UNIVERSIDAD NACIONAL "PEDRO RUIZ GALLO"

FACULTAD DE CIENCIAS FISICAS Y MATEMATICAS

ESCUELA PROFESIONAL DE INGENIERÍA EN COMPUTACIÓN E INFORMÁTICA

"PLAN INFORMÁTICO PARA BRINDAR CONTINUIDAD OPERATIVA A LAS ENTIDADES FINANCIERAS EN EL PERÚ"

TESIS

PARA OPTAR EL TITULO DE :

INGENIERO EN COMPUTACIÓN E INFORMATICA

PRESENTADO POR EL BACHILLER:

BENJAMIN HUMBERTO QUIÑONES QUIÑONES

ASESOR

ING. PEDRO FIESTAS RODRIGUEZ

LAMBAYEQUE - PERÚ
2014

"PLAN INFORMÁTICO PARA BRINDAR CONTINUIDAD OPERATIVA A LAS ENTIDADES FINANCIERAS EN EL PERÚ"

ELABORADO POR:

BACH. BENJAMIN HUMBERTO QUIÑONES QUIÑONES

APROBADO POR:

ING. PEDRO FIESTAS RODRIGUEZ
ASESOR

ING. ARMANDO MORENO HEREDIA
PRESIDENTE DEL JURADO

ING. JANET AQUINO LALUPÚ
MIEMBRO DEL JURADO

ING. LUIS REYES LESCANO
MIEMBRO DEL JURADO

"PLAN INFORMÁTICO PARA BRINDAR CONTINUIDAD OPERATIVA A LAS ENTIDADES FINANCIERAS EN EL PERÚ"

ELABORADO Y PRESENTADO POR:

BACH. BENJAMIN HUMBERTO QUIÑONES QUIÑONES

A mi esposa Carmen y a mi hijita Ariana Cristel por su ayuda constante que me motivó a ser perseverante para cumplir con mis objetivos.

A mis padres José Domingo y Tarcila por haberme brindado todo lo necesario para cumplir con cada uno de mis objetivos tanto profesionales como personales, a mis hermanos: José y Carmen y a mis sobrinos: Andrea, Amalia, Joab y Luciana por su íntegro apoyo.

Un agradecimiento especial a todos mis amigos que con su apoyo desinteresado me ayudaron a realizarme como persona y profesional.

Benjamin Humberto Quiñones Quiñones

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

Este tema de investigación propone una guía para gestionar la Continuidad y Contingencia Operativa de un Banco en el Sector Financiero Peruano. En la primera parte se introduce al tema, presentando el problema de la investigación, los alcances y objetivos de la tesis.

En el cual se explica la importancia de contar con una estrategia de continuidad y contingencia, así como también, se definen los conceptos básicos de: amenazas, vulnerabilidades, riesgos y desastres tanto naturales como los causados por el hombre.

Luego se desarrolla el Marco legal, en el que se revisan las reglas que las entidades financieras deben cumplir, indicadas por los organismos reguladores en el Perú, así también se revisan las mejores prácticas de gestión de continuidad en el mundo. Dentro de los organismos reguladores se encuentran Defensa civil, que cumple la función de velar por el bienestar de la comunidad, y la Superintendencia de Banca, Seguros y AFP, la cual regula al sistema financiero peruano.

Como tema principal, en el Marco teórico, se desarrolla el Planeamiento de continuidad operativa de negocios, en el que se describe la evolución del concepto "Continuidad de Negocios" y se definen otros conceptos como Gestión

de Continuidad de Negocios, Programa y Plan de Continuidad del Negocio, para finalmente listar las metodologías más resaltantes respecto al tema de Continuidad, como son: Metodología BCI – Business Continuity Institute, Metodología DRII – Disaster Recovery Institute International, Metodología Strohl Systems.

En el siguiente Capítulo se desarrolla el análisis del entorno y del sector. En el análisis del entorno se describen los riesgos a los que están expuestos los negocios en el mundo, brindando algunos ejemplos de desastres naturales y su impacto, así como eventos destructivos causados por el hombre y su impacto. Por otro lado, se describen los riesgos a los que están expuestos los negocios en el Perú.

Luego se describe el Plan de continuidad operativa de negocios en el cual se incorporan los Planes de Recuperación y Continuidad, estos son: Planes de Recuperación de desastres y Planes de continuidad operativa del negocio.

Antes de empezar el plan de continuidad de negocios se debe obtener el compromiso y soporte de la alta gerencia, sin esto el plan no dará los resultados esperados. La siguiente actividad es definir los objetivos, supuestos o premisas, alcances, políticas y el propósito.

Luego, al tener identificados los procesos de negocio, se debe definir tiempos de recuperación para cada uno, dependiendo de los objetivos de recuperación (tiempo y pérdida de información). Al final del análisis de impacto en

el negocio, los procesos de negocio son calificados y clasificados según su criticidad.

En este capítulo también se propone la recuperación de información en un centro alterno, para lo cual se detallan los tipos de instalaciones alternativas para respaldo y formas de respaldar la información.

A continuación, se definen las estrategias a partir de diferentes escenarios, las que serán utilizadas para el desarrollo e implementación del plan de continuidad.

Como tema importante, se desarrollan los Planes de gestión de crisis, los que indican cómo responder a una emergencia, cómo administrar incidentes y cómo administrar una crisis global o mayor, también se propone, como parte importante de la administración de crisis, un plan de administración de las comunicaciones dentro y fuera de la organización.

Para afianzar y familiarizar a los equipos de respuesta con los planes de continuidad se plantean programas de capacitación. Así como también se sugieren programas de capacitación a los usuarios para lograr su concientización en el tema.

Luego de tener el plan de continuidad operativa del negocio desarrollado, es necesario probarlo, para lo cual se debe generar un plan de pruebas en el que se incluyan diferentes escenarios de prueba.

Con el fin de mantener el plan de continuidad constantemente actualizado y validado, se recomienda formar en la organización, una unidad interna para la gestión de continuidad de negocio en la que los equipos están formados por los líderes de la organización. Estos equipos tendrán tareas y responsabilidades permanentes, durante la interrupción, la recuperación y durante el período de retorno a la normalidad.

Finalmente se desarrollan las conclusiones y recomendaciones del presente tema de investigación.

Benjamin Humberto Quiñones Quiñones

INTRODUCCION

El presente plan de continuidad operativa de negocios tiene la intención de servir de guía a las empresas del sector financiero del Perú, específicamente a los Bancos peruanos. La idea en este trabajo es brindar las pautas y ejemplos para el desarrollo de un plan de continuidad incluyendo un plan de recuperación de desastres, de modo que aseguren en gran medida la disponibilidad de las operaciones y del servicio al cliente, aún después de la ocurrencia de un evento que interrumpa los procesos del negocio.

El plan de recuperación contra desastres (DRP) se considera como un control correctivo. No se trata por tanto de prevenir o detectar posibles desastres, sino de limitar las pérdidas ocasionadas por desastres comunes. La prevención o detección de eventos que pudieran desencadenarse en desastres es tarea del plan de seguridad física y del plan de seguridad informática, así también de la unidad de administración de riesgos.

Como primer paso se debe asumir que los desastres sí ocurren, y estos impactan directamente en la infraestructura tecnológica de una empresa. Un plan de contingencia permite la recuperación rápida de las capacidades de procesamiento de información crítica para la supervivencia de la empresa de manera que pueda continuar brindando eficiente y eficazmente productos y servicios a los clientes.

La preparación de los planes mencionados se basa principalmente en el conocimiento de los procesos del negocio, aquellos procesos que son críticos para la continuidad del negocio, entonces se deben categorizar los procesos, así como las aplicaciones que los soportan. Las aplicaciones son importantes debido a que de ellas depende el procesamiento de la información de los procesos del negocio.

CAPÍTULO I: ASPECTOS DE LA INVESTIGACIÓN

1.1. Situación Problemática

Es cierto que en el Perú no se tienen huracanes ni tornados, pero si existe la probabilidad de que sucedan desastres naturales como terremotos, tsunamis, o desastres causados, directa o indirectamente, por el hombre como terrorismo, incendios, etc. Estos desastres podrían tener un impacto sumamente negativo en la empresa, dependiendo de la magnitud podrían tener efectos devastadores en la infraestructura informática y las aplicaciones críticas del negocio, con lo que la empresa tendría graves dificultades para continuar operando. En el caso de un Banco, no podría continuar con la atención a sus clientes lo que causaría una mala imagen, además de las pérdidas económicas.

Debido a lo mencionado es importante que toda empresa cuente con planes preventivos, así como con planes reactivos, ya que también se debe conocer cómo y en qué orden responder a un evento que impacte negativamente a la empresa. Entre los planes preventivos se debe desarrollar un plan de seguridad informática, pero sucede que hasta el día de hoy el tema de seguridad sigue siendo el tema menos tratado en muchas empresas, en el Perú gracias a las exigencias del ente regulador de la Banca, los Bancos peruanos han venido desarrollando planes de

seguridad, han despertado su interés por adoptar medidas preventivas, así también la regulación obliga a desarrollar planes de contingencia informática, el problema es que estos planes suelen ser olvidados o son pospuestos año tras año en el presupuesto informático, en el caso de que el Banco cuente con un plan de contingencia, se tiene otro problema: el plan no es actualizado hasta que se necesite. Un plan de contingencia, de recuperación o de continuidad es tan válido como tan actualizado esté.

¿Cuántos Bancos peruanos han analizado el riesgo y el impacto que supondría la pérdida del procesamiento de sus operaciones por varios días o meses?, dado este caso, realmente ¿podrían garantizar la continuidad del negocio?, el mejor escenario podría ser una pérdida cuantiosa, el peor escenario sería la desaparición de la empresa.

1.2. Problema

¿Las Instituciones Financieras en el Perú podrían garantizar la continuidad del negocio ante un desastre?

1.3. Hipótesis

Los planes de continuidad operativa del negocio y de recuperación de desastres, aplicados a los bancos peruanos, asegurarán la continuidad de la atención a sus clientes ante cualquier evento inesperado, lo que mitigará la pérdida de imagen y las pérdidas económicas.

La administración de continuidad de negocios facilitará la coordinación entre las unidades de la organización para desarrollar y mantener constantemente actualizados los planes de continuidad operativa del negocio y de recuperación de desastres.

1.4. Objetivos

1.4.1. Objetivo General

Brindar al sector financiero del Perú, específicamente al sistema bancario, un plan compuesto de procedimientos y recomendaciones que les sirva como guía para el desarrollo e implementación de sus propios planes de continuidad operativa y de recuperación, planes que les servirán en el caso de que se presente un evento que ocasione la interrupción prolongada y no planeada del negocio, de manera que puedan definir los tiempos óptimos de recuperación de sus operaciones con la mínima pérdida de información.

1.4.2. Objetivos Específicos

Proveer a los bancos del sector financiero del Perú de un plan de continuidad operativa y de recuperación que permitan continuar con las operaciones normales del negocio en caso de desastre, en un período de tiempo acordado y aprobado por la Alta Dirección, tanto para casos que puedan resolverse dentro de la región, como para aquellos casos extremos en los que sea necesario activar un centro de datos alterno fuera de la región.

Proporcionar a los bancos peruanos, propuestas para el diseño, desarrollo e implementación, así como para la elaboración de flujos de procesos, normas y políticas necesarias para mantener un plan de continuidad y de recuperación permanentemente actualizado de manera que se mantenga vigente con el pasar del tiempo y no se vea afectado por los continuos cambios en los procesos de negocios, aplicaciones e infraestructura tecnológica, los cuales deberán ser reflejados en el plan.

Brindar un modelo o metodología que permita a las unidades internas de la organización, evaluar periódicamente la vigencia del plan de continuidad y recuperación, detectar oportunidades de mejora y retroalimentar el mantenimiento del plan, por medio de los ejercicios continuos, sean con o sin intervención o interrupción en los sistemas y aplicaciones, planificados o sorpresivos.

1.4.3. Justificación e Importancia

Proponer a los bancos peruanos una guía sencilla que les permita desarrollar un plan de continuidad operativa a su medida, que simplifique la actualización del mismo, el cual finalmente contribuirá a mantener la atención a sus clientes incluso después de ocurrido un desastre, aumentando así la confiabilidad de la empresa.

1.4.4. Alcance de la investigación

El alcance de la presente investigación comprende los siguientes aspectos:

- ✓ Investigar los riesgos en el Perú según ubicación geográfica, profundizando el estudio en el departamento de Lima.
- ✓ Resaltar la existencia de la probabilidad de ocurrencia de desastres naturales y humanos en la realidad peruana.
- ✓ Analizar los estándares y mejores prácticas, así como la regulación peruana sobre continuidad y recuperación de desastres.
- ✓ Describir la situación actual del riesgo operativo de los bancos en el sector financiero peruano.
- ✓ Analizar la importancia del desarrollo de planes de continuidad operativa de los procesos del negocio y planes de recuperación de la infraestructura tecnológica ante un desastre.
- ✓ Analizar el impacto de no contar con un plan adecuado sobre continuidad operativa del negocio en el sector financiero.
- ✓ Desarrollar un plan de acción que sirva como guía para asegurar la continuidad operativa de un Banco.
- ✓ Proponer un plan de recuperación del sistema informático de manera que la empresa pueda continuar con sus operaciones en caso de desastre.
- ✓ Esquematizar cada fase del plan de continuidad operativa mediante flujos de procesos de manera que sea fácilmente adaptable a cualquier entidad financiera.

2.1. Importancia de una estrategia de continuidad de negocios

Los negocios no están preparados para lo peor, ¿qué pasaría si toda la infraestructura tecnológica es interrumpida por un desastre natural?. La recuperación de un desastre antes era considerada solo para grandes corporaciones, hoy es necesario en empresas de cualquier tamaño.

Figura 1 Caricatura Plan de Recuperación de Desastres

Fuente: Wayne Pollock, Tampa Florida USA.

2.2. Definiciones de amenazas, vulnerabilidades, riesgos y desastres

2.2.1. ¿Qué es una amenaza?

Es la probabilidad de ocurrencia de un fenómeno natural o inducido por el hombre que puede ocasionar graves daños a una localidad o territorio. Las principales amenazas a las que estamos expuestos en el Perú son los terremotos, sequías, inundaciones, aluviones, deslizamientos, heladas, maremotos y erupciones volcánicas.

De acuerdo con su origen podemos clasificarlas en tres categorías:

Tabla 1 Clasificación de desastres por su origen

Naturales	Socionaturales	Humanas
Se originan en la dinámica propia de la tierra. Los seres humanos no intervienen en la ocurrencia de estos fenómenos, menos están en la capacidad de evitarlos. Estos eventos pueden estar relacionados: Con el agua y clima, como es el caso de las fuertes lluvias, crecidas de los ríos, heladas o sequías. Con la tierra, como son los sismos, la erosión natural y sus efectos sobre los deslizamientos y huaycos.	Aparentemente son naturales, pero en su ocurrencia y en la intensidad de sus efectos intervienen los seres humanos. Ejemplos: Inundaciones, sequías o deslizamientos que muchas veces son más frecuentes e intensos debido a la deforestación y el manejo inadecuado de los suelos.	Atribuidas directamente a la acción del ser humano sobre elementos de la naturaleza. Ejemplos: La contaminación del agua, tierra y aire. Fuga de materiales peligrosos. Acciones en el manejo de sustancias tóxicas, radioactivas, etc.

Fuente: Sistema Nacional de Defensa Civil del Perú

2.2.2. ¿Qué es la vulnerabilidad?

Es el conjunto de condiciones ambientales, sociales, económicas, políticas y educativas que hacen que un negocio y/o comunidad estén más o menos expuestas a un desastre, sea por las condiciones inseguras existentes o por su capacidad para responder o recuperarse de tales desastres. La vulnerabilidad de una comunidad cambia continuamente con las fluctuaciones de la población, la construcción de nuevas viviendas, carreteras, instalaciones industriales y otras infraestructuras. El grado de vulnerabilidad de una población expuesta a una amenaza puede ser reducido si es que se diseñan acciones de preparación para las emergencias o si se reducen las condiciones de riesgo existentes mediante las políticas y estrategias de desarrollo local.

2.2.2.1. Factores que inciden en la vulnerabilidad

a. Físicos

Localización de poblaciones con respecto a una amenaza o en zonas de riesgos, como el cauce de los ríos o en zonas inundables, en las cuales influyen factores como la pobreza, el desconocimiento o la falta de alternativas para su reubicación.

b. Técnicos

Construcciones inadecuadas, edificadas sin respetar las pautas técnicas o que se encuentran en estado de deterioro. Muchas de estas construcciones son consecuencia del incumplimiento de las normas y procedimientos existentes en las municipalidades y otras por la ausencia

de tales procedimientos. La licencia de construcción debe ser un requisito a cumplir antes del inicio del levantamiento de la vivienda.

c. Ecológicos

Debilitamiento y/o destrucción de las reservas o recursos del ambiente (agua, suelo, flora, fauna, biodiversidad) y ecosistemas naturales. Por ejemplo, la deforestación aumenta la fragilidad frente a las lluvias y provoca erosión, deslizamientos, derrumbes, inundaciones o avalanchas.

d. Económicos

Se refiere a cómo se usan los recursos económicos o la ausencia de ellos para las acciones de prevención. La pobreza de las poblaciones aumenta los riesgos de desastres. Los más pobres son siempre los más expuestos a los desastres y sus impactos negativos pues, por lo general, ocupan zonas en riesgo y disponen de viviendas con construcciones deficientes.

e. Sociales

Se refiere a la carencia de redes sociales y liderazgos capaces de generar cohesión y capacidad para reducir los riesgos o responder adecuadamente a las emergencias.

f. Políticos

Grado de descentralización de las decisiones y fortaleza de las instancias locales, participación de la población, representatividad y autonomía de las instituciones, para acciones de prevención o respuestas a los desastres.

g. Culturales

Autoestima colectiva, sentido de pertenencia a una comunidad, identidad nacional, regional y local. En muchas comunidades se asumen los desastres como hechos que van a ocurrir de todas maneras, lo que reduce el esfuerzo para prevenir los riesgos; mitos que tenemos sobre la ocurrencia de los desastres, lo cual no permite plantear acciones para la prevención o respuesta oportuna.

h. Educativos

Limitada calidad de la educación e insuficiente incorporación dentro de los programas de estudio de las temáticas de gestión de riesgo, protección ambiental o preparación para emergencias.

2.2.2.2. Dimensiones de la vulnerabilidad

La vulnerabilidad está determinada por causas estructurales, procesos sociales y condiciones inseguras que interactúan entre sí.

La ausencia de evaluaciones de riesgo en los programas y proyectos de desarrollo, la ineficacia e ineficiencia de la normatividad vigente para preservar la seguridad, la centralización de las decisiones políticas y administrativas y el limitado apoyo a las iniciativas e institucionalidad local para prevenir o responder a situaciones de desastre, representan una significativa vulnerabilidad.

La desinformación, la carencia de responsabilidades ciudadanas, el asistencialismo, la ausencia de horizontes de desarrollo y progreso, el predominio de actitudes autoritarias y la exacerbación del individualismo condicionan la vulnerabilidad en la dimensión cultural.

La ocupación de espacios anegadizos, la construcción sobre terrenos inestables, el deterioro de las edificaciones y la ausencia y deficiencia de medidas de protección contribuyen a acentuar la inseguridad física.

Son más vulnerables a los desastres los segmentos pobres de la población porque ven limitado o prácticamente prohibido su acceso a terrenos y viviendas seguras, a la información y educación y, en general, a los recursos para prevenir, prepararse para enfrentar emergencias o para recuperarse de ellas.

2.2.3. ¿Qué es el riesgo?

Es la probabilidad de que suceda un desastre como consecuencia de la combinación de las amenazas con las condiciones de vulnerabilidad. El riesgo puede ser estimado por el número probable y características de pérdidas humanas, heridos, propiedades dañadas e interrupción de actividades económicas que podría producirse luego de un desastre.

Todos los desastres van construyéndose o formándose antes de su ocurrencia con el desarrollo de las condiciones de riesgo.

De un lado se generan las amenazas tanto por los cambios naturales en nuestro planeta como por la creciente influencia de las actividades humanas: la contaminación que provocan algunas grandes empresas multinacionales está incidiendo sobre los cambios de clima en el planeta, agudizando las sequías y fenómenos climáticos como El Niño; la ocupación (para fines de vivienda o agrícolas) y modificación de los cauces de los ríos y quebradas; la erosión de los suelos a consecuencia de prácticas inadecuadas en la minería, agricultura y ganadería; y la destrucción acelerada de los bosques que contribuye aún más a la erosión de los suelos e inestabilidad de las laderas.

De otro lado, la vulnerabilidad de las personas ha tendido a incrementarse en nuestro país con el crecimiento de las ciudades en torno a las actividades productivas más rentables, como es el caso de la agricultura y la industria en la costa o la minería en la sierra; la ubicación de carreteras y centros poblados cerca de los cauces de los ríos, la ocupación de terrenos de mala calidad para usos de vivienda, la construcción de viviendas sin la adecuada regulación y dirección técnica, la construcción de locales de uso público en lugares inseguros, la debilidad de las instituciones públicas y privadas para incorporar en sus planes y políticas las estrategias para reducir los riesgos que afectan, por ejemplo, la seguridad de los niños y maestros en las escuelas tanto por la insuficiente formación sobre los riesgos de desastres como por la deficiente calidad de las instalaciones

Un aspecto realmente clave para la reducción de los riesgos es la información y la educación. En casi todos los desastres la mayoría de pérdidas económicas y las víctimas podrían haberse salvado con un comportamiento adecuado que se logra con el concurso de los medios de comunicación y de las instituciones educativas. Las condiciones de riesgo tienden a crecer por la insuficiente vinculación de las autoridades municipales con los ciudadanos, del gobierno central con los gobiernos locales y regionales, y de la gerencia administrativa de una empresa con sus empleados.

El riesgo puede ser parcialmente dimensionado y zonificado, mediante evaluaciones y estudios con diversos grados de complejidad. Los datos relativos a los riesgos que pueden ser medidos o estimados cuantitativamente son la frecuencia y los daños producidos por desastres anteriores y el número de personas, viviendas, locales públicos y empresas que pueden ser afectados. Los datos que pueden expresarse en mapas son la localización de eventos peligrosos, la ubicación de poblaciones, instituciones e instalaciones (colegios, fábricas, empresas, negocios, instalaciones de agua, desagüe y electricidad) en zonas de mayor o menor riesgo.

2.2.3.1. Clasificación de riesgos

a. Financieros

- ✓ Balance
- ✓ Mercado
- ✓ Crédito
- ✓ Liquidez
- ✓ Inversiones
- ✓ Adecuación de capital

b. De proyecto

- ✓ Calidad
- ✓ Costo
- ✓ Plazo de tiempo

c. De negocio

- ✓ Estratégicos
- ✓ Competitivos
- ✓ País
- ✓ Reputación o imagen

d. Sistémicos

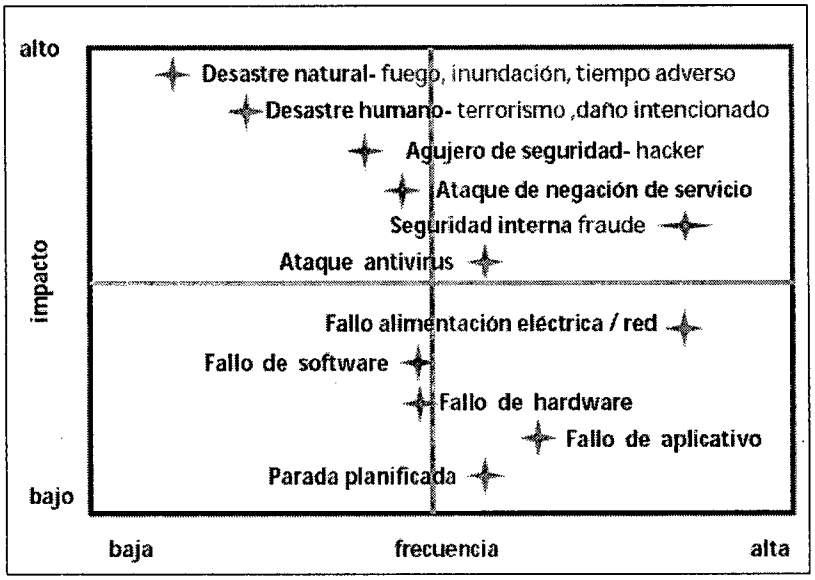
- ✓ Crisis bancarias
- ✓ Catástrofes

e. Operacional

- ✓ Fallo de alimentación eléctrica o fallo de la red.
- ✓ Fallo del software o del hardware.

En la siguiente figura se pueden ver los incidentes o desastres potenciales y su nivel de impacto en el negocio, así como la probabilidad o frecuencia de ocurrencia.

Figura 2 Interrupciones y su nivel de impacto y frecuencia



Adaptado de: Telefónica España. Fuente Original: HP Invent

El riesgo viene a ser la combinación del Impacto y la Frencuencia de los incidentes. Son los incidentes cotidianos los que ocasionan un importante impacto en el negocio.

2.2.3.2. Gestión de riesgos

a. Para qué sirve la gestión del riesgo?

Para identificar riesgos, mediante:

- ✓ Listas de verificación
- ✓ Brainstorming

- ✓ Temas pendientes
- ✓ Diagramación
- ✓ Procesos
- ✓ Reuniones periódicas

Para el análisis del riesgo, de forma:

- ✓ Cuantitativa
- ✓ Cualitativa
- ✓ Mixta
- ✓ Técnica
  - ✓ Entrevistas
  - ✓ Experiencia interna
  - ✓ Experiencia externa
  - ✓ Checklist

Para el tratamiento del riesgo

- ✓ Disminuir posibilidad
- ✓ Disminuir consecuencias
- ✓ Implementar planes

Para evaluar los riesgos

- ✓ Comparar contra criterios
- ✓ Lista de riesgos priorizada

La gestión del riesgo permite optimizar la productividad ya que evita tener que arreglar problemas que pudieron preveerse y elimina actividades que no generen valor. Lo mas importante, permite que se

tomen decisiones con conocimento del riesgo y no basandose en el azar de los eventos.

2.2.4. ¿Qué es un desastre?

Cuando un fenómeno destructivo actúa sobre condiciones de vulnerabilidad produciendo graves daños contra vidas humanas y bienes o interrumpiendo por ello el normal funcionamiento de la sociedad y de los negocios se produce un desastre.

Un desastre puede causar cuantiosas pérdidas humanas, materiales, ambientales, culturales y económicas. La comunidad afectada no puede seguir adelante por sus propios medios, requiere de la ayuda nacional y/o internacional.

El impacto de los desastres no debe ser medido solo en función de la valorización monetaria de los daños. Es necesario tener en cuenta la valoración social de tal impacto, las capacidades de rehabilitación y reconstrucción y, por lo tanto, las desigualdades sociales y el sistema de relaciones entre lo local, regional y nacional.

Un desastre puede resultar en la destrucción de viviendas, de los medios e infraestructura productiva. Aunque en el ámbito local o regional los daños pueden tener un valor monetario similar, la capacidad o posibilidad de reposición puede variar en función de la concentración y centralización de las decisiones.

La valorización económica de los daños en las ciudades tiende a ser mayor que en el campo porque allí se concentra más infraestructura, recursos productivos y de consumo. En las regiones con mayor infraestructura productiva la valorización de los daños tenderá a ser mayor que en las regiones con menor infraestructura. En países donde se concentra la riqueza el valor económico de los daños tenderá siempre a ser mayor que en los países donde se concentra la pobreza. La cuantificación del daño económico es al desastre, lo que el ingreso per cápita es a la sociedad.

Por lo general, los desastres son consecuencia de las decisiones acerca del desarrollo y del manejo del entorno natural y social. Todos los desastres pueden ser minimizados o evitados si se plantea el desarrollo teniendo en cuenta los peligros que provienen de la naturaleza y de las formas de vida sustentadas en el deterioro del medio ambiente. Los desastres pueden causar destrucción, cuantiosas pérdidas humanas y económicas si las personas, la comunidad, las empresas y el gobierno no están suficientemente preparados para responder ante ellos.

En términos de continuidad de negocios, un desastre significa la interrupción no planificada, no esperada, de los procesos normales de negocio como resultado de la interrupción de los componentes de la infraestructura IT utilizados para soportarlos. En infraestructura IT se

incluyen los componentes de los sistemas de información y de las redes, todo el hardware y software así como la data en sí.

De las interrupciones relacionadas a la infraestructura de los procesos de negocio, aquellos que resultaron en la pérdida de la data son los más devastadores. Sea que la pérdida de data resulte de un evento accidental o intencional, y/o la destrucción del medio en el cual era almacenada la data, la data es el componente más complicado de recuperar de todos los componentes de la infraestructura.

Además de la perdida de data, las interrupciones en los procesos de negocio pueden comprometer los componentes de la infraestructura tecnológica que es utilizada para transportar, procesar y presentar la data. Muchos factores pueden llevar a la pérdida de la infraestructura, estos incluyen eventos que ocasionen la destrucción de la llave del sistema, la red o el Storage. También podrían perderse la infraestructura regional, dependiendo de la magnitud del desastre como por ejemplo la electricidad de la ciudad o las redes y telecomunicaciones.

Los efectos de las interrupciones en la infraestructura pueden ser minimizados a través de la aplicación de estrategias de continuidad y recuperación las cuales son el resultado de un planeamiento y preparación avanzado.

Generalmente calificamos como desastre un evento mayor como por ejemplo una bomba terrorista, un terremoto o una guerra. En cualquier

caso, si el resultado es una interrupción no planificada en los procesos del negocio, este evento se podría considerar como un desastre.

2.2.5. Clasificación de desastres

2.2.5.1. Terremotos

Los sismos constituyen una de las principales amenazas y pueden ser medidos por su magnitud (escala de Richter) y por su intensidad (escala de Mercalli). La magnitud se refiere a la energía liberada en el epicentro del sismo, mientras que la intensidad está referida al daño que el sismo causa sobre determinadas construcciones. El valor MSK es el asignado a las recientes variaciones en la escala modificada de Mercalli, ver detalle en el **¡Error! No se encuentra el origen de la referencia.**.

En el cuadro siguiente se comparan las escalas de medición de sismos:

Tabla 2 Escalas de Ritcher y Mercalli

Escala de Richter	Escala de Mercalli
2	I – II Movimiento registrado en el sismógrafo. No es percibido por la población.
3	III Se siente en el interior de las viviendas.
4	IV – V Es sentido por un buen número de la población. Ligeros daños materiales.
5	VI Todos lo sienten. Alerta en la mayoría de la población. Daño menor - moderado.
6	VII – VIII La gente se asusta y se genera pánico. Daño moderado en las construcciones.
7	IX – X Gran daño y muertes.
8	XI – XII Destrucción total. Catástrofe. Drásticos cambios en la superficie terréstre.

Fuente: Guía del participante / PCC. Programa de Capacitación para Comunicadores Sociales. Perú.

El peligro sísmico presenta dos aspectos importantes uno el científico y el otro el económico. Dentro del aspecto científico existen dos puntos de vista, del sismólogo que se interesa por la probabilidad de ocurrencia de un terremoto de ciertas características y el del ingeniero, que le interesa la probabilidad de que una estructura se comporte de una cierta forma bajo la acción de un sismo.

2.2.5.1.1. Medidas preventivas

Un plan de mitigación o acción, consiste en la planificación e implementación de las actividades propuestas inicialmente para la reducción del riesgo sísmico, la priorización y puesta en marcha de dicho plan. Puesto que este tipo de eventos serían mas prejudiciales para ciudades de bastante población, también lo es para todos los asentamientos humanos que ultimadamente están arriesgándose a tener viviendas en zonas no aptas para la construcción, según las características geomorfológicas del entorno y de acuerdo al código sísmico del Perú.

Si bien es cierto de todos los métodos utilizados en predicción, como el de "Predicción Tectónica", no permiten conocer la fecha de un posible sismo si indica el lugar donde podría ocurrir y posible tamaño, este sería un muy buen punto de partida para la prevención de un terremoto en

determinada ciudad, teniendo en cuenta que se podría elaborar un plan de mitigación en base a la información.

Para poder determinar cuales son las zonas de mayor riesgo sísmico se debe tener énfasis en los siguientes puntos. Teniendo como referencia la ciudad de Arequipa, Lima y otras que cuentan con un numero considerable de habitantes, se puede considerar como riesgos primarios los siguientes:

- ✓ **Tipos de suelos:** En los que se pretende hacer edificaciones en zonas como laderas de ríos, bordes de torrenteras y zonas altas donde el suelo no es compacto. Para reducir el peligro se debe hacer un estudiogeológico de la zona y además una zonificación geotectónica.
- ✓ **Calidad de las Construcciones**: Basado en el diseño sismorresistente, teniendo en cuenta el código sísmico peruano. Por lo tanto se debe tener especial interés en las edificaciones antiguas como casonas, iglesias, algunos puentes y calles que generalmente forman parte del patrimonio cultural e histórico de todas las ciudades, porque son una de las principales fuentes de riesgo para todos los habitantes de las diversas ciudades.
- ✓ **Servicios Vitales de abastecimiento de Agua potable:** como las presas, ubicadas en las grandes ciudades de Perú como Lima, Arequipa y otras mas, deben de contar con

métodos de construcción modernos, para evitar desastres de inundaciones; en el caso de zonas rurales especial cuidado con los pozos para agua ya que con los movimientos telúricos suelen sufrir las consecuencias.

- ✓ **Comunicaciones y energía:** Para estos tipos de servicios se debe tener en cuenta la posibilidad de descentralizar lascentrales hidroeléctricas y además redes tensiométricas que podrían ocasionar grandes incendios y desastres en zonas pobladas.
- ✓ **Transporte:** Es recomendable crear conciencia ciudadana para los conductores, peatones y pasajeros en cuanto a la evacuación en caso de ocurrir un sismo, así mismo hacer señalizaciones de zonas realmente peligrosas para transitar.
- ✓ **Servicios de Emergencia:** Los servicios médicos, bomberos y policía, todos estos deben estar con plena disposición para evacuar a los heridos, en caso de producirse incendios provocados por fugas de gas y además evitar saqueos provocados por delincuentes.

Y como riesgos secundarios se puede considerar a los Tsunamis, deslizamientos y derrumbes.

Debido a la geometría de las zonas sismogénicas y a la información disponible sobre intensidades y a los diferentes mapas de zonificación; se considera como una zona de alto riesgo sísmico al borde

Oeste de Perú, asimismo la zona de riesgo medio es la región Nororiental y Sur, y el resto de Perú con riesgo sísmico bajo o nulo.

2.2.5.2. Huaycos e Inundaciones

Los huaycos y las inundaciones constituyen las amenazas más frecuentes de la naturaleza en una geografía compleja como la peruana. Se encuentran asociados a la temporada de lluvias. La abundancia de descargas pluviales aumenta los caudales de los ríos, provocando desbordes. Los huaycos son precipitaciones masivas de agua y lodo que arrastran a su paso todo lo que encuentran, pudiendo causar graves daños personales y materiales.

En la temporada que se presenta el fenómeno de El Niño aumenta la probabilidad de las inundaciones. A ello se debe las sequías en zonas donde habitualmente llueve así como las lluvias torrenciales en otros lugares.

El fenómeno de El Niño es un trastorno de naturaleza global cuya principal característica es el calentamiento anormal de las aguas superficiales del Océano Pacífico que afecta su hábitat y determina un incremento sustantivo de la variabilidad del clima del mundo (lluvias e inundaciones, sequías y friajes).

El Niño deviene de una compleja relación entre la superficie del Océano Pacífico y la atmósfera, que determina el incremento de la

temperatura del agua en el Pacífico central y oriental, repercutiendo en las condiciones atmosféricas y en las pautas meteorológicas de todo el planeta.

Afecta a muchos países a la vez. El Perú es escenario recurrente de este fenómeno que se está repitiendo con mayor frecuencia, aparentemente por la propia acción del hombre que afecta los equilibrios naturales. Antes se estimaba una frecuencia regular de alrededor de diez años entre un fenómeno y otro, pero ahora puede llegar a repetirse en un lapso de tres años.

2.2.5.3. Volcanes

Una amenaza relacionada con la actividad sísmica es la volcánica. El sur del Perú es la región que presenta el mayor número de volcanes en actividad. En la cordillera occidental existen 250 volcanes. De este número, trece son potencialmente activos. Además, se les puede añadir los volcanes Camiri (en Bolivia) y Tacora (Chile), que son muy próximos a la frontera peruana.

Un estudio sobre la actividad volcánica y su impacto geológico en el sur peruano realizado por el Instituto Geológico, Minero y Metalúrgico del Perú (Ingemmet), «Zonificación y riesgo geológico en el sur del Perú» en una franja que comprende 71.500km² (área que encierra los principales volcanes en actividad) y que abarca las regiones de Tacna, Moquegua, Arequipa y Puno.

Esta investigación determinó, que en la zona de estudio están comprometidas diez de las cincuenta y tres principales cuencas de la vertiente del Pacífico y cuatro de diez cuencas pertenecientes a la hoya hidrográfica del Titicaca, las que pueden ser afectadas en mayor o menor medida por eventuales erupciones volcánicas.

Volcanes activos que podrían afectar el territorio nacional:

Tabla 3 Volcanes activos que podrían afectar al Perú

Ubicación	Nombre	Altura (m.s.n.m.)
Arequipa	Sara Sara	5.450
	Solimaná	6.093
	Coropuna	6.377
	Sabancaya	5.976
	Ampato	6.288
	Chachani	6.057
	Misti	5.820
	Pichu Pichu	5.440
Moquegua	Ubinas	5.536
	Huaynaputina	4.300
	Ticsani	5.408
Tacna	Tutupaca	5.815
	Yucamane	5.508
Bolivia	Camiri	5.300
Chile	Tacora	5.600

Fuente: Instituto Geofísico del Perú. Mapa de peligros potenciales.

2.2.5.4. Tsunami

El tsunami es una ola o un grupo de olas de gran energía que se producen cuando algún fenómeno extraordinario desplaza una gran masa de agua verticalmente. Esta palabra proviene de los vocablos

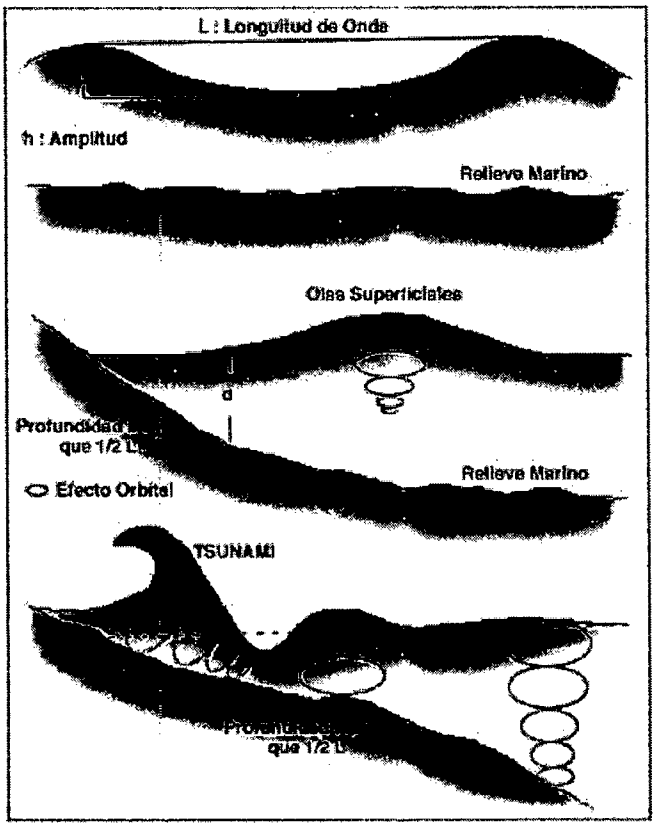
japoneses «tsu», que significa puerto o bahía, y «nami», que significa ola. Los tsunamis son menos frecuentes pero de gran peligrosidad en la costa en el Perú por tener un litoral de 2.500km. A lo largo de la costa se asienta buena parte de las principales ciudades del país, con una población que bordea los 13 millones de habitantes (52,1% del total). La historia colonial y republicana registra la ocurrencia de doce tsunamis, todos ellos muy destructivos. El más antiguo del que se tiene data es el ocurrido en 1586. El organismo encargado del monitoreo y seguimiento de los tsunamis en el Perú es la Dirección de Hidrografía y Navegación de la Marina de Guerra del Perú.

Parámetros físicos que definen las características de un Tsunami:

La velocidad de propagación del tsunami depende de la profundidad oceánica. Para el Océano Pacífico la profundidad media es de 4,000 m, lo que da una velocidad de propagación promedio de 198 m/s ó 713 km/h. Si la profundidad de las aguas disminuye, la velocidad del tsunami decrece.

Al aproximarse las aguas bajas, las olas sufren fenómenos de refracción y disminuyen su velocidad y longitud de onda, aumentando su altura. La longitud de onda de un tsunami corresponde al producto entre la velocidad de propagación y el período de tiempo.

Figura 3 Longitud de onda de un tsunami



2.2.5.5. Deslizamientos, Aluviones

Los deslizamientos de tierra destruyen estructuras, caminos, acueductos y cables ya sea a causa de los movimientos terrestres debajo de ellos o sepultándolos. El movimiento gradual del terreno deja edificios inclinados y fuera de uso. Las grietas del terreno separan los cimientos y rompen sistemas de servicio público enterrados.

La falla repentina de las laderas arranca el terreno de asentamientos lanzándolos colina abajo. Los desprendimientos de piedras causan destrucción por la fragmentación de las piedras contra rocas que caen y chocan contra estructuras y asentamientos. Los escombros

circulan hacia terrenos blandos, materiales lechados, escombros artificiales apilados y la tierra con alta concentración de agua fluye como líquido, amontonándose en valles, enterrando asentamientos, bloqueando los ríos (posiblemente causando inundaciones) y bloqueando caminos. La Licuefacción de la tierra en terrenos planos bajo fuertes vibraciones causadas por un terremoto produce como resultado la pérdida repentina de la solidez del terreno para resistir las estructuras en ese lugar. El suelo efectivamente se transforma temporalmente en líquido ocasionando el hundimiento o caída de las estructuras.

Los aluviones son los fenómenos de mayor letalidad en la historia del país. Se originan con el desprendimiento de nevados que arrastran grandes masas de nieve y rocas sobre zonas pobladas o sobre lagunas que a su vez se desbordan arrasando lo que encuentran a su paso. El Callejón de Huaylas, en el departamento de Ancash, ha sido escenario de grandes aluviones en 1941, 1962 y 1970.

2.2.5.6. Tormentas de alta intensidad

Pueden ser huracanes, tormentas invernales o tornados. Presión y succión causada por la presión del viento que resopla durante horas seguidas. La fuerza que los vientos fuertes imponen en una estructura pueden derrumbarla, particularmente después de repetidos cambios en la dirección del impacto. Los daños más comunes se producen en edificaciones y elementos no estructurales (planchas de techumbres,

revestimientos de acero inoxidable, chimeneas), derribados por el viento. Los escombros impulsados por el viento causan daño y lesiones. Los vientos altos son motivo de mares tormentosos que pueden hundir barcos y azotar las orillas de las playas. Muchas tormentas acarrean abundantes lluvias. La presión extremadamente baja del aire en el centro del tornado es sumamente destructiva pudiendo hacer volar las casas con su contacto.

2.2.5.7. Otros eventos

Terrorismo, fuego, incendios, Explosión, Sabotaje informático, Pandemias (gripe aviar), Robo, Interrupción del fluido eléctrico, Fallos de comunicaciones, Rotura de los conductos de gas, agua, y desagües.

2.3. Marco legal, organismos reguladores y mejores prácticas

Para el sector de servicios financieros, el riesgo ha sido siempre parte del negocio. Pero en los últimos años, la incertidumbre del mercado y la turbulencia del mercado de capitales han transformado el peligro de riesgos - y las consecuencias de su mal manejo - en el centro de la escena. La continua explosión de los volúmenes de transacciones y la demanda de automatización y velocidad han crecido a costas del riesgo. En consecuencia, también ha crecido el clima regulatorio que exige nuevos niveles de control y visibilidad - y considera al directorio y al equipo ejecutivo responsables por ello.

El primer paso para la administración de riesgos tal como lo indican las mejores prácticas internacionales es modelar el negocio. COSO (Committee of Sponsoring Organizations of the Treadway Commission), COBIT (Control Objectives for Information and related Technology), ITIL (Information Technology Infrastructure Library), e ISO/IEC (International Organization for Standardization and the International Electrotechnical Commission) 17799:2005, son organizaciones internacionales que generan estándares, algunos de los cuales tienen el fin de incentivar el cumplimiento del desarrollo de un plan de la continuidad del negocio.

2.2.1. Defensa civil

La historia moderna de las políticas públicas en relación con la eventualidad de desastres comienza tras el impacto del violento terremoto y aluvión de Áncash en 1970. Desde ese momento se han desarrollado una serie de pasos en la legislación peruana para contribuir a la prevención y mitigación de desastres, la organización de la sociedad civil y creación de organismos del Estado.

- ✓ 1972 Ley Nº 19338 Creación del Sistema de Defensa Civil (Sideci)

  Como consecuencia del terremoto y aluvión en el Callejón de Huaylas en mayo de 1970, el gobierno militar crea este

sistema para proteger a la población frente a nuevos desastres.

- ✓ 1987 Decreto Legislativo Nº 442 Creación del Instituto Nacional de Defensa Civil (Indeci)

  Esta norma modifica y precisa la Ley 19338.

- ✓ 1991 Decreto Legislativo Nº 735 Creación del Sistema Nacional de Defensa Civil (Sinadeci)

  Define la responsabilidad de planear, coordinar y dirigir las medidas de previsión necesarias para disminuir los efectos de los desastres o calamidades. Planear y coordinar la utilización de los recursos necesarios, públicos o privados, con el fin de contar con los medios para proporcionar ayuda en la recuperación de las personas y los bienes en caso de desastre, asegurando la movilización inmediata de los elementos de rescate.

- ✓ 1997 Resolución de Superintendencia Nº 359-97-Sunass

  Medidas que deben adoptar las entidades prestadoras de servicio de saneamiento

  Establece lineamientos y orientaciones para que las Entidades Prestadoras de Servicios adopten medidas que permitan asegurar el adecuado funcionamiento de los servicios de saneamiento en emergencias.

- ✓ 2001 Decreto Supremo Nº 024-2001-PCM Forman la Comisión Nacional de Emergencia

  Crea la Comisión Nacional de Emergencia por desastres naturales encargada de coordinar, evaluar, dar prioridad y supervisar acciones urgentes en las zonas que se declaren en emergencia.

- ✓ 2002 Acuerdo Nacional - Décima política de Estado Reducción de la pobreza

  Fomentará una cultura de prevención y control de riesgos y vulnerabilidades de los desastres, asignando recursos para la prevención, asistencia y reconstrucción.

- ✓ Decreto Supremo Nº 053-2002-PCM

  Forman la Comisión Multisectorial de Reducción de Riesgo para el Desarrollo

  Tiene por finalidad coordinar las acciones conducentes a la incorporación del enfoque de prevención y mitigación de riesgos frente al peligro, en el proceso de planeamiento del desarrollo.

- ✓ Resolución Ministerial Nº 030-2002-Vivienda

  Designa al despacho viceministerial de Construcción encargado de tramitar coordinaciones, planeamientos y

acciones en caso de desastres por causas naturales Su función es tramitar todo tipo de coordinaciones, planeamientos y acciones, ya sean previas o posteriores, en los casos que se suscite un desastre por causas naturales.

- ✓ 2003 Decreto Supremo Nº 081-2002-PCM

  Crean la Comisión Multisectorial de Prevención y Atención de Desastres

  Coordina, evalúa, da prioridad y supervisa medidas de prevención, daños, atención y rehabilitación en las zonas del país que se encuentren en peligro inminente, o afectadas por los desastres.

- ✓ 2004 Directiva N° 52-2004-ME

  Establece medidas para promover la cultura de prevención de desastres en los educandos a través de la educación formal.

  Todas las instituciones educativas de educación básica (inicial, primaria, secundaria), educación básica alternativa (educación de adultos) y de formación magisterial deben considerar en el Proyecto Educativo Institucional y Proyecto Curricular del Centro, los contenidos de la propuesta «Aprendiendo a Prevenir», la cual busca el desarrollo de capacidades, actitudes y valores que conduzcan a forjar una

cultura de prevención de desastres en los educandos a través de la educación formal.

- ✓ Decreto Supremo Nº 001-A-2004-DE-SG

  Aprueba el Plan Nacional de Prevención y Atención de Desastres

  Plan estratégico integral: objetivos, estrategias y programa que dirigirán y orientarán el planeamiento sectorial y regional para la prevención, mitigación de riesgos, preparación y atención de emergencias, así como para la rehabilitación en caso de desastres, permitiendo reducir daños, víctimas y pérdidas que puedan ocurrir como consecuencia de un fenómeno natural o tecnológico, mediante medidas de formación ciudadana, legislación, organización y la incorporación de nuevos modelos en prevención y desarrollo sostenible.

- ✓ Resolución Ministerial Nº 771/MINSA

  Establece las estrategias sanitarias nacionales del Ministerio de Salud y sus respectivos órganos responsables Se plantean diez estrategias sanitarias nacionales del Ministerio de Salud con sus respectivos órganos responsables de su ejecución. Cada estrategia sanitaria estará a cargo de coordinadores nacionales encargados de diseñar, planificar, programar, monitorear, supervisar y evaluar.

2.2.2. Basilea

El Comité de Basilea sobre Supervisión Bancaria fue creado en 1974 por acuerdo de los representantes de los Bancos Centrales de los 10 países más industrializados. Este Comité, si bien no posee ninguna autoridad de supervisión sobre los países miembros y sus conclusiones no tienen fuerza legal, ha formulado una serie principios y estándares de supervisión bancaria, que han sido acogidos no solo por los países miembros, sino por la mayoría de países en el mundo.

2.2.3. Basilea II

En 1988, el comité de Basilea generó un documento llamado Acuerdo de Capital de Basilea ó Basilea I en el que se propuso una metodología para medir el riesgo crediticio. Hoy cerca de 150 países se rigen por estos principios, incluyendo el Perú. Pero el comité de Basilea I se percató de algunas deficiencias, por lo que decidieron reformar Basilea I y generar un esquema más sensible al riesgo.

En junio del 2004 se aprobó el Nuevo Acuerdo de Capital o Basilea II el cual está compuesto por una serie de principios y recomendaciones del Comité de Basilea sobre Supervisión Bancaria cuyo objetivo es propiciar la convergencia regulatoria hacia los estándares más eficaces y avanzados sobre medición y gestión de los principales riesgos en la industria bancaria.

El Perú, por medio de la Superintendencia de Banca, Seguros y AFP, es consciente de las ventajas en seguridad y estabilidad que genera un esquema como el propuesto en Basilea II y no está al margen de esta reforma internacional de la regulación bancaria.

El nuevo acuerdo de Capital o Basilea II, contribuye a incrementar la seguridad y solidez del sistema financiero. Uno de los cambios más notables es la introducción del costo de capital para el riesgo operativo.

Basilea II se puede definir como un marco global de supervisión bancaria, basado en tres pilares:

- ✓ El pilar 1 es el que dicta los requerimientos mínimos de capital que constituyen el riesgo.
- ✓ El pilar 2 dirige y supervisa que los bancos evalúen su solvencia e incluye directrices para los supervisores.
- ✓ El pilar 3 procura la transparencia, disciplina a los bancos para que informen su riesgo en el mercado.

Figura 4 Pilares en los que se basa Basilea II

El Riesgo operativo según Basilea II es el riesgo de pérdidas directas y/o indirectas resultante de fallas o inadecuados procesos internos, personas, sistemas de información y/o eventos externos.

Para cumplir con los principios de Basilea II, el sistema financiero peruano debe asumir el reto de:

Ajustar sus sistemas de medición y administración de riesgos, hacia el uso de modelos internos que les permita realizar una administración eficiente del riesgo.

Generar información relevante y suficiente de las operaciones con sus clientes, para que los modelos puedan estimar adecuadamente el riesgo al que está expuesta la institución.

Desarrollar una plataforma informática capaz de almacenar y explotar adecuadamente la información generada.

Adecuar sus mecanismos de control interno hacia un esquema más sensible al riesgo.

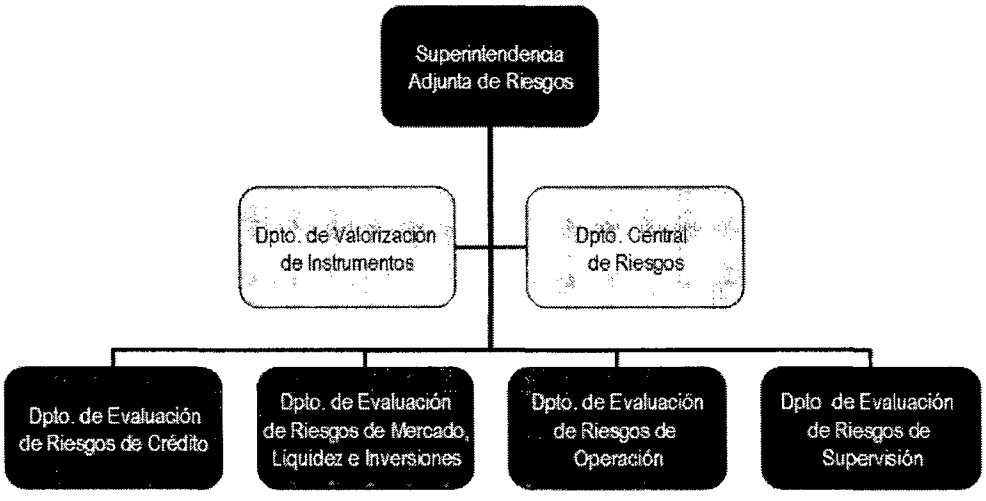
Finalmente, establecer programas de capacitación orientados a satisfacer la demanda de personal altamente capacitado en técnicas de medición y gestión de riesgo, que generara esta transición.

2.2.4. Superintendencia de Banca, Seguros y AFP

Antiguamente las empresas captadoras de depósitos no eran controladas, ni reguladas, podían operar todo tipo de servicios y establecer oficinas en cualquier lugar. No se realizaban auditorías internas, y las externas eran inútiles por que la información financiera no era confiable.

En 1992 se realiza un ajuste fiscal del sistema financiero con lo que quebraron 40 instituciones que manejaban el 78% de los depósitos del Perú. A fines del 1992 el Decreto Legislativo 26091 dispone que la Superintendencia de Banca, Seguros y AFP (llamada SBS) regule las instituciones financieras.

Figura 5 Estructura organizacional de la Superintendencia adjunta de riesgos



Fuente SBS.

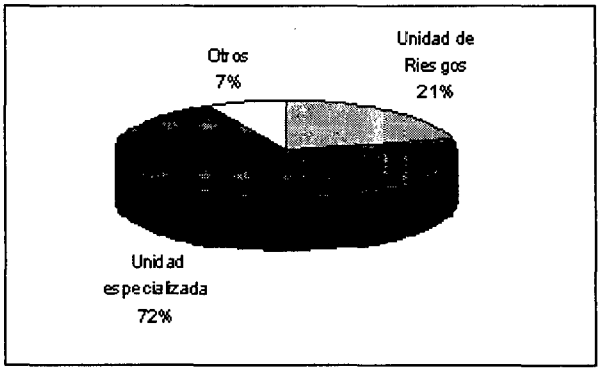
2.2.4.1. Reglamento para la administración de los riesgos de operación

En enero del 2002, la Superintendencia de Banca, Seguros y AFP emitió el Reglamento para la Administración de Riesgos de Operación (Resolución SBS N° 006-2002 del 04.01.02, ver **¡Error! No se encuentra el origen de la referencia.**), para lo cual estableció un periodo de adecuación que venció el 30 de junio del 2003.

En mayo del 2003, ya eran 14 los bancos que tenían definida un área específica encargada del manejo del riesgo operacional, de los cuales, 10 bancos cuentan con una unidad especializada y 3 bancos cuentan con un área de riesgos. En cuanto a la administración del riesgo, 12 bancos

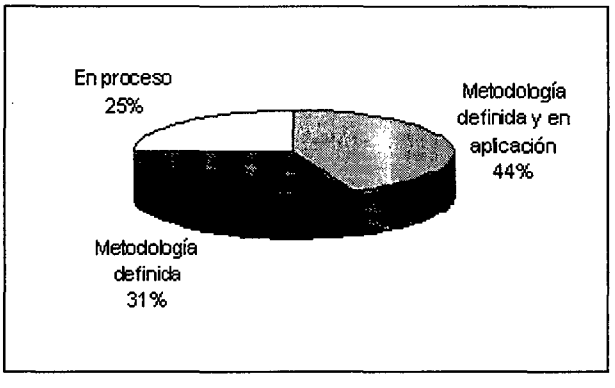
cuentan con una metodología para manejar el riesgo, de los que 7 tienen una aplicación para la metodología y 5 sólo definida.

Figura 6 Unidad especializada para la administrar el riesgo operacional



Fuente: SBS – Presentación Nuevo Acuerdo de Capital

Figura 7 Metodología para administrar el riesgo operacional



Fuente: SBS – Presentación Nuevo Acuerdo de Capital

3.1. Plan de Continuidad Operativa de Negocios

Cualquier negocio podría sufrir un serio incidente que paralice el normal funcionamiento de las operaciones del negocio, y esto podría suceder en cualquier momento. La gerencia tiene la responsabilidad de recuperar el negocio en el menor tiempo posible.

Esto requiere preparación y planificación en detalle, por lo que es conveniente que el equipo responsable de desarrollar y mantener el Plan de Continuidad de negocios de la organización (BCP) sea liderado por un Project Manager. Es necesario controlar el desarrollo del plan, así como las estrategias y procedimientos para el proceso de recuperación.

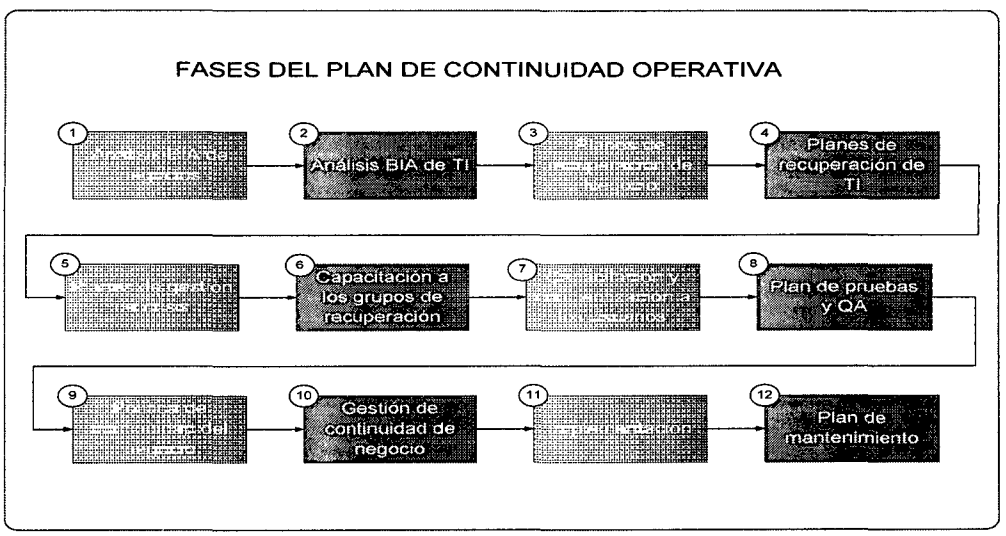
El plan de continuidad es costoso y no todas las empresas lo implementan en su totalidad. No es imprescindible que se automatice la recuperación de todos los procesos de una gran empresa. Se requiere un adecuado estudio de riesgos y balancear "el costo de la implementación de un plan de continuidad" con "el riesgo de no tenerlo".

Se deben definir el alcance y las premisas para el desarrollo del plan. Los objetivos y metas que la compañía desea alcanzar. Los escenarios que se analizarán, la interrupción menor y la mayor en términos de impacto en el negocio y la duración máxima que el negocio estaría dispuesto a operar desde un sitio alterno.

El primer paso es determinar la criticidad de cada proceso dentro de la empresa. Para los de muy alta criticidad se deberá implementar un plan de continuidad, para otros, bastará con un plan de contingencia.

Diagrama de bloques que esquematiza las fases para el desarrollo del plan de continuidad operativa:

Figura 8 Plan de continuidad operativa



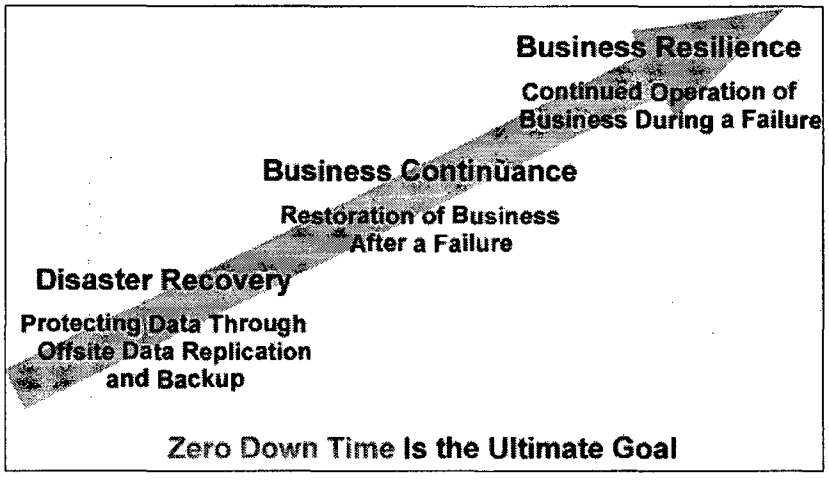
Fuente: elaboración propia.

3.1.1. Planes de Recuperación y Continuidad

Los planes de recuperación de un desastre y los planes de continuidad del negocio sirven para preservar la existencia de una organización. No todas las organizaciones cuentan con un plan, y si lo tienen, no lo mantienen actualizado, una de las razones se debe a la complejidad de ésta tarea.

El objetivo principal de invertir tiempo y dinero en el desarrollo de planes de continuidad y recuperación es lograr un tiempo cero de fuera de servicio, es decir que a pesar de ocurrido un evento que cause la interrupción de los procesos se pueda contar con procesos alternos para asegurar la continuidad del negocio.

Figura 9 Objetivo de los planes de continuidad

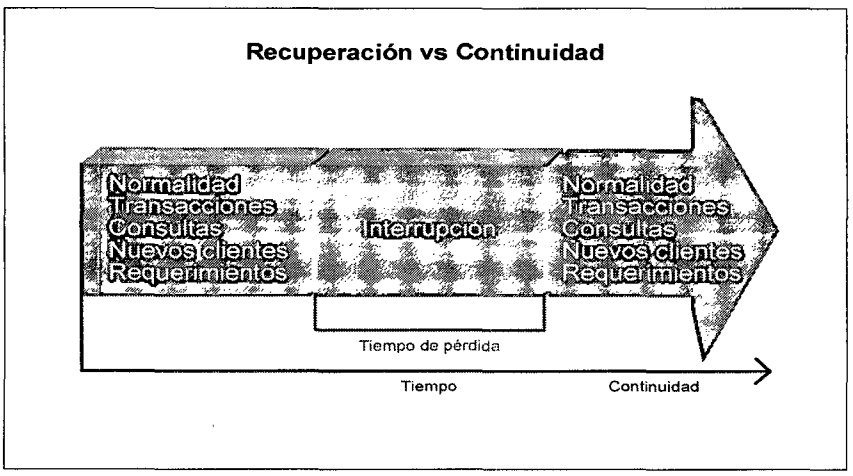


Fuente: Data Center Disaster Recovery – Nelson Muñoz – Cisco.

Para el sector financiero, no hay seguro que cubra la retención, ni la confianza del cliente.

Inicialmente la planeación se concentraba en la recuperación de interrupciones sobre sistemas de información. Hoy no sólo se busca recuperar los sistemas, también se busca garantizar la continuidad de la funcionalidad del negocio.

Figura 10 Recuperación versus Continuidad



Adaptado de: Continuidad del Negocio

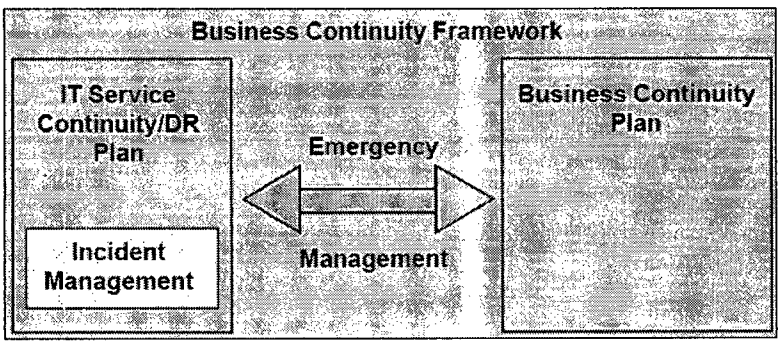
Debido a la sinergia de la administración de Tecnologías de Información y los dueños de los procesos de negocios, se puede establecer un modelo de continuidad de negocios en el que se definen los roles, responsabilidades, metodología basada en riesgos y procedimientos de aprobación.

El plan de continuidad de negocios identifica las aplicaciones críticas, servicios de terceros, sistemas operativos, personal, archivos y ventanas de tiempo necesarios para la recuperación.

El plan de continuidad de Tecnologías de Información identifica los incidentes y los administra, también se le puede llamar plan de Recuperación de desastres.

El plan de continuidad de Tecnologías de Información debe estar alineado con el Plan de continuidad del negocio para asegurar la consistencia de ambos.

Figura 11 Business Continuity Framework



Fuente: Revista ServiceTalk de ITSMF n°67.

3.1.1.1. Planes de Recuperación de un desastre

Son un conjunto integrado de procedimientos que se utilizarán para la recuperación ante un evento que cause la interrupción de las operaciones del negocio.

Además del modelo de regulación y legislación en la que una organización está basada, la continuidad de negocios y la continuidad de la tecnología representan buenas prácticas de negocios, debido a esto, la Administración de continuidad de TI y el Plan de Recuperación de desastres caben perfectamente en el marco de una disciplina ITIL.

3.1.1.2. Planes de Continuidad operativa del negocio

El plan de continuidad operativa del negocio es un proceso complejo que a través del tiempo afectará potencialmente todos los aspectos del negocio. Para elaborar un plan de continuidad operativa de negocios es recomendable utilizar un plan proyecto, el cual simplifica la administración del proceso de desarrollo del plan. El administrador de la continuidad del negocio debe prepararse adecuadamente para conseguir un conocimiento global de los procesos del negocio desde una variedad de perspectivas.

El objetivo del administrador de la continuidad debe ser asegurar que cada plan de continuidad solucione los problemas correctos, involucre el personal apropiado y utilice los recursos internos y externos que sean necesarios.

La siguiente figura ilustra los componentes para desarrollar un plan de continuidad de negocios completo.

Figura 12 Componentes del Plan de Continuidad

Fuente: M&M Auditores de Colombia Ltda

3.1.2. Compromiso y soporte de la alta gerencia

El apoyo de la alta gerencia es el componente mas importante en el desarrollo del plan. El desarrollo del plan de continuidad de negocios debe ser tratado como uno de los temas más importantes de la organización y requiere el compromiso y el involucramiento directo de la gerencia. Un proyecto de esta naturaleza contiene el esfuerzo de muchas personas, el uso de muchos recursos, y mucho tiempo invertido. Debido a que el plan está directamente relacionado a la supervivencia de la organización después de una interrupción, el planeamiento de la continuidad de negocios merece todo el apoyo de la alta gerencia.

3.1.3. Objetivos

Los objetivos proporcionan al lector un entendimiento del nivel de respuesta, reanudación y recuperación que se quiere alcanzar.

El objetivo de un plan de continudad operativa es definir estrategias y procedimientos los cuales serán implementados por un equipo de personas que facilitarán la administración, soporte, equipamiento, métodos y estándares para la continuidad operativa.

Es importante identificar las responsabilidades según la función del personal y proporcionar un framework estandar consistente dividido en fases para que el plan se pueda implementar satisfactoriamente.

Las operaciones y procesos del negocio, y la infraestructura tecnológica son reconocidas como activos valiosos; el planeamiento de la continuidad evalua los activos de la organización y su correspondencia con los requerimientos de reanudación y recuperación.

En el **¡Error! No se encuentra el origen de la referencia.** se describen ejemplos de los objetivos que podrían ser definidos para una Banco en el Perú.

3.1.4. Supuestos

Los supuestos o premisas proporcionan al lector una idea de las consideraciones al desarrollar el plan. El coordinador de la continuidad de negocios debe ajustar estas premisas para que encajen en el caso específico de la empresa.

Las premisas deben incluir lo siguiente:

- ✓ Metas y Objetivos de la organización.
- ✓ Políticas de la organización sobre planificación de la continuidad del negocio.
- ✓ Escenarios de interrupción del negocio para cada área funcional y/o localización.
- ✓ Definir una interrupción menor y un mayor desastre en términos del impacto sobre el negocio y la duración de la misma.
- ✓ Los objetivos del plan que indiquen que será reanudado o recuperado, en qué nivel de capacidad y en qué período de tiempo.
- ✓ Qué operaciones deben ser recuperadas en forma inmediata.
- ✓ Qué operaciones no requieren ser recuperadas en forma inmediata y cuando deben estar disponibles.
- ✓ Qué operaciones del negocio pueden ser prescindibles.
- ✓ Las estrategias de reanudación y recuperación a utilizar así como sus prioridades.

- ✓ Estrategias que consideren la disponibilidad y utilización de recursos pre-ubicados para soportar la ejecución del plan.

Algunas de las premisas bajo las cuales se deben desarrollar los planes de continuidad:

- ✓ El peor escenario ocurre sin aviso o advertencia.
- ✓ No ocurrirá más de un evento en forma simultánea.
- ✓ El sitio de almacenamiento externo está lo suficientemente lejos como para no ser afectado por la interrupción.
- ✓ La recuperación puede realizarse usando únicamente los datos y registros vitales ubicados en el almacenamiento externo.
- ✓ El equipo designado y otros recursos pre-ubicados están instalados y disponibles.
- ✓ Las operaciones de reanudación / recuperación requieren del uso de recursos / capacidades alternas inferiores a las de operación normal.
- ✓ Se cuenta con suficientes miembros del equipo de recuperación para realizar las tareas planeadas.
- ✓ La alta dirección está disponible para decidir la activación del plan y tomar las decisiones no previstas.
- ✓ Existen instalaciones apropiadas para el centro de control, reuniones y necesidades de almacenamiento.

3.1.5. Alcance

En esta parte se determina el número de planes, departamentos y operaciones relacionadas a las actividades de planeamiento las cuales serán necesarias para cumplir con los objetivos.

Antes el desarrollo de los planes estaba focalizado en los centros de datos, actualmente los planes incluyen las operaciones del negocio y los departamentos que vienen a ser los clientes de la tecnología.

El planeamiento de continuidad de negocios es un esfuerzo de toda la organización debido a que se incluyen sus procesos de negocio, sus productos y servicios. Visto de esta forma, la tecnología viene a ser sólo uno de los varios recursos que dependen del tiempo.

Adoptando un alcance a nivel organización, el coordinador del plan de continuidad podrá identificar no sólo los tipos de planes que serán necesarios elaborar, si no también, las relaciones de la lógica del negocio que el plan generado debe soportar.

En el **¡Error! No se encuentra el origen de la referencia.** se describen ejemplos de los alcances que podrían ser definidos para una Banco en el Perú.

3.1.6. Políticas

Las políticas deben brindar al usuario una definición clara de las áreas sensibles al tiempo.

Las políticas deben servir de base a los gerentes para que puedan responder a los intereses de los empleados, de los clientes y del público en general. Durante un desastre será de vital importancia que los gerentes cuenten con guías aprobadas para manejar diferentes situaciones.

- ✓ Políticas de Recursos Humanos
  - ✓ Deben poder continuar ofreciendo los beneficios, autorizando y aprobando gastos y asistencia a los familiares.
  - ✓ Deben restringir la liberación de información confidencial de la empresa.
- ✓ Políticas de Relaciones públicas
  - ✓ Deben aplicar las restricciones y penalidades en caso de que se libere información confidencial, o que se brinden sin autorización medios con voz, impresos o electrónicos con información confidencial.
- ✓ Políticas de Relaciones con el cliente
  - ✓ Estas políticas deben existir a nivel corporativo, pero los departamentos también deben contar con políticas

internas para administrar problemas en un producto o servicio relacionado con los clientes

- ✓ Políticas de Seguridad y salud
  - ✓ Son precauciones que asegurarán la salud y seguridad de los empleados en las instalaciones afectadas y en las alternas. Estas políticas deben describir las condiciones en las que los empleados serán para ingresar a las instalaciones y ejecutar tareas relacionadas a la Respuestas, Reanudación, Recuperación y Retorno.
- ✓ Políticas de Relaciones con los proveedores
  - ✓ Estas políticas deben existir a nivel corporativo, pero los departamentos también deben contar con políticas internas para administrar problemas en un producto o servicio relacionado con los proveedores.

Las recomendaciones del plan de continuidad deben ser contempladas en todos los contratos con proveedores.

3.1.7. Propósito

El propósito debe dar una clara idea del por qué la organización decidió desarrollar un plan de continuidad de negocios. Debe estar relacionado a la protección de la vida y la seguridad de los empleados, a la satisfacción de los requerimientos del gobierno. Generalmente el propósito está incluido en la parte de la introducción del plan.

3.1.8. Análisis de impacto en el negocio (BIA)

El análisis de impacto en el negocio da a conocer a la organización cuál sería el impacto en el caso de una interrupción del servicio. El análisis de impacto en el negocio o Business Impact Analysis (BIA) es el mejor punto de inicio para el desarrollo de la estrategia, debido a que está basado en información de toda la organización.

Considerar el impacto potencial de cada tipo de problema. No es adecuado planificar la recuperación de un desastre si no se tiene buen conocimiento del impacto en la organización en los diferentes escenarios. Aun así, es sorprendente cuántas organizaciones ignoran este primer paso en el proceso de continuidad.

El Análisis de impacto en el negocio ó Business Impact Analysis (BIA), evalúa sistemáticamente el impacto potencial resultante de diferentes eventos o incidentes. El objetivo es ayudar a entender el grado del impacto ante la pérdida potencial de un servicio. La pérdida puede ser financiera, de imagen, por efectos regulatorios, etc.

El desarrollo de un Plan de continuidad se inicia por la identificación de los procesos críticos del negocio. La información es entregada por las áreas de negocio de la compañía. Éste análisis determinará las funciones y departamentos dependientes del tiempo en operación, las vulnerabilidades financieras, el impacto operacional y la

estimación de los recursos en total que serían necesarios para lograr el reinicio de las operaciones inmediatamente después de ocurrida una interrupción.

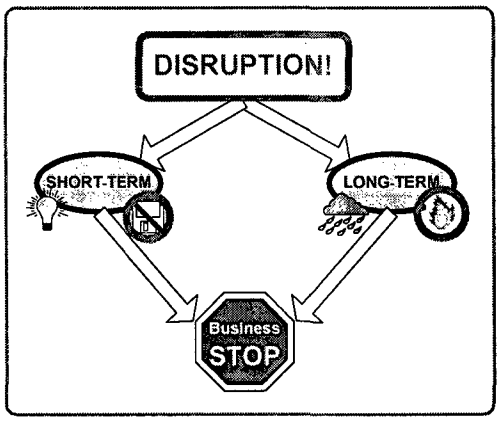
El BIA o Análisis de impacto en el negocio, provee también un centro de atención de toda la organización, de manera que se tiene mayor entendimiento y colaboración de la gerencia.

La definición de estos procesos críticos se realiza en una matriz de impacto estratégico de los procesos, en el que se debe identificar cuáles son aquellos procesos del negocio que se tienen que ejecutar siempre.

El análisis de impacto en el negocio es desarrollado para calificar y cuantificar los riesgos y vulnerabilidades a los que están expuestos las operaciones de la organización así como la habilidad de la compañía para responder a un evento en una ventana de tiempo.

Un evento o interrupción en las operaciones puede tomar varias formas: Corto, debido a un corte de electricidad o a un problema en los sistemas de información; Largo, debido a un incendio o a un desastre natural. Sin importar la causa de la interrupción, las operaciones del negocio se detienen.

Figura 13 Interrupción del negocio



Fuente: Elaboración propia

Se debe entender cómo afectaría un evento al negocio para poder tomar las mejores decisiones que protejan los activos de la compañía y administren correctamente los riesgos.

Un BIA ayuda a definir el impacto concerniente a perder operaciones de negocio y analiza el efecto de este impacto sobre determinadas ventanas de tiempo. El impacto se puede clasificar en dos categorías: Financiero y Operacional. El impacto Financiero como las pérdidas en ventas y las multas por incumplimiento de contratos se reflejan rápidamente. El impacto Operacional como las pérdidas de mercados o la pérdida de la confianza de inversores ocurre lentamente pero el resultado es devastador.

Se deben determinar las ventanas de tiempo de recuperación y requerimientos de recursos mínimos para los procesos del negocio

identificados y categorizados. También se deben determinar los tiempos de reemplazo.

3.1.8.1. Objetivos BIA

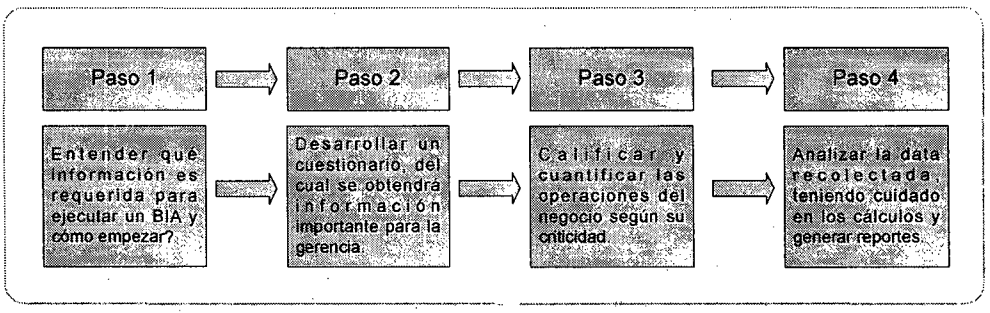
Un BIA consiste en realizar una evaluación de los procesos y sistemas del negocio, para identificar:

- ✓ Áreas, funciones y/o procesos sensibles a interrupciones.
- ✓ Interdependencia entre procesos internos y externos.
- ✓ Impactos financieros de las interrupciones por proceso de negocio.
- ✓ Impactos Operacionales de las interrupciones por proceso de negocio.
- ✓ Sistemas de información críticos para la operación.
- ✓ Requerimientos tecnológicos para el re-inicio y recuperación.
- ✓ Procedimientos de soporte para las operaciones de re-inicio y recuperación.
- ✓ Tiempos objetivo de recuperación (RTO).
- ✓ Puntos Objetivo de recuperación (RPO).
- ✓ Clientes y proveedores críticos de la organización.
- ✓ Recursos necesarios para la recuperación de operaciones.
- ✓ Fechas críticas para la operación del negocio.
- ✓ Los gastos cuantiosos que serán necesarios para continuar con las operaciones después de una interrupción.

✓ El estado actual de preparación de la organización.

Consideraciones para ejecutar un BIA exitoso:

Figura 14 Consideraciones ejecución de BIA



Fuente: Elaboración propia

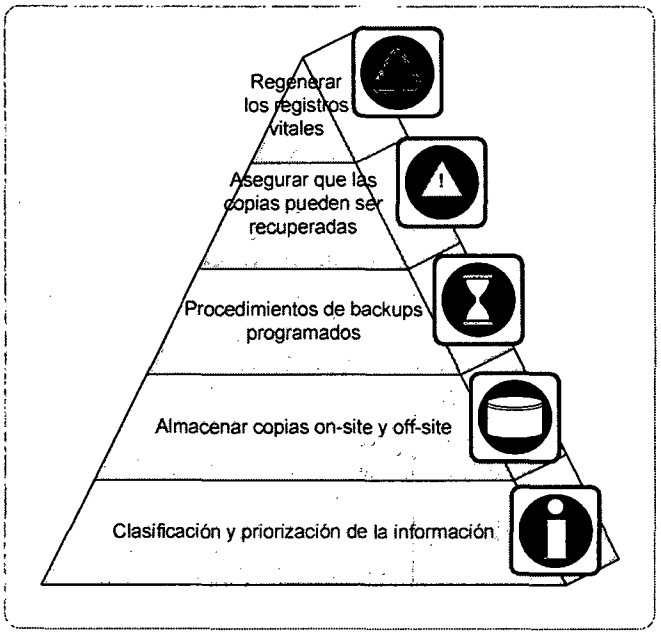
3.1.8.2. Identificación de Registros vitales

Generalmente las discusiones acerca de los riesgos del negocio y los controles preventivos se centran en las facilidades de infraestructura en la que la organización opera.

Los registros vitales son activos importantes de la información de la organización. Un registro vital es aquel que es esencial para preservar, continuar o reconstruir las operaciones de la organización, protegiendo los derechos de la organización, a sus empleados, a sus clientes y a sus dueños.

La supervivencia de un negocio depende de la disponibilidad de la información. Identificar y resguardar de forma segura los registros vitales es un prerequisito esencial para lograr una capacidad de reinicio y recuperación.

Figura 15 Identificar y proteger los registros vitales



Fuente: elaboración propia

Es importante tener en cuenta:

- ✓ La naturaleza de los registros.
- ✓ El tiempo y requisitos para su disponibilidad.
- ✓ El impacto financiero y operativo en procesos dependientes.
- ✓ Multas por la pérdida de registros.

- ✓ Costo de mantener copias adicionales.

Dependiendo de la organización, la protección de los registros vitales puede recaer en un grupo de la compañía o en custodios individuales. El propietario o usuario principal de la información es el responsable de identificar la información como registro vital.

Para el almacenamiento de los registros vitales se debe definir:

- ✓ Medio físico de almacenamiento.
- ✓ Frecuencia de rotación.
- ✓ Patrones estándares de almacenamiento fuera del site (días, semanas, meses..).
- ✓ Criterios de recuperación y autorizaciones (para el escenario en condiciones normales, en reinicio y en recuperación).

3.1.8.3. Identificación de necesidades de respaldo

La responsabilidad de registrar, almacenar, rotar y asegurar los registros vitales debe recaer en las mismas personas que tienen la función de Administrar el Almacenamiento de los datos. En algunos casos podría asignarse esta responsabilidad al personal administrativo de cada area de operación de negocio. En el Data Center, la información vital está bajo el control del Administrador de Almacenamiento de datos o del Administrador de la Red.

Las técnicas para ejecutar un BIA se aplican a cualquier parte de la organización, pero se recomienda que el alcance del BIA abarque toda la empresa.

Los resultados del BIA son utilizados por la gerencia para decidir:

- ✓ Qué operaciones y procesos son esenciales para la supervivencia de la organización.
- ✓ Qué tan rápido deben recuperarse las operaciones y procesos antes de que el impacto de una interrupción se convierta en un desastre.
- ✓ Cuáles son las estrategias para cumplir con las ventanas de re-inicio de operaciones.
- ✓ Qué recursos son necesarios para volver a iniciar las operaciones críticas, funciones y procesos de la empresa.

Las respuestas a estas preguntas son utilizadas para elaborar la estrategia de continuidad de negocio de la empresa.

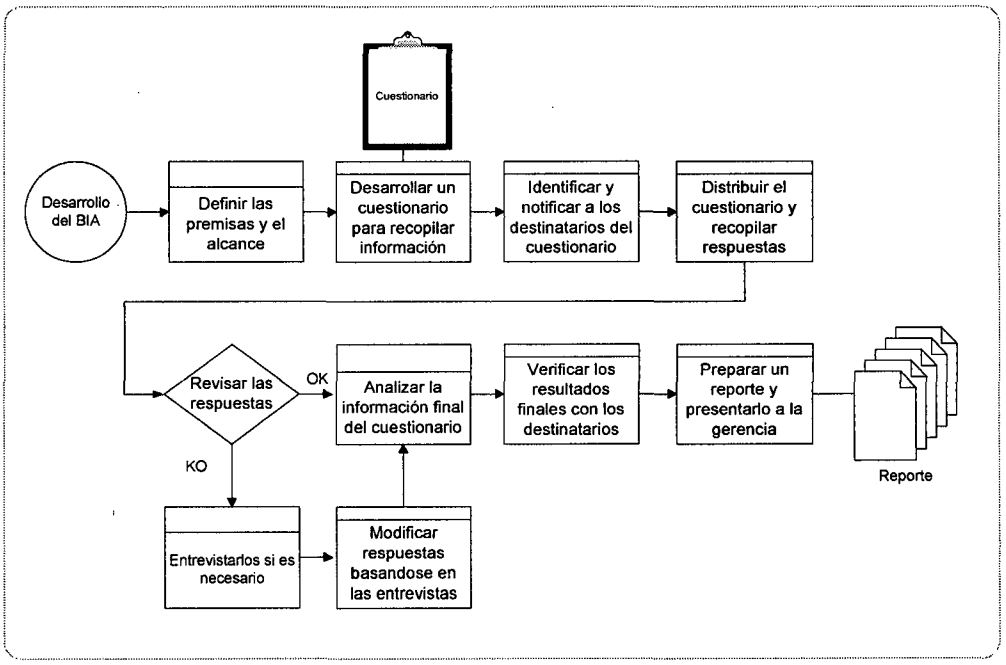
3.1.8.4. Entrevistas y Cuestionarios a la empresa

El encargado del planeamiento de la continuidad debe estar bien preparado para presentar una vista entendible de las pérdidas potenciales

del negocio y tomar las acciones necesarias basadas en las prioridades definidas por la gerencia.

Desarrollar un BIA requiere, como cualquier otro proyecto, de un plan basado en una metodología estructurada. Para obtener información fidedigna lo mejor es acudir a los dueños de los productos y servicios del negocio para que a través de una entrevista y cuestionarios entreguen un feedback que luego servirá para identificar el riesgo potencial de no recuperar tal o cual producto o servicio. A continuación se muestran los pasos que se deben seguir para realizar una entrevista y/o cuestionario:

Figura 16 Pasos para realizar el cuestionario BIA



Fuente: elaboración propia

Por medio del cuestionario se deberá recopilar la siguiente información:

- ✓ Datos básicos del proceso y de su dueño.
- ✓ Frecuencia del proceso.
- ✓ Períodos de tiempo críticos.
- ✓ Tiempo máximo de interrupción.
- ✓ Volumen de trabajo del proceso.
- ✓ Indicadores y medidas de desempeño existentes.
- ✓ Impactos: Financiero, cliente interno, cliente externo, eficiencia operativa, aspectos legales, imagen - reputación y en general para la organización como negocio.
- ✓ Dependencias internas y externas.
- ✓ Aplicaciones informáticas que lo soportan.
- ✓ Procedimientos alternos existentes o sugeridos.
- ✓ Efectividad de los procedimientos alternos.
- ✓ Registros vitales de cada proceso.
- ✓ Complejidad de recuperación de las dependencias evaluadas.
- ✓ Recursos mínimos para la recuperación de cada dependencia.

Ver **¡Error! No se encuentra el origen de la referencia.** para mas detalle acerca de cómo ejecutar un BIA, Ejemplos y Formato del Reporte.

3.1.8.5. Tiempos de recuperación del proceso de negocio

Los tiempos de recuperación que deben ser considerados para las operaciones y servicios de la empresa deben estar documentados en el reporte BIA que es enviado a la gerencia. Si no se utilizaron métricas formales para identificar la criticidad de las operaciones de negocio, es muy importante que se establezcan, se documenten y se mantengan como parte de las políticas para la continuidad de negocio de la empresa.

Las calificaciones generalmente están expresadas en términos del mínimo y máximo tiempo que puede ser interrumpido un proceso o servicio de la organización. La gerencia debe conocer y entender que algún proceso o servicio en particular podría no estar disponible luego de una interrupción. Con esta información se puede determinar la tolerancia y concentrarse en el re-inicio de las operaciones, lo cual queda documentado en el plan.

3.1.8.6. Objetivos de recuperación

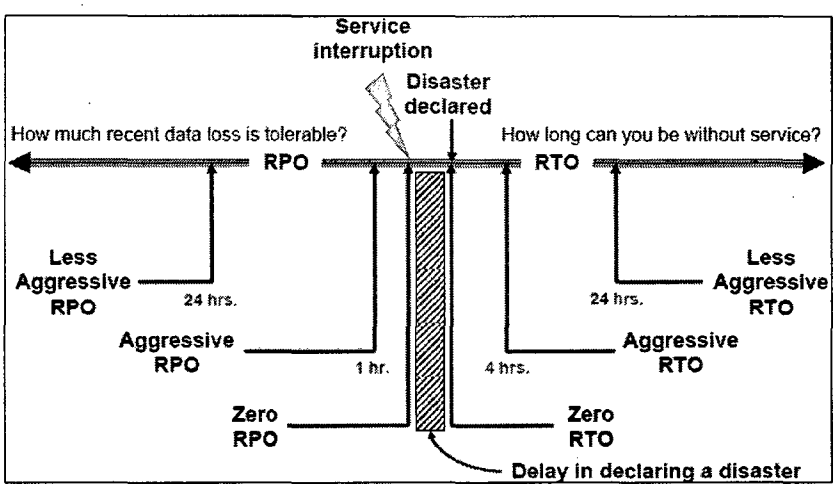
Cuando ocurre un desastre y el negocio sufre una interrupción en sus operaciones, el tiempo es considerado un elemento muy importante para la continuidad operativa del negocio.

A partir de ocurrida la interrupción, se debe asumir que correrá un tiempo que debe ser pequeño hasta que la interrupción se declare como desastre y se decida iniciar los procedimientos de contingencia.

Luego del tiempo que toma declarar un desastre, siguen dos tipos de tiempo importantes para el negocio, como son: el tiempo de recuperación de las operaciones y el punto en el tiempo a partir del cual se recupera la información.

En la siguiente figura se representan dos objetivos de recuperación, tanto de tiempo – RTO, como de pérdida de información - RPO.

Figura 17 Objetivos de recuperación RTO/RPO



Fuente: Symantec Corporation

- ✓ Tiempo objetivo de recuperación ó Recovery Time Objective (RTO)

Éste objetivo busca responder las siguientes preguntas:

- ✓ Cuál es la tolerancia de tiempo fuera de servicio?.
- ✓ Cuánto tiempo puede estar el negocio sin operar?.

El RTO no se refiere únicamente al tiempo que toma recuperar un sistema, una aplicación y su data, como su nombre lo dice, el RTO es el objetivo o el tiempo ideal en el cual se necesita la disponibilidad de una funcionalidad o servicio específico inmediatamente después de ocurrida una interrupción.

Entonces, el RTO representa el tiempo máximo que pasa antes de que una organización sea vea afectada negativamente por la interrupción de uno de sus procesos o funcionalidades de negocio principales. Debido a esto, la tarea de definir el RTO recae principalmente en los administradores del negocio y no en los administradores de los sistemas.

La información (procesos de negocio) debe ser recopilada de las diferentes unidades de negocio y luego analizada, para obtener algunas conclusiones respecto a las pérdidas financieras y de imagen en los que se podría incurrir y a la ventana de tiempo en la que se deben reiniciar las operaciones. Para los cálculos del

RTO considerar el peor momento en el cual podría ocurrir una interrupción, por ejemplo en quincena o a fin de año.

Para casos en el que no se pueda recuperar una funcionalidad o proceso de negocio porque depende de un sistema o aplicación que demorará en recuperar, se deben generar documentos con procedimientos manuales que puedan brindar el servicio temporalmente mientras se cumple el RTO definido.

Se debe definir el tiempo máximo de "fuera de servicio" que el negocio está dispuesto a tolerar por cada uno de sus procesos. El RTO no debe superar el tiempo máximo tolerado.

El RTO debe considerar el tiempo que ocupa la notificación, la respuesta, la evaluación de la situación y otras demoras, ya que todos estos elementos pueden consumir parte del RTO antes de que el verdadero esfuerzo de recuperación sea iniciado.

- ✓ Punto objetivo de recuperación ó Recovery Point Objective (RPO)

Éste objetivo busca responder las siguientes preguntas:

- ✓ Qué tan actualizados necesitan estar los datos para el momento de recuperación de operaciones del negocio?.
- ✓ Cuánta pérdida de información se puede tolerar?.

El RPO es la métrica del punto en el tiempo hasta el cual la data puede ser recuperada luego de ocurrido un evento que podría causar pérdida de data. Por ejemplo si una organización utiliza los tradicionales tapes backups (cintas de respaldo) y experimenta un problema en sus bases de datos en el que se malogra la data, el punto de recuperación para esa base de datos sería el último backup antes de este evento.

Una manera práctica de determinar el RPO para un tipo de data es evaluar cuánto de esta data la organización está dispuesta a perder, es decir data que no será respaldada, comparándolo con el costo de respaldarla.

Actualmente la mayoría de organizaciones modernas dependen de su infraestructura tecnológica. Durante un programa de continuidad de negocios se debe determinar como una actividad crítica de la organización la definición de la escala de RPOs, desde cero hasta el punto de falla que impacta a la organización. Esta información sirve para que la organización decida cuánto dinero está dispuesta a invertir en resiliencia.

Entonces, almacenar mucha data puede ser muy costoso, almacenar poca data puede impactar negativamente en el negocio. Debido a que se debe tomar la decisión de cuánta data almacenar, se debe trabajar con los especialistas en tecnología para llegar a

un nivel en el que la inversión sea la adecuada para la continuidad del negocio.

- ✓ Tiempo objetivo de recuperación de la Red ó Network Recovery Objective (NRO)

  Este objetivo no es muy utilizado, pero es de gran utilidad en organizaciones en las que la red es el elemento primordial para las operaciones del negocio.

  NRO indica el tiempo requerido para recuperar la operatividad de la red. Tener en cuenta que la recuperación de los sistemas no está completa si los clientes no pueden acceder a las aplicaciones vía las conexiones de red. El NRO incluye el tiempo requerido para conmutar a enlaces de comunicaciones alternas, re-configurar routers y equipos necesarios para la operatividad de la red, así como modificar configuraciones en los sistemas de los equipos clientes.

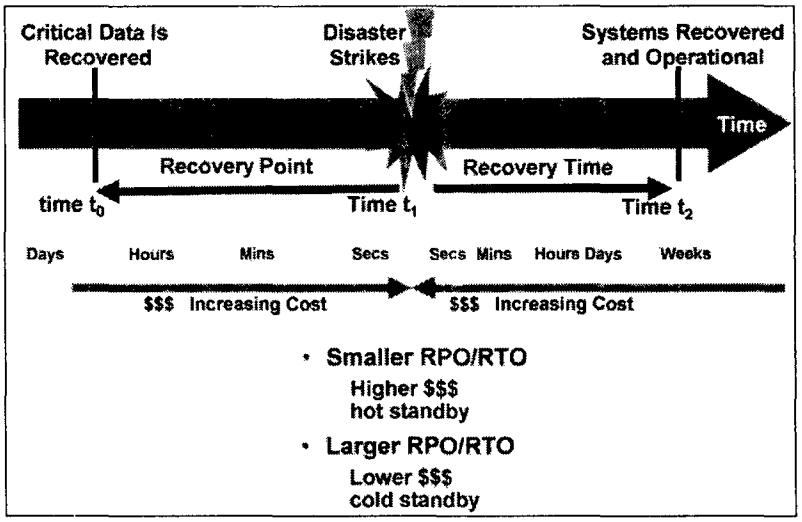
  Se debe contar con un plan detallado de recuperación de redes y este plan es tan importante como la recuperación de la data en un escenario de Recuperación de un desastre.

Para determinar cuáles son los objetivos asignados a cada operación, proceso o sistema que soporta el negocio es necesario contar con la aprobación de los dueños del servicio o producto, ya que son ellos

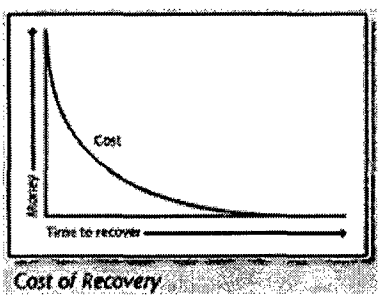
quienes mejor conocen la criticidad y el impacto que podría causar el no contar con ésta información.

Identificando correctamente los procesos de negocio críticos, las organizaciones estarán en una mejor posición para calcular y aprovechar la ecuación Costo versus Riesgo. Una organización podría intentar proteger todas los procesos de negocio posibles por medio de varios métodos: Storage Area Networks (SANs), Servicios de terceros, Transferencia de data en modo síncrono o asíncrono, pero no todos los procesos de negocio valen la inversión. Identificando los objetivos de tiempo de recuperación y de punto de recuperación necesarios para cada proceso, las organzaciones podrán asignar eficientemente los recursos. Por ejemplo: Una aplicación de facturación. Aunque es crítica para el negocio debido a que representa una entrada a en las ganancias, el proceso de facturación en muchas organizaciones tiene un RPO alto (>72 hours). Si un cliente recibe una factura un jueves en vez de un lunes de la misma semana, realmente no hace una diferencia en las ganancias anuales. Para este caso en particular, el costo de tener un RTO de horas no hace ninguna diferencia en el negocio, a menos que presente interdependencias en el sistema y ocasione que otro proceso importante para el negocio falle.

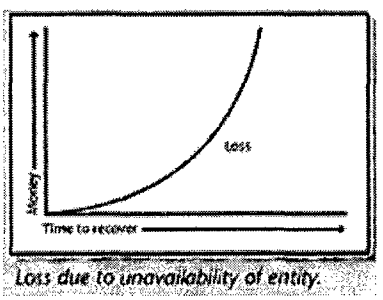
Figura 18 Variación del costo cuando varía el RTO/RPO



Fuente: Data Center Disaster Recovery – Nelson Muñoz – Cisco.

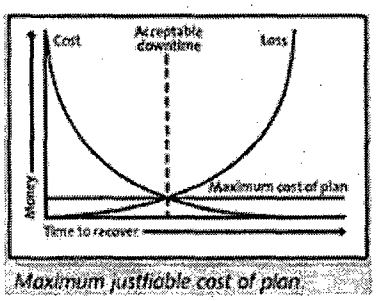


Cuanto más largo es el tiempo de recuperación, menor es el costo involucrado en la recuperación. Así mismo, si el tiempo de recuperación se va acercando a cero, el costo involucrado en la recuperación va aumentando.



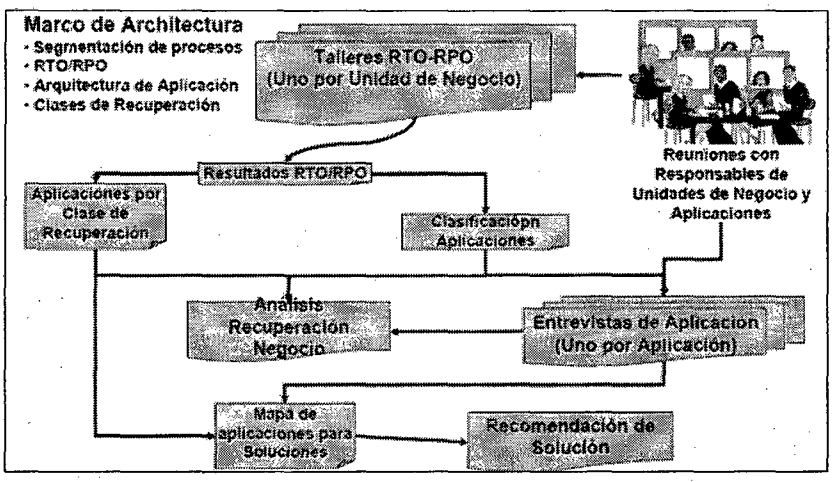
De la misma forma, así como a mayor tiempo de recuperación menor costo, se cumple que a mayor tiempo de recuperación mayor pérdida de información y de imagen, ya que el tiempo que demore en respaldarse la data sería mayor, además del tiempo de recuperación de las operaciones.

Cruzando ambas gráficas, la de costos y la de pérdida se puede obtener el tiempo aceptable para estar en modo fuera de servicio, así como también se puede obtener el máximo costo del plan.



En la siguiente figura se puede apreciar el flujo de validación de objetivos asignados a las operaciones de negocio.

Figura 19 Flujo de validación de objetivos RTO/RPO



Fuente: Symantec Corporation

Luego de contar con la información brindada y validada por los dueños de las operaciones de negocios y por los administradores de las aplicaciones o sistemas que soportan estas operaciones se elabora un mapa en el que se cruza la información para proceder a generar la

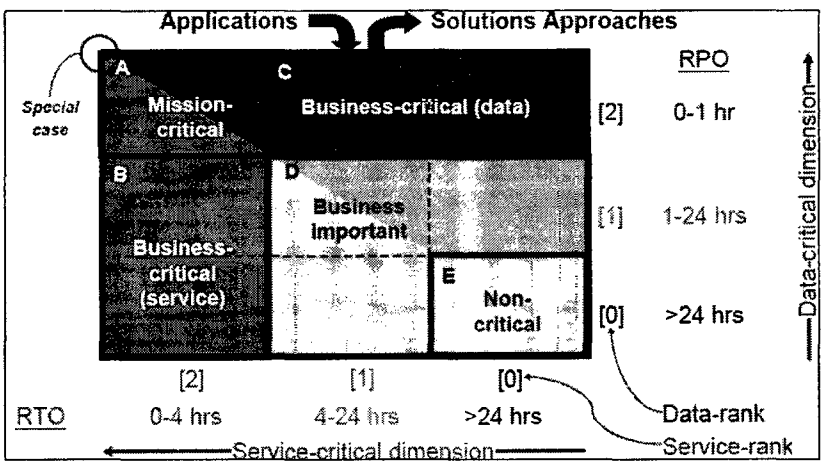
recomendación final en la que se calificarán las operaciones/procesos versus las aplicaciones/sistemas.

3.1.8.7. Calificaciones de las operaciones de negocio

Las operaciones de negocio son clasificadas según la criticidad, la cual se define en base a parámetros identificados en el análisis de impacto:

- ✓ El tiempo de recuperación de la operación (RTO).
- ✓ El punto de recuperación de la información (RPO).
- ✓ El costo de recuperación de las operaciones y los sistemas que las soportan.

Figura 20 Clasificación de criticidad de los procesos de negocio



Fuente: Symantec Corporation

Según la figura anterior, la clasificación de la criticidad de las operaciones de negocio se puede dividir en 5 tipos:

Tabla 4 Clasificación de la criticidad de los procesos de negocio

	Criticidad de las operaciones de negocios	Descripción
A.	Mission-critical	Crítico para la supervivencia del negocio, el tiempo de recuperación tiene que ser mínimo, así como la pérdida de información.
B.	Business-critical (service)	Crítico para la continuidad del servicio.
C.	Business-critical (data)	Crítico para la preservación de la información.
D.	Business important	Importante para el negocio.
E.	Non-critical	No impacta directamente en la supervivencia del negocio, pueden ser recuperados en tiempos mayores al día, y la información también puede reprocesarse con un día de atraso.

Fuente: Symantec Corporation

De otra manera, la criticidad de las operaciones se puede dividir en 4 tipos, los cuales se describen en la siguiente figura:

Tabla 5 Clasificación de la criticidad de los procesos de negocio

	Criticidad de las operaciones de negocios	Descripción
A.	Críticos	Sus funciones no pueden ser ejecutadas a menos que sean reemplazadas por recursos idénticos.
		No se pueden usar métodos manuales.
		Costo de interrupción es muy alto.
B.	Vitales	Sus funciones pueden ser ejecutadas manualmente durante un período corto.
		Mayor tolerancia a las interrupciones.
		Costos de interrupción menores si la caída es menor a 3 días.
C.	Sensitivos	Sus funciones pueden ser ejecutadas manualmente durante un período largo.
		Mientras se hace manualmente requiere staff adicional.
		Costos de interrupción medios.
D.	No Críticos	Sus funciones pueden ser interrumpidas durante un periodo relativamente largo.
		Costos de interrupción mínimos o cero.

Fuente: Manuel Ballester – RedSeguridad – Conferencias FIST.

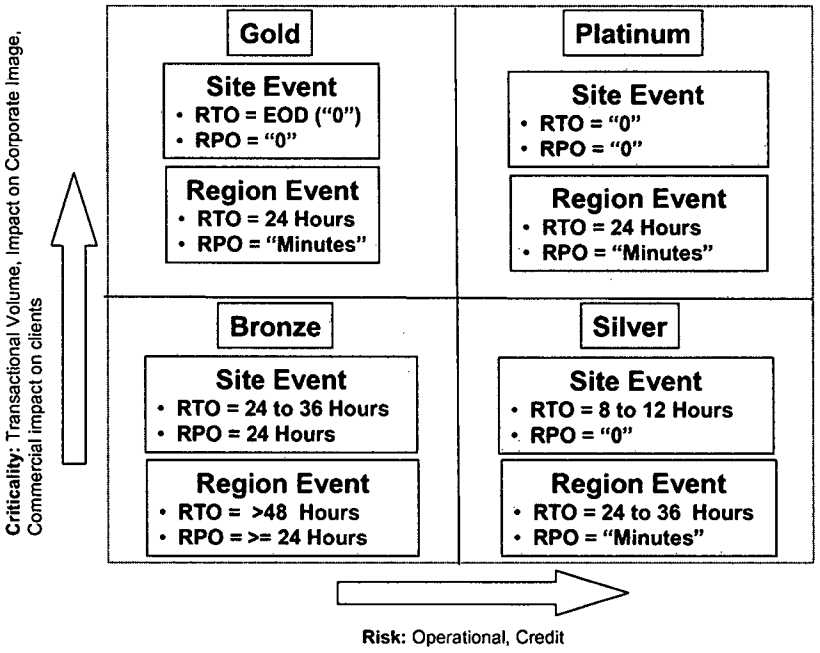
También se puede asignar pesos al resultado de la clasificación de las operaciones/procesos y aplicaciones/sistemas, y a estos pesos llamarlos con la nomenclatura de metales-preciosos que suelen ser utilizados para niveles de Calidad de servicio (QoS) o Acuerdos de niveles de servicio (SLA):

Tabla 6 Clasificación de la criticidad de los procesos de negocio

	Criticidad de las operaciones de negocios	Descripción
A.	Premium	Respaldo en tiempo real, No tolera demoras, el RTO y RPO es cero
B.	Platinum	Respaldo en tiempo real, Tolera demoras
C.	Gold	Respaldo en tiempo real, Tolera demoras
D.	Silver	No se respalda en tiempo real
E.	Bronze	No se respalda en tiempo real
F.	Standard	No se consideran críticos

Adaptado de: Clasificación por criticidad.

Figura 21 Clasificación Criticidad versus Riesgo



Fuente: Tomado del informe de IBM Consulting group

3.1.8.8. Recuperación e información almacenada off-site

Las interrupciones más prolongadas y más costosas, en particular los desastres que afectan a las instalaciones, requieren recuperación (off-site)

Para asegurar que la información crítica estará disponible, una o más ubicaciones para el storage secundario deben ser utilizadas para resguardar la data backup, esto puede significar tener la data en otros

Data Centers, considerar que las ubicaciones secundarias deben estar lo suficientemente lejos de la primaria, tal que no deben ser afectados por el mismo evento, pero también debe considerarse que las ubicaciones deben ser de fácil acceso.

Seleccionar la ubicación del Data Center secundario en un lugar que supere o iguale las medidas de seguridad del ambiente que ya posee la ubicación primaria. Se deben tener procedimientos estrictos para el control del acceso a la data e incluir estos procedimientos en el plan de continuidad, además de los números de contacto y los procedimientos detallados de recuperación.

3.1.8.9. Tipos de instalaciones alternativas para respaldo

- ✓ Mirrored sites

  Se llama Mirrored site o Instalaciones de procesamiento duplicados al data center que en todos los aspectos es idéntico al site principal, ambos tienen la misma disponibilidad de la información. Es equivalente a tener un site redundante y por lo mismo es la opción más costosa.

- ✓ Hot sites

  Se llama Hot site al data center que cuenta con espacio para el personal y está totalmente equipado con los recursos y computadores en stand-by necesarios para recuperar y soportar las

funciones críticas del negocio inmediatamente después de ocurrido un desastre.

- ✓ Warm sites

  Es similar el Hot site, pero está parcialmente equipado y la data almacenada no está al día pero tampoco es muy antigua.

- ✓ Cold sites

  Se llama Cold site al data center que se encuentra acondicionado pero no tiene ningún equipo. Está listo para que se mueva todo el equipo y sea instalado en los espacios asignados. Cuenta con puntos para la telefonía, puntos de energía eléctrica, UPS, además de otras facilidades. Toma algo de tiempo lograr que este tipo de site o sitio quede completamente operativo. Contratar un Cold site implica que el negocio determine clausulas en que el proveedor debe cumplir con terminar la instalación de todos los equipos y dejar el site listo.

- ✓ Mobile sites

  Se llama Mobile site o Sitio móvil al data center que es portable por lo que tiene una configuración de menores dimensiones. Éste puede ser ubicado cerca del sitio o data center principal para evitar los viajes del personal clave.

- ✓ Acuerdos recíprocos con otras organizaciones

  En este caso, la información del negocio A es almacenada en el data center de la organización B y la información de aquella organización B es almacenada en el data center del negocio A.

La siguiente tabla describe los tipos de sites para la recuperación de un desastre, los costos y el tiempo de la configuración inicial.

Tabla 7 Tipos de instalaciones para la recuperación de un desastre

Tipo de sitio (Data Center)	Costo	Tiempode configuración inicial
Cold Site	Bajo	Largo
Warm Site	Medio	Medio
Hot Site	Medio/Alto	Corto
Mirrored Site	Alto	Ninguno

Fuente: Disaster Recovery Planning Procedures and Guidelines - USAID

Para seleccionar el site adecuado se debe tener en cuenta su compatibilidad, disponibilidad, los costos, y el tiempo que demora en tener lista la configuración inicial.

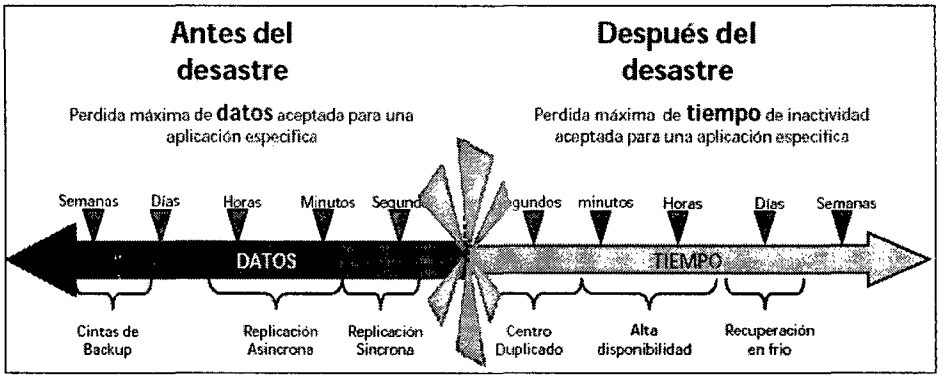
3.1.8.10. Tipos de respaldo de data

- ✓ **Replicación síncrona –** el tiempo de la copia o backup es cero, así como el RPO es cero.
- ✓ **Replicación asíncrona –** el tiempo de la copia o backup se define de acuerdo al punto en el tiempo hasta el cual se desea poder

recuperar información, el RPO en este tipo de respaldo no debe superar las 24 horas.

- ✓ **Cintas de Respaldo** – el intervalo de tiempo entre las copias o backups es mayor a 24 horas, por lo que el RPO es mayor a 24 horas.

Figura 22 Tipos de respaldo de data



Fuente: Telefónica - Juan Carlos Muñoz de Toro - Gestor de Producto de BRS

3.1.8.11. Evaluación de riesgos de la recuperación en storage off-site

Se debe obtener copias secundarias del software desarrollado en casa, ya que es vital para la continuidad de las operaciones del negocio. En una situación de desastre, el software resguardado localmente podría ser inutilizable, por lo que es necesario copiar el software localmente y además en otra ubicación a la que llamamos off-site, tanto el código fuente como el formato ejecutable.

También se debe obtener copias del software licenciado, esto se logra por medio de acuerdos contractuales con los proveedores de los paquetes licenciados de software. Generalmente la copia de estos programas está prohibido por lo que se debe contactar al proveedor para que entregue nuevas copias. Algunos acuerdos contractuales permiten expresamente la creación de copias del programa para ser utilizados en ejercicios de Recuperación o en respuesta a una interrupción del negocio. Se debe revisar detalladamente cada licencia y generar procedimientos especiales para la copia de los programas.

3.1.8.12. Análisis BIA de TI

El propósito del análisis de impacto de la Tecnología en el negocio es combinar las prioridades del BIA con la capacidad actual de recuperación de la organización.

El análisis de impacto en el negocio se centra en el entorno actual, generalmente en la infraestructura de tecnología de información del negocio. Se debe ejecutar una evaluación para comprobar si se puede recuperar la infraestructura tecnológica. La evaluación de los centro de datos o de los sistemas de Información debe ser detallada, se debe validar las prácticas actuales de administración de la información, de las aplicaciones, servidores y de la red.

La estrategia de recuperación se obtendrá del análisis del costo que supondría una interrupción en las operaciones del negocio, el cual se calcula en base a la información recopilada y analizada en el BIA y a los objetivos de recuperación definidos.

En el análisis de impacto en el negocio de las tecnologías de información es necesario identificar:

- ✓ La criticidad de los recursos de información relacionados con los procesos críticos del negocio, enumerando y clasificando las Aplicaciones de más a menos críticas.
- ✓ El período de tiempo de recuperación crítico por Aplicación antes de incurrir en pérdidas significativas.
- ✓ Con qué elementos completar el sistema de clasificación de riesgos.
- ✓ Los Puntos únicos de falla para la planificación de su eliminación.

3.1.8.13. Resultados BIA

El resultado principal de un BIA son las Estrategias de Recuperación, las cuales son una combinación de medidas de prevención, detección y corrección.

Una vez que se tiene la información y operaciones clasificadas tanto de los procesos como de las aplicaciones del negocio, se generan reportes que indiquen:

- ✓ Inventario de los procesos críticos del negocio.
- ✓ Inventario de aplicaciones que soportan las aplicaciones críticas del negocio.
- ✓ Mapa de procesos y aplicaciones a ser recuperadas por escenario.
- ✓ Secuencia de recuperación de procesos y sistemas críticos
- ✓ Tiempos de recuperación por escenario para cada proceso crítico del negocio.
- ✓ Impacto financiero y operacional de una interrupción en los procesos críticos del negocio.
- ✓ Requerimientos mínimos de los procesos o aplicaciones críticas del negocio durante las operaciones de recuperación.

3.1.9. Estrategias

La estrategia está conformada por: La Formulación, La Selección y La Implementación de los métodos que mitigarán los riesgos y vulnerabilidades, minimizarán la probabilidad de que ocurra algún incidente y minimizarán los efectos. Las estrategias deben ser desarrolladas de manera que cumplan con los objetivos y metas de cada una de las fases que compongan el plan de continuidad operativa, como

por ejemplo las fases de respuesta, reanudación, recuperación y retorno a la normalidad.

3.1.9.1. La Formulación

Las estrategias para la continuidad de negocios suelen ser resultado del BIA, que generalmente es ejecutado para calificar y cuantificar las vulnerabilidades de las operaciones de la organización.

El BIA proporcionará información para definir preliminarmente las estrategias. La definición final debe ser desarrollada por el coordinador de la continuidad de negocios y los demás equipos. Las estrategias resultantes serán los métodos usados durante las pruebas de los planes de continuidad de negocios.

Cada estrategia debe cumplir las siguientes condiciones:

- ✓ Debe ser técnica y económicamente viable
- ✓ Debe tener alta probabilidad de éxito
- ✓ Debe permitir ser validado por medio de las pruebas
- ✓ Debe soportar las actividades de las fases de respuesta, reanudación y recuperación, controladas por tiempo.

3.1.9.2. La Selección

Las estrategias pueden enfrentar muchas variaciones, una probable duración o tipo de interrupción, el ciclo del negocio en el cual ocurre el desastre, o la disponibilidad de recursos.

La selección de la estrategia depende de:

- ✓ La criticidad del proceso a proteger.
- ✓ El costo de la estrategia.
- ✓ El tiempo de recuperación objetivo.
- ✓ El punto de recuperación objetivo.

Por ejemplo, la estrategia para reiniciar las operaciones luego de una interrupción ocurrida durante un período pico de producción podría ser utilizar una instalación Hot Standby. Otra estrategia podría aplicarse cuando la interrupción ocurre en un período de baja demanda de la producción, en este caso bastaría con subcontratar los servicios de producción.

3.1.9.3. La Implementación

Dependiendo del alcance del plan, el desarrollo de la estrategia podría ser un proceso complejo para definir y analizar alternativas para hacer negocios, investigar y seleccionar tecnologías alternativas, evaluar los logros y errores de otras organizaciones buscando alcances similares,

determinar el proveedor que mejor servicio ofrezca y finalmente seleccionar una estrategia la cual brinde una nivel aceptable de servicio y costo/beneficio.

Las estrategias deben cambiar con los cambios en la organización. Dependiendo del costo y del riesgo, podría ser necesario adoptar una estrategia temporal que cumpla con una porción de las necesidades hasta que se pueda establecer la estrategia definitiva.

3.1.10. Desarrollo de los Planes de Continuidad

En esta parte se define el número y la estructura de los planes de la organización. Dependiendo de factores como la ubicación geográfica o el número de departamentos, productos y servicios por ubicación o lineas de negocio, se necesitarán pocos o muchos planes.

Es muy importante determinar una agrupación lógica de los departamentos, operaciones o canales de negocio para la definición de los planes, ya que esto asegura que el número de planes definidos proporcionarán una continuidad efectiva a la organización.

Las actividades para diseñar, desarrollar e implementar los planes de continuidad del negocio son:

- ✓ Identificar requerimientos para el desarrollo de los planes.
- ✓ Definir requerimientos de control y administración de la continuidad.
- ✓ Definir un formato y la estructura principal de los componentes de los planes.
- ✓ Elaborar un borrador de los planes.
- ✓ Definir procedimientos de manejo de crisis y continuidad del negocio.
- ✓ Definir las estrategias de evaluación de daños y reanudación.
- ✓ Desarrollar una introducción general a los planes.
- ✓ Desarrollar la documentación de los equipos de operación del negocio.
- ✓ Desarrollar la documentación de los equipos de recuperación de tecnología informática.
- ✓ Desarrollar el sistema de comunicaciones.
- ✓ Desarrollar los planes de los usuarios finales de aplicaciones.
- ✓ Implementar los planes.
- ✓ Establecer los procedimientos de mantenimiento, control y distribución de los planes.

Finalmente, todas estas actividades sirven para proveer continuidad en los marcos establecidos por los RTO'S y RPO'S.

3.1.11. Planes de gestión de crisis

El objetivo principal de la fase de respuesta de un programa de continuidad de negocios es administrar la crisis.

La gestión de crisis es la fase en la que se planea e implementa la reacción o respuesta de la organización frente a un incidente o emergencia.

Los objetivos de esta fase incluyen:

- ✓ La protección de la vida humana, salvaguardar la seguridad de las personas tanto en su salud como en su vida personal.
- ✓ Limitar el daño al Data Center y a los equipos, evaluar los daños.
- ✓ Estabilizar las operaciones, el servicio y el impacto en la imagen pública.
- ✓ Administrar y comunicar la información acerca del incidente.

Actividades para el planeamiento de la respuesta de la organización:

- ✓ Respuesta a una emergencia - Procedimientos de respuesta para minimizar daños al personal.

- ✓ Administración de incidentes - Planes de administración de incidentes para controlar y mitigar daños al Data Center y a los equipos.
- ✓ Administración global de crisis - Plan de administración de crisis desarrollado para establecer tareas que la gerencia deberá ejecutar con el fin de limitar el impacto.
- ✓ Comunicaciones internas y externas - Planes de comunicaciones de crisis para identificar cómo será administrada y comunicada la información acerca de la crisis.

3.1.11.1. Plan de respuesta a una emergencia

El plan de respuesta a una emergencia es la parte más importante de administrar una crisis, este demuestra el compromiso que tiene la organización con la vida y seguridad de los empleados. Contiene las políticas, procedimientos y actividades/tareas a ser ejecutadas en caso ocurra una emergencia.

a) Desarrollo de planes de respuesta

La fase de respuesta es el proceso de planear e implementar la reacción de la organización a un incidente o emergencia.

Los objetivos de esta fase incluyen:

- ✓ Proteger las vidas, la seguridad y la salud del personal.
- ✓ Limitar el daño a las instalaciones y equipos.
- ✓ Estabilizar la operatividad.
- ✓ Limitar el impacto en la imagen pública.
- ✓ Administrar y comunicar la información acerca del incidente.

Los planes a desarrollar podrían incluir, por ejemplo:

- ✓ Plan de respuesta a desastres naturales: Terremotos, Tornados, Huracanes e Inundaciones.
- ✓ Plan de respuesta a desastres causados por el Hombre: Terrorismo, Sabotaje

b) Equipos de respuesta a emergencias

Un equipo de respuesta a emergencias debe:

- ✓ Trabajar eficientemente bajo condiciones de alto estrés.
- ✓ Establecer y mantener buenas comunicaciones a través de la organización.
- ✓ Contar con miembros de equipo primario y secundario.
- ✓ Facilitar la toma de decisiones.

- ✓ Usar los recursos limitados para responder de la mejor manera tanto a interrupciones cortas como a desastres de gran escala.

3.1.11.2. Plan de administración de incidentes

Establece la presencia inmediata de los miembros del equipo en el site de la emergencia.

Implementa la estructura de administración de incidentes.

Clasifica el impacto de la emergencia y las consecuencias en estimados realistas.

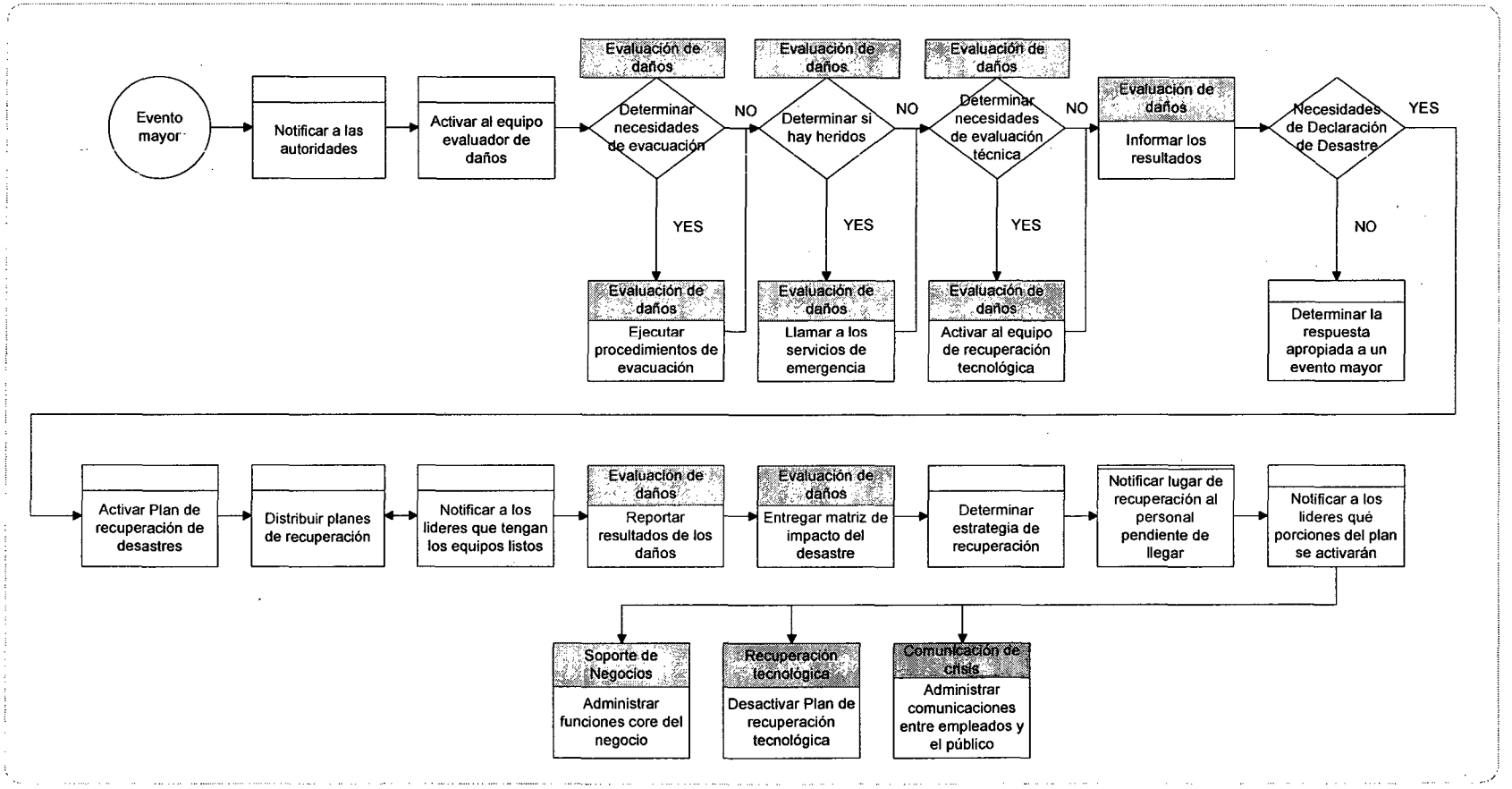
Toma decisiones y brinda recomendaciones si se tiene que escalar el plan.

Administra el nivel de controles requeridos en las actividades.

3.1.11.3. Plan de administración de crisis global

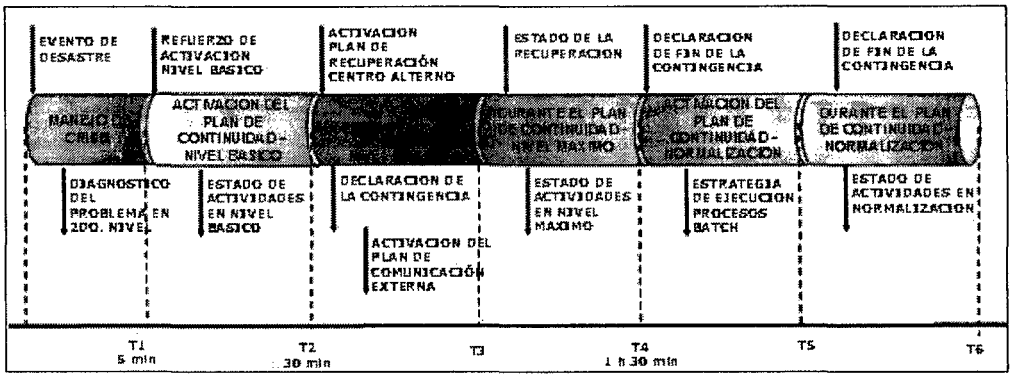
El impacto y alcance de un evento puede ser mayor que uno ocurrido en un solo site. El evento puede convertirse en una situación que puede agravarse con poca o ninguna advertencia. Esto podría afectar la supervivencia de la corporación, incluyendo problemas en el flujo de caja, la imagen y la reputación de la organización, el mercado, cambios de regulación.

Figura 23 Flujo de procesos para la administración de una crisis



3.1.11.4. Plan de administración de las comunicaciones

Figura 24 Plan de administración de las comunicaciones



Para llevar un mejor control del plan de comunicaciones se puede elaborar una matriz en la que se indiquen los responsables de la comunicación según sea el caso. En el Anexo **¡Error! No se encuentra el origen de la referencia.** se puede encontrar la matriz cuyos campos son descritos a continuación:

Tipo de comunicación - Es el tipo de comunicaciones que se desea tener, como por ejemplo:

- ✓ Comunicación con equipos de recuperación/contingencia
- ✓ Comunicación al cliente
- ✓ Comunicación a la organización
- ✓ Comunicación con otras unidades

Medio - Es el tipo de herramienta o medio de comunicación que desea emplear. Ej. Email, website, etc

Responsable - Es el encargado de la tarea de comunicación.

Frecuencia - Es la periodicidad con que se realizará la comunicación. Ej. Cada vez que se requiere, diaria, semanal, mensual, etc.

Disparador - Indica la circunstancia o evento que genera la comunicación. Ej: cliente en ventanilla.

Descripción de la comunicación - En qué consiste la comunicación y cuál es su objetivo.

Audiencia - Es la audiencia a quien estará dirigida la comunicación. Ej. Al equipo de trabajo, a todo el personal de una división, etc.

3.1.12. Programa de capacitación a los grupos de recuperación

3.1.12.1. Entrenamiento

Se requiere entrenamiento para asegurar la efectividad y eficiencia de los equipos que están desarrollando los planes para la continuidad de la organización.

El entrenamiento puede darse durante un prueba dirigida, una reunión, discusiones de grupo, revisiones uno a uno, etc.

El propósito es brindar al empleado la confianza y habilidades para que complete las tareas asignadas con responsabilidad.

3.1.12.2. Por especialización de equipos

El equipo de respuesta a emergencias, debe estar familiarizado con los planes de administración de crisis de la organización, con escenarios de interrupciones y respuesta en ventanas de tiempo. Debe participar en ejercicios de respuesta a escenarios de desastre.

El equipo de reinicio de operaciones, debe estar familiarizado con las capacidades del data center, deben conocer sus responsabilidades sobre el mantenimiento y la operatividad del data center. Debe participar en ejercicios del plan de continuidad que involucren al data center.

El equipo de tecnología, debe participar en los ejercicios dirigidos por el coordinador de la continuidad de negocios. Deben revisar las políticas y validar los procedimientos del equipo de reinicio de operaciones. Luego de grandes cambios los equipos se deben reunir y revisar qué se debe actualizaren los planes.

3.1.13. Programa de capacitación y concientización a los usuarios

- ✓ Definