación de zonas seguras |
| | | Simulacros |
| | | Centro alterno de Negocio |
| | | Centro de Computo Alterno |
| | | Digitalización de documentos |
| | | Pisos antideslizantes |
| | | Instalar Luces de emergencia |
| ER04 | Maremoto | Taller de capacitación sobre el uso adecuado de los instrumentos de primeros auxilios |
| | | Evaluación de la Infraestructura |
| | | Implementación de plan de emergencia |
| | | Conformación de Brigadas de Emergencia |
| | | Identificación de zonas seguras |
| | | Simulacros |
| | | Centro alterno de Negocio |
| | | Centro de Computo Alterno |
| | | Digitalización de documentos |
| | | Pisos antideslizantes |
| | | Instalar Luces de emergencia |
| ER05 | Incendio | Taller de capacitación sobre el uso adecuado de los instrumentos de primeros auxilios |
| | | Evaluación de la Infraestructura |
| | | Implementación de plan de emergencia |
| | | Conformación de Brigadas de Emergencia |
| | | Identificación de zonas seguras |
| | | Simulacros |
| | | Centro alterno de Negocio |
| | | Centro de Computo Alterno |
| | | Digitalización de documentos |
| | | Pisos antideslizantes |
| | | Instalación de tomas de agua en lugares estratégicos |
| | | Instalación de sensores de humo |
| | | Instalar Luces de emergencia |
| ER11 | Explosión | Taller de capacitación sobre el uso adecuado de los instrumentos de primeros auxilios |
| | | Evaluación de la Infraestructura |

| | | |
|---|---|---|
| | | Implementación de plan de emergencia |
| | | Conformación de Brigadas de Emergencia |
| | | Identificación de zonas seguras |
| | | Simulacros |
| | | Centro alterno de Negocio |
| | | Centro de Computo Alterno |
| | | Digitalización de documentos |
| | | Pisos antideslizantes |
| | | Instalar Luces de emergencia |
| ER12 | Accidente Aéreo | Taller de capacitación sobre el uso adecuado de los instrumentos de primeros auxilios |
| | | Evaluación de la Infraestructura |
| | | Implementación de plan de emergencia |
| | | Conformación de Brigadas de Emergencia |
| | | Identificación de zonas seguras |
| | | Simulacros |
| | | Centro alterno de Negocio |
| | | Centro de Computo Alterno |
| | | Digitalización de documentos |
| | | Pisos antideslizantes |
| | | Instalar Luces de emergencia |
| | | Luz de balizaje |
| ER13 | Falla de Red de Comunicaciones | Verificar Línea alterna de comunicaciones |
| | | Equipos de comunicación satelital |
| | | Calendario de Mantenimiento |
| ER14 | Falla de Energía Eléctrica | Verificar Línea alterna de comunicaciones |
| | | Equipos de comunicación satelital |
| | | Calendario de Mantenimiento |
| ER15 | Sabotaje | Capacitación de seguridad |
| | | Políticas de Seguridad |
| | | Implementación cámaras de vigilancia en zonas estratégicas |
| | | Evaluación Psicológica anual al personal |
| ER16 | Falla de Internet, Correo Electrónico | Verificar Línea alterna de comunicaciones |
| | | Equipos de comunicación satelital |
| | | Rpm |
| ER17 | Falla en las Aplicaciones | Evaluar Implementación de ambiente de preproducción |
| | | Evaluar implementación área de control de calidad |
| | | Definición de políticas |

Fuente: Elaboración propia.

### 5.8.9. MEDIDAS DE ACCIÓN INMEDIATAS RECOMENDADAS SEGÚN ESCENARIOS

Se ha considerado las recomendaciones propuestas por los participantes en el mini taller de Análisis de Riesgo (RA) del Edificio Principal CMAC Ica Camaná y se han agrupado los controles recomendados de una manera estructurada.

Se sugiere la implementación prioritaria de la lista siguiente de recomendaciones, lo cual permitirá mitigar los eventos de riesgo y disminuir los niveles de riesgo extremo (según política de la empresa).

- ***Evaluar la implementación de un centro alterno de negocio***, con la finalidad de que CMAC Ica cuente con un área de trabajo ante una interrupción de la continuidad de sus operaciones y/o servicios: lo cual permitirá mitigar 05 eventos de riesgos de nivel extremo.
- ***Evaluar la implementación de un centro de cómputo alterno***, con la finalidad de que la empresa cuente con un servidor alterno, que permita mantener la información ante una interrupción de la continuidad de sus operaciones y/o servicios: lo cual permitirá mitigar 05 eventos de riesgos de nivel extremo.
- ***Taller de Capacitación sobre el uso adecuado de los instrumentos de primeros auxilios,*** con la finalidad de que la organización cuente con el personal capacitado en el caso

suceda un evento de riesgo. Lo cual permitirá mitigar 06 eventos de riesgos de nivel extremo.

- ***Implementación de un Plan de Emergencia,*** con la finalidad de que el personal de CMAC Ica cuente con una guía actualizada en caso suceda un evento de riesgo. Lo cual permitirá mitigar 05 eventos de riesgo de nivel extremo.
- ***Evaluación de la Infraestructura Física,*** con la finalidad de que se conozca la situación actual del edificio y poder realizar las correcciones pertinentes, en el caso sea necesario. Lo cual permitirá mitigar 05 eventos de riesgo de nivel extremo.
- ***Digitalización de Documentos,*** con la finalidad de que se pueda evitar la pérdida de información crítica, en caso de ocurrir un evento de continuidad que amenace la documentación física de la empresa.
- ***Evaluar implementación de Luces de emergencia,*** con la finalidad de que el personal cuente con las medidas necesarias para actuar durante la ejecución de un evento de continuidad. Lo cual permite mitigar 05 eventos de riesgo de nivel extremo.

### 5.8.10. CONCLUSIONES

- Se logró identificar las amenazas más importantes para el edificio de la CMAC Ica Camaná, clasificándolas para conocer el nivel de riesgo que tiene cada una.
- Se identificaron los controles actuales, su estado, y su relación con elementos vulnerables para la empresa.

- Se establecieron recomendaciones de controles y se definió los que deben ser aplicados inmediatamente para mitigar las amenazas con mayor riesgo, según los escenarios que se presentan y que se estudiaron.
- El desarrollo completo se encuentra documentado, en este contenido sólo se encuentra el informe final

## CONCLUSIONES

**PRIMERA:**

Se logró desarrollar y diseñar una metodología sistemática, flexible y de fácil comprensión, que incluye las actividades, recomendaciones y procedimientos necesarios para implementar un sistema de gestión de continuidad del negocio, en base a la norma ISO 22301, que se ajusta a cualquier tipo de organización.

**SEGUNDA:**

Para el diseño de la metodología, se logró recolectar y evaluar toda la información sobre los estándares internacionales referidos a la Continuidad del Negocio, extrayendo sus fortalezas y adicionándolas al contenido de la norma ISO 2230; la cual se consideró como base teórica para el desarrollo de la metodología.

**TERCERA:**

Con el desarrollo de un diagnóstico situacional básico de las empresas de Perú y la región Arequipa, se verificó que la implementación de un Sistema de Gestión de Continuidad del Negocio tiene un campo de acción considerable; y es factible para cualquier empresa considerando el recuro tecnológico y financiero.

**CUARTA:**

Se logró diseñar y tener documentada una metodología que contiene los requerimientos y consideraciones de la norma ISO 22301:2012, en un

conjunto de fases y tareas específicas, flexibles y sistemáticas; que mediante una evaluación, busca asegurar la continuidad de las operaciones de cualquier tipo de organización.

**QUINTA:**

Se verificó la aplicación de la metodología, logrando desarrollar, por circunstancias de tiempo y recursos solamente el Análisis de Impacto del Negocio (BIA), y un Análisis de Riesgo para una empresa financiera; siguiendo secuencialmente los pasos de la metodología; lo cual permitió identificar los procesos críticos y amenazas que presenta la organización, estableciendo controles que lograrán apoyar a mantener la continuidad de las operaciones.

## RECOMENDACIONES

**PRIMERA:**

Todas las organizaciones, sin importar su tamaño ni tipo de negocio, deben aplicar, a la medida de sus posibilidades, las actividades de la metodología para estar preparados ante un evento fortuito que afecte sus operaciones

**SEGUNDA:**

La metodología es flexible, y se puede variar las actividades descritas o las formas de evaluación (como se hizo en la financiera donde se aplicó), en relación a las circunstancias y condiciones propias de cada empresa; pero el contenido sí especifica todos los requisitos y requerimientos de la norma.

**TERCERA:**

Se recomienda que las actividades sean desarrolladas en el orden que se presentan en la metodología, ya que es un proceso sistemático debido a que la información de una fase es de utilidad para el desarrollo de la siguiente.

**CUARTA:**

La asignación de recursos para el desarrollo como tiempo y personal, debe evaluarse en relación a la necesidad específica de cada organización y la complejidad de sus funciones.

**BIBLIOGRAFIA**

A., M. (2013). *El incendio del Edificio Windsor un caso real. En: CONFERENCIA UPM TASSI: Planes de Contingencia.* Madrid: Universidad Politécnica de Madrid.

Alejandro, S. V. (2012). *Modelo Integral para la implementación de un Plan de Continuidad de Negocio en Chile.* Arica: Universidad Austral de Chile.

Alexander, A. G. (2007). *Diseño de un Sistema de Gestión de Seguridad de Información. Óptica ISO 27001:2005.* Colombia: Alfaomega.

ANN, Z. (8 de diciembre de 2014). *Wal-Mart respondió a Katrina mejor que el gobierno de USA*. Obtenido de http://www.forodeseguridad.com/artic/admin/5228.htm>

*Banco Central de Reserva*. (05 de noviembre de 2014). Obtenido de http://www.bcrp.gob.pe/docs/Sucursales/Arequipa/2014/sintesis-arequipa-01-2014.pdf

BCI. (2010). Good Practice Guidelines. *BCI*, 108.

*Bolsa de Valores de Lima*. (10 de enero de 2015). Obtenido de http://calidad.pucp.edu.pe/el-asesor/bolsa-de-valores-de-lima-primera-empresa-certificada-en-continuidad-de-negocio#sthash.Q7cjEfVw.dpbs

*CAMARA DE COMERCIO E INDUSTRIA AREQUIPÁ*. (03 de marzo de 2015). Obtenido de http://www.camara-requipa.org.pe/index.php?option=com_content&view=article&id=28&Itemid=210

Candy, C. P. (2012). *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.* Lima: PUCP.

Castro Marquina, L. D. (2013). *DISEÑO DE UN SISTEMA DE GESTIÓN DE CONTINUIDAD DE NEGOCIOS (SGCN) PARA LA RENIEC BAJO LA ÓPTICA DE LA NORMA ISO/IEC 22301.* PUCP.

*Deolitte y Touche (s.f.)*. (10 de enero de 2015). Obtenido de http://www.deloitte.com/view/es_cr/cr/7df967e035fec310VgnVCM2000003356f70aRCRD.htm

GROUP, B. (2006). Code of practice (BS 25999-1: 2006). *Business continuity management*, 50.

GROUP, B. (2008). Code of practice (BS 25777: 2008). *Information and communications technology continuity management.*, 40.

Hiles, A. (2004). *Business Continuity: Best Practices.* Reino Unido: DRI International.

*Instituto Nacional de Estadística e Informática*. (05 de noviembre de 2014). Obtenido de http://www.inei.gob.pe/media/MenuRecursivo/boletines/comportamiento-economia-peruana-2014-i.pdf

*IPE INSTITUTO PERUANO DE ECONOMIA*. (05 de noviembre de 2014). Obtenido de http://www.ipe.org.pe/ahorro

*IPE: INSTITUTO PERUANO DE ECONOMIA*. (02 de febrero de 2015). Obtenido de http://www.ipe.org.pe/documentos/pbi-de-arequipa-crecio-11-en-el-2013-y-este-ano-sera-de-92

ISO. (2005). Security technique - Code of practice for information security management. *ISO 27002: 2005 Information technolog*, 115.

J, G. (2004). *Planes de contingencia: la continuidad del negocio en las organizaciones.* España: Díaz de Santos.

Jimenez, L. d. (2007). *Guía de Desarrollo de un Plan de Continuidad del Negocio.* Madrir: Universidad Politécnica de Madrid.

Negocio, I. c. (08 de diciembre de 2014). *Plan de Manejo de Crisis y Riesgo Empresarial*. Obtenido de http://www.iteam.com.co/index.php?option=com_content&view=article&id=10%3Ariesgos-que-pueden-impactar-negativamente-las-operaciones-normales-de-una-empresa&catid=1%3Aiteam&Itemid=8

P., W. (2007). *Business continuity Management.* Reino Unido: Chartered Management Institute.

SEGUROS, S. D. (2009). *Circular N° G – 139 – 2009.*

# ANEXOS

## ANEXO N° 01 – Organizaciones que regulan la Gestión del Riesgo

Es relevante mencionar que en las últimas décadas se ha observado un crecimiento de una serie de requerimientos legales y regulatorios para una gama de industrias, exigiendo que las empresas desarrollen un sistema de gestión de riesgo, dándole cada vez más importancia al PCN. Así, en el Reino Unido existe el denominado *Turnbull Report* que hace exigencias muy puntuales para las empresas que coticen en bolsa de valores de Londres. En esencia, se exige que las empresas que coticen tengan un sistema de control interno para poder facilitar la gestión de los riesgos del negocio.

En los Estados Unidos aparece el llamado *Sarbanes-Oxley Act*, conocido como el SOX 404. Desde julio del 2002, esta ley requiere que toda empresa que cotice en la bolsa de valores estadounidense tenga instaurado un sistema de análisis de riesgo y controles para mitigarlos.

En el mundo existen las regulaciones de Basilea II, con una serie de exigencias para la banca internacional, en relación con el manejo del riesgo operativo. En la industria alimentaria, en muchos países, existe un requerimiento para realizar el análisis del riesgo exigido por el denominado Hazardous Analysis Critical Control Point (HACCP), convertido recientemente en el ISO 22000.

En los Estados Unidos el Federal Financial Institutions Examination Council (FFIEC) es el organismo encargado específicamente de supervisar los bancos; para asegurar que éstos tienen un adecuado desempeño, exige a cada entidad bancaria y a todas sus sucursales que tengan un PCN implantado y ensayado. (Diseño y Gestión de un Sistema de Seguridad de Información, 2007)

## ANEXO N° 02 – Listado de Amenazas

| AMENAZAS |
|---|
| **DESASTRES NATURALES** |
| Huracanes |
| Inundaciones |
| Incendios |
| **DAÑOS ACCIDENTALES** |
| Fuego fortuito |
| Inundaciones |
| Fallo del aire acondicionado |
| Exceso de humedad |
| Humo, gases tóxicos |
| Subida de tensión |
| Fallo de suministro eléctrico |
| Fallo de la UPS |
| Accidentes del personal |
| Capacidad inadecuada de las comunicaciones |
| Fallo/degradación del hardware |
| Fallo/degradación de las comunicaciones |
| Errores de operación |
| Fallos en las copias de seguridad |
| Fallos de los sistemas de autenticación/autorización |
| Pérdida de confidencialidad |
| Incumplimientos legales |
| **ATAQUES INTENCIONADOS** |
| Explosivos |
| Fuego intencionado |
| Accesos no autorizados al edificio |
| Actos de vandalismo |
| Radiaciones electromagnéticas |
| Robos intencionados |
| Manipulación de datos/software |
| Manipulación de hardware |
| Uso de software por personal no autorizado |
| Acceso no autorizados a datos de la compañía |
| Software malicioso |

| |
|---|
| Robo de equipos<br>Descarga de software no controlada |
| Robo de documentos |
| Interceptación de las líneas de comunicación |
| Manipulación de las líneas de comunicación |
| Abuso de privilegios de acceso |
| Introducción de virus en los sistemas |
| Ataques por ingeniería social |
| Bombas lógicas |
| Errores en el mantenimiento |
| Corrupción de datos |
| Incumplimientos legales intencionados |

Fuente: Laura del Pino (2007). Elaboración propia.

## ANEXO N° 03 – Ejemplos de Vulnerabilidades

| VULNERABILIDADES |
|---|
| Existencia de materiales inflamables como papel o cajas |
| Cableado inapropiado |
| Ancho de banda inapropiado |
| Suministro eléctrico inapropiado |
| Mantenimiento inapropiado del servicio técnico |
| Ausencia de mantenimiento |
| Educación inadecuada del personal en virus y malware |
| Políticas de firewall inadecuadas |
| Política de seguridad de la información inadecuada |
| Ausencia de política de seguridad |
| Derechos de acceso incorrectos |
| Ausencia de un sistema de extinción automática de fuegos/humos |
| Ausencia de backup |
| Ausencia de control de cambios de configuración eficiente y efectiva |
| Ausencia de mecanismos de identificación y autenticación |
| Ausencia de política de restricción de personal para uso licencias de software |
| Ubicación física en un área susceptible de desastres naturales |
| Carencia de software antivirus |
| Descarga incontrolada y uso de software de Internet |
| Ausencia de mecanismos de cifrado de datos para la transmisión de datos confidenciales |
| Protección física de equipos inadecuada |
| Personal sin formación adecuada |
| Incumplimientos legales (LOPD, Ley Sarbanes Oxley, etc.) |
| Definición de privilegios de acceso inadecuada |
| Ausencia de un Plan de recuperación de incidentes |

Fuente: Laura del Pino (2007). Elaboración propia.

## ANEXO N° 04 – Tipos de controles

Para reducir riesgos se utilizan los denominados controles o medidas de seguridad. Podemos clasificar los controles en:

**Controles preventivos**

- Identifican potenciales problemas antes de que ocurran
- Previenen errores, omisiones o actos maliciosos.

Ejemplos:

- Realizar copias de seguridad de los archivos.
- Contratar seguros para los activos.
- Establecer procedimientos / políticas de seguridad.
- Establecer control de acceso a la información.
- Establecer control de acceso físico.

**Controles detectivos:**

- Identifican y “reportan” la ocurrencia de un error, omisión o acto malicioso ocurrido.

Ejemplos:

- Monitorización de eventos.
- Auditorías internas.
- Revisiones periódicas de procesos.
- Sensores de humo.
- Detección de virus (Antivirus).

**Controles Correctivos:**

- Minimizan el impacto de una amenaza.
- Solucionan errores detectados por controles detectivos.

- Identifican la causa de los problemas con el objeto de corregir errores producidos.
- Modifican los procedimientos para minimizar futuras ocurrencias del problema.

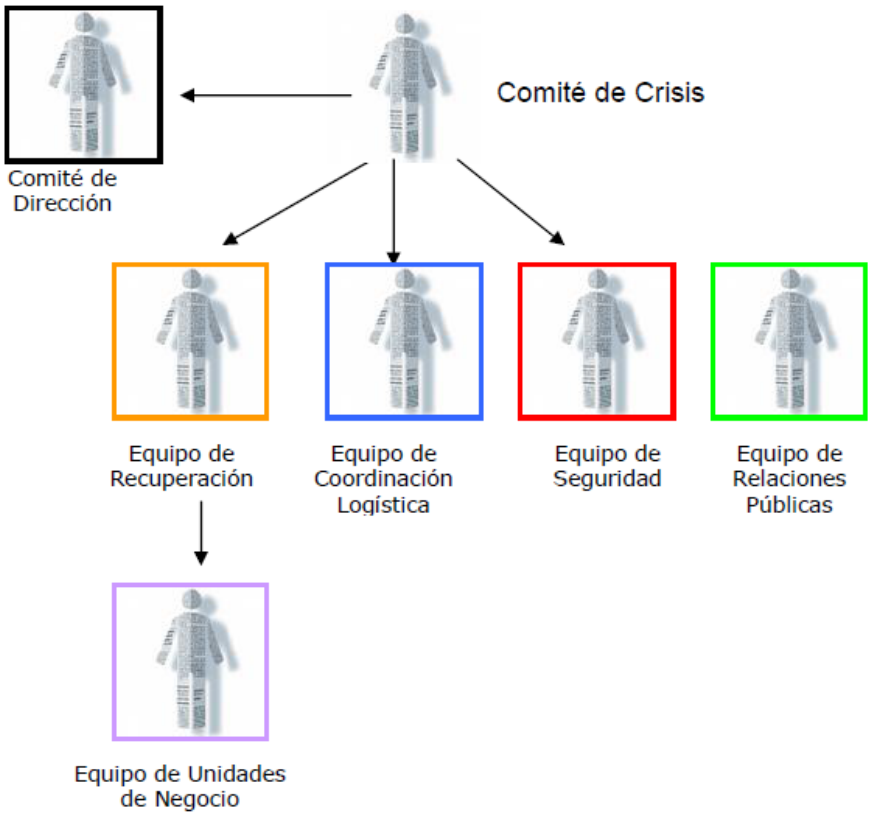
Ejemplos:

- Parches de seguridad.
- Corrección de daños por virus.
- Recuperación de datos perdidos.

Las medidas seleccionadas para mitigar riesgos deben mantener una proporción entre el esfuerzo y coste necesarios para su implantación y el riesgo que mitigan (evaluación del coste-beneficio).[2]

[2] Extraído de: www.cert.org/octave/ Visitado: 17/02/2015 Metodología de Análisis de Riesgos OCTAVE

## ANEXO N° 05 – Árbol de Llamadas




Fuente: Revista de Seguridad SIC. (Perú, 2010)

## ANEXO N° 06 – Lista de Procesos CMAC Ica

| |
|---|
| CN-Cierre Diario |
| CN-Creación y Modificación de una Cuenta |
| CN-Registro de Asientos Manuales y de Ajustes |
| CN-Análisis y Validación del Registro de Operaciones Contables |
| CN-Análisis de Cifras |
| CN-Conciliación Bancaria |
| CN-Generación de Estados Financieros Anexos y Reportes |
| CN-Registro Complementarios y Opcionales |
| CN-Archivo y Custodia de Documentos |
| CN-Cierre Mensual |
| CN-Cierre Anual |
| CR-PROMOCION DE CREDITO |
| CR-SOLICITUD DE CREDITO |
| CR-EVALUACION DE CREDITO |
| CR-APROBACION DE CREDITOS |
| CR-DESEMBOLSO DE CREDITO |
| CR-SEGUIMIENTO Y RECUPERACION DE CREDITO |
| RG-Calificación de Cartera de Colocaciones |
| RG-Elaboración de Anexos y Reportes y remisión via SUCAVE |
| RG-Envió de Anexo 15-A |
| RG-Envió de Estadísticas FEPMAC |
| RG-Informe de Opinión de Créditos |
| RG-Elaboración de Informes de Riesgos |
| RG-Administración de Riesgos |
| RG-Reporte de Liquidez Adelantada |
| OP-Promoción |
| OP-Inicio de cajero |
| OP-apertura de cuentas (ahorro, DPF y CTS) |
| OP-movimientos en cuentas de operaciones de ahorro |
| OP-cancelaciones de cuentas de ahorro |
| OP-Operaciones Intercalas |
| OP-Ingreso de expedientes |
| OP-Desembolso de Créditos |
| OP- Cobranzas de créditos |
| OP-Servicio de Cobranza APAFAS |
| OP-cierre de operaciones |
| TS-apertura y registro de cuentas. |
| TS-Control de Encaje |
| TS-Emisión diaria de Reporte de tesorería |
| TS-Remesas de Efectivo de Bancos |
| TS-Pago a proveedores |

| |
|---|
| TS-Abono de planilla y liquidaciones |
| TS-Transferencias bancarias |
| TS-Corresponsalía Banco de la Nación |
| TS-Habilitaciones de efectivo a ventanillas |
| TS-Habilitaciones de efectivo a agencias |
| TS-Custodia de Valores |
| PL-ELABORACION DE METAS |
| PL-ELABORACION DEL PRESUPUESTO INSTITUCIONAL |
| PL-IMPLEMENTACION DE PRODUCTOS |
| PL-ELABORACION DEL PLAN ESTRATEGICO |
| RH-Selección de personal |
| RH-Administración de personal |
| RH-Desarrollo de personal |
| RH-Jubilación o término de la relación laboral |
| LG-Compras y adquisiciones |
| LG-Gestión de almacenes |
| LG-Administración de Bienes patrimoniales |
| LG-Servicios Generales |
| AU-Acciones de Control |
| AU-Actividades de Control |
| AU-Elaboración de Informes |
| LI-Proceso de Constitución de Garantías Preferidas |
| LI-Proceso de Cancelación de Garantías Preferidas |
| LI-Proceso de Actualización de Valuaciones |
| LI-Proceso de Contratación de Pólizas de Seguros de Bienes con Garantía Preferida |
| LI-Proceso de Evaluación, Seguimiento y Control de Acciones Judiciales |
| LI-Proceso de Visación de Contratos (en general) |
| OM-Elaboración de Reglamento de la CMAC |
| OM-Elaboración de Manual de Políticas y Procedimiento |
| OM-Elaboración de Directivas |
| OM-Capacitación de los Manuales a los usuarios |
| OM-Elaboración del Organigrama institucional y funciones |
| SF-Captación de depósitos |
| SF-Colocación de créditos |
| SF-Recuperación de créditos |
| SF-acceso locales bóveda y caja fuerte |
| SF-acceso de claves sensibles |
| SF-apertura y ampliación de caja chica |
| SF-custodia de valores |
| SF-aprobación de créditos |
| SF-pagos servicios de luz, agua y telefonía |
| SF-reporte contable diario |
| SF-cierre diario de operaciones |
| SF-control archivo documentario de la agencia |
| SF-emisión y cancelación de órdenes de Pago |

| |
|---|
| SF-traslado de dinero Prosegur de agencia |
| AT-ORIENTACION AL USUARIO |
| AT-INFORMACIÓN AL USUARIO |
| AT-IMPLEMENTACION DEL AREA |
| AT-ATENCIÓN DE RECLAMOS |
| AT-VERIFICAR LOS MEDIOS DE DIFUSIÓN |
| AT-SELECCIÓN DE PERSONAL ENCARGADO |
| AT-COMUNICACIÓN PERIODICA AL USUARIO |
| AT-CUMPLIMIENTO DE LA NORMATIVIDAD PERTINENTE |

Fuente: Talleres de SGCN, CMAC ICA. Elaboración propia.

**ANEXO N° 07 – Lista de Sistemas de la CMAC Ica**

| |
|---|
| Cierre diario / mensual |
| Flamenco - Créditos |
| Flamenco - Ahorros |
| Flamenco - Clientes |
| Flamenco - Prendario |
| Flamenco - Judicial |
| Flamenco - Caja General |
| Flamenco - Contabilidad |
| Flamenco - Logística |
| Flamenco - Presupuesto |
| Flamenco - Riesgos |
| Flamenco - Administración |
| Flamenco - Planillas |
| Flamenco - Reportes |
| Correo Electrónico |
| Servicio Web |
| ACL |
| SAGU |
| PDT |
| Ofimatica |

Fuente: Talleres del SGCN, CMAC ICA. Elaboración propia.

## ANEXO N° 08 – Documentos y Registros necesarios por ISO 22301:2012

| DOCUMENTOS Y REGISTROS | Punto en ISO 22301 |
|---|---|
| Determinación del contexto de la organización | 4.1 |
| Procedimiento para identificación de requerimientos legales y normativos aplicables | 4.2.2 |
| Lista de requisitos legales, normativos y de otra índole | 4.2.2 |
| Alcance del SGCN (Sistema de gestión de la continuidad del negocio) y explicación de las exclusiones | 4.3 |
| Política de la continuidad del negocio | 5.3 |
| Objetivos de la continuidad del negocio | 6.2 |
| Competencias del personal | 7.2 |
| Comunicación con las partes interesadas | 7.4 |
| Proceso para análisis de impactos en el negocio y evaluación de riesgos | 8.2.1 |
| Resultados del análisis del impacto en el negocio | 8.2.2 |
| Resultados de la evaluación de riesgos | 8.2.3 |
| Procedimientos de la continuidad del negocio | 8.4.1 |
| Procedimientos de respuesta a incidentes | 8.4.2 |
| Decisión sobre si los riesgos e impactos se deben comunicar externamente | 8.4.2 |
| Comunicación con las partes interesadas, incluido el sistema nacional o regional de asesoramiento de riesgos | 8.4.3 |
| Registros de información importante sobre el incidente, medidas adoptadas y decisiones tomadas | 8.4.3 |
| Procedimientos para respuesta ante incidentes disruptivos | 8.4.4 |
| Procedimientos para restaurar y reiniciar actividades a partir de las medidas temporales | 8.4.5 |
| Resultados de las acciones que abordan tendencias o resultados adversos | 9.1.1 |
| Datos y resultados de seguimiento y medición | 9.1.1 |
| Resultados de la revisión posterior al incidente | 9.1.2 |
| Resultados de la auditoría interna | 9.2 |
| Resultados de la revisión por parte de la dirección | 9.3 |
| Naturaleza de las no conformidades y acciones tomadas | 10.1 |
| Resultados de acciones correctivas | 10.1 |

Fuente: ISO 27001 Academy, Información de la norma ISO 22301.

## ANEXO N° 09 – Resolución SBS N° 2116 - 2009

En el siguiente anexo, se adjunta la resolución que define obligaciones para administración del riesgo operativo de las empresas que supervisa la SBS. Dentro de estas se encuentra, como una actividad obligatoria para estas empresas, el establecimiento de actividades ligadas a la continuidad del negocio. Se presenta algunas consideraciones, y el artículo donde se menciona dentro de la resolución en la Gestión del Riesgo Operacionales, la mención a las actividades de continuidad:

*Resolución S.B.S.*
*N° 2116 -2009*

*El Superintendente de Banca, Seguros y*
*Administradoras Privadas de Fondos de Pensiones*

**CONSIDERANDO:**

Que, mediante la Resolución SBS N° 37-2008 del 10 de enero de 2008, se aprobó el Reglamento de la Gestión Integral de Riesgos, que establece que las empresas supervisadas deben contar con una gestión integral de riesgos adecuada a su tamaño y a la complejidad de sus operaciones y servicios;

Que, entre los riesgos que enfrentan las empresas supervisadas en el desarrollo de sus actividades se encuentra el riesgo operacional, el cual puede generarse por deficiencias o fallas en los procesos internos, en la tecnología de la información, en las personas o por ocurrencia de eventos externos;

**LA GESTIÓN DEL RIESGO OPERACIONAL**

**Artículo 13°.- Gestión de la continuidad del negocio y de la seguridad de la información**
Como parte de una adecuada gestión del riesgo operacional, las empresas deben implementar un sistema de gestión de la continuidad del negocio que tendrá como objetivo implementar respuestas efectivas para que la operatividad del negocio de la empresa continúe de una manera razonable, ante la ocurrencia de eventos que pueden crear una interrupción o inestabilidad en las operaciones de la empresa.

Asimismo, las empresas deben contar con un sistema de gestión de la seguridad de la información, orientado a garantizar la integridad, confidencialidad y disponibilidad de la información.

Para ello, las empresas deberán aplicar las disposiciones que se establezcan en las normas específicas sobre estos temas.

## ANEXO N° 10 – Circular N° G-139-2009

En el siguiente anexo, la SBS establece disposiciones mínimas necesarias para las actividades de Gestión de Continuidad del Negocio. Se presentan los puntos más importantes:

Lima, 02 de abril de 2009

**CIRCULAR Nº G- 139 -2009**

---

Ref.: Gestión de la continuidad del negocio

---

Señor
Gerente General
Sírvase tomar nota que, en uso de las atribuciones conferidas por el numeral 7 del artículo 349º de la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros - Ley Nº 26702 y sus modificatorias en adelante Ley General, y por el inciso d) del artículo 57° del Texto Único Ordenado de la Ley del Sistema Privado de Administración de Fondos de Pensiones aprobado por el Decreto Supremo N° 054-97-EF, con la finalidad de establecer criterios mínimos para la gestión de la continuidad del negocio, que forma parte de una adecuada gestión del riesgo operacional que enfrentan las empresas supervisadas, esta Superintendencia ha considerado conveniente establecer las siguientes disposiciones, las cuales toman como referencia estándares internacionales como el BS-25999, disponiéndose su publicación en virtud de lo señalado en el Decreto Supremo N° 001-2009-JUS:

**Alcance**

Artículo 1º.- La presente Circular será de aplicación a las empresas señaladas en los artículos 16° y 17° de la Ley General, así como a las Administradoras Privadas de Fondos de Pensiones (AFP), en adelante empresas. También será de aplicación a las Cajas Municipales de Ahorro y Crédito (CMAC), la Caja Municipal de Crédito Popular, el Fondo de Garantía para Préstamos a la Pequeña Industria (FOGAPI), el Banco de la Nación, el Banco Agropecuario, la Corporación Financiera de Desarrollo (COFIDE), el Fondo MIVIVIENDA S.A., las Derramas y Cajas de Beneficios bajo control de la Superintendencia, la Federación Peruana de Cajas Municipales de Ahorro y Crédito (FEPCMAC) y el Fondo de Cajas Municipales de Ahorro y Crédito (FOCMAC), en tanto no se contrapongan con las normativas específicas que regulen el accionar de estas empresas.

**Gestión de la continuidad del negocio**

Artículo 3º.- 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. Las empresas deben realizar una gestión de la continuidad del negocio adecuada a su tamaño y a la complejidad de sus operaciones y servicios.

**Responsabilidad del Directorio**

Artículo 4º.- El Directorio es responsable de establecer una adecuada gestión de la continuidad del negocio. Entre sus responsabilidades específicas están: a. Aprobar una política general que defina el alcance, principios y guías que orienten la gestión de la continuidad del negocio. b. Aprobar los recursos necesarios para el adecuado desarrollo de la gestión de la continuidad del negocio, a fin de contar con la infraestructura, metodología y personal apropiados. c. Obtener

aseguramiento razonable que la empresa cuenta con una efectiva gestión de la continuidad del negocio.

**Responsabilidad de la Gerencia**

Artículo 5º.- La gerencia general tiene la responsabilidad de implementar la gestión de la continuidad del negocio conforme a las disposiciones del Directorio. La gerencia podrá constituir comités para el cumplimiento de sus responsabilidades relacionadas con la gestión de la continuidad del negocio.

**Fases de la gestión de la continuidad del negocio**

Artículo 8º.- Las empresas deberán desarrollar como mínimo las siguientes fases como parte de la gestión de la continuidad del negocio:

**8.1. Entendimiento de la organización** Esta fase consiste en conocer los objetivos y metas de la empresa; identificar los principales procesos, productos, servicios y proveedores, así como las actividades y recursos requeridos; evaluar los riesgos que podrían causar una interrupción de dichas actividades, y el impacto que podría tener dicha interrupción.

Las actividades mínimas a desarrollar durante esta fase son las siguientes:

a. Análisis de impacto: Consiste en determinar el impacto que tendría una interrupción de los procesos que soportan los principales productos y servicios de la empresa. Para ello, deben considerarse aspectos como: daños a la viabilidad financiera de la empresa, daños a su reputación, incumplimiento de requerimientos regulatorios, daños al personal o al público en general. Según ello, debe establecerse el período máximo tolerable de interrupción por cada uno de estos procesos. El análisis de impacto debe ser revisado periódicamente y actualizado cuando existan cambios en la organización o en su entorno, que puedan afectar sus resultados.
b. Evaluación de riesgos: Consiste en identificar y evaluar los riesgos que podrían causar una interrupción del negocio. Para ello, deberá seguirse una metodología consistente con aquella utilizada para la evaluación de los demás riesgos que enfrenta la empresa. La empresa debe definir qué procesos requieren contar con una estrategia de continuidad de negocios, considerando los resultados del análisis de impacto y de la evaluación de riesgos

**8.2. Selección de la estrategia de continuidad** En esta fase, se determinan las estrategias de continuidad que permitirán mantener las actividades y procesos de negocio luego de ocurrido un evento de interrupción de operaciones. Debe desarrollarse, como mínimo, la siguiente actividad: Evaluación y selección de estrategias de continuidad por proceso: Se refiere a seleccionar las estrategias que permitirán mantener la continuidad de los procesos que soportan los principales productos y servicios de la empresa, dentro del tiempo objetivo de recuperación, definido para cada proceso.

**8.3. Desarrollo e implementación de la estrategia de continuidad** En esta fase, se deben desarrollar los planes de respuesta ante los eventos analizados en las fases previas, e implementar un modelo de respuesta flexible y escalable que permita cubrir los eventos inesperados y proveer los recursos necesarios, acorde con la estrategia seleccionada, para enfrentar con éxito un evento de interrupción de operaciones.

**8.4. Pruebas y actualización** Los planes de continuidad del negocio deberán ser probados cuando menos una vez al año. A continuación se detallan las actividades mínimas que deben ser aplicadas en esta fase: a. Ejecución de pruebas: El alcance de las pruebas debe ser consistente con el alcance de los planes de continuidad del negocio. Cada prueba debe tener objetivos definidos y un reporte que resuma los resultados alcanzados y recomendaciones. Esta información debería ser usada para mejorar los planes de continuidad del negocio en forma oportuna. Pueden aplicarse diferentes tipos de prueba, desde las pruebas de escritorio hasta las simulaciones completas de escenarios de interrupción de operaciones. Las empresas deberán asegurarse que sus principales proveedores de servicios cuenten con planes de continuidad y

que éstos cumplan con lo señalado en el presente numeral. b. Actualización de los planes: Las empresas deben definir políticas y procedimientos para la actualización de los planes de gestión de la continuidad del negocio, de tal manera que cualquier cambio que impacte a la empresa (ya sea interno o externo) sea revisado en relación con la continuidad del negocio.

**8.5. Integrar la gestión de la continuidad del negocio a la cultura organizacional** Las actividades mínimas a desarrollar en esta fase son las siguientes: a. Evaluación del grado de conocimiento sobre la gestión de continuidad: Tiene como objetivo determinar el nivel de conocimiento actual y esperado sobre la gestión de continuidad del negocio, los procedimientos implementados, las tareas específicas señaladas en los planes de continuidad, entre otros aspectos. b. Desarrollo y mejora de la cultura de continuidad: Diseñar e implementar planes de capacitación y entrenamiento, a fin de cubrir las deficiencias encontradas en la actividad previa. c. Monitoreo permanente: Revisar periódicamente el nivel de entendimiento de la gestión de continuidad del negocio a fin de identificar requerimientos adicionales.

**Cambios significativos**

Artículo 10°.- Las empresas analizarán el impacto que tienen los cambios significativos sobre la continuidad del negocio. Los cambios significativos podrán considerar entre otros: cambio de la infraestructura tecnológica que soporta los principales productos y/o servicios, fusión con otra empresa, implementación de un nuevo producto, cambio de un proveedor principal, cambio de oficina principal, entre otros.

**Auditoría Interna**

Artículo 11º.- La Unidad de Auditoría Interna evaluará el cumplimiento de lo dispuesto en la presente norma de acuerdo a su plan de trabajo.

**Plan de Adecuación**

Artículo 12°.- En un plazo que no excederá de noventa (90) días calendario de haberse publicado la presente Circular, las empresas deberán remitir a la Superintendencia un plan de adecuación a las disposiciones contenidas en la presente norma. Dicho plan deberá incluir un diagnóstico de la situación existente en la empresa respecto al cumplimiento de cada uno de los artículos de la presente Circular, las acciones previstas para la total adecuación y el cronograma de las mismas, así como los funcionarios responsables del cumplimiento de dicho plan.

**Vigencia y Plazo de Adecuación**

Artículo 13°.- La presente Circular entra en vigencia a partir del día siguiente a su publicación en el Diario Oficial El Peruano, otorgándose para su cumplimiento un plazo de adecuación hasta el 31 de marzo de 2010. A partir de dicha fecha, queda derogado el artículo 83° del Título III del Compendio de Normas de Superintendencia Reglamentarias del Sistema Privado de Administración de Fondos de Pensiones, referido a Gestión Empresarial.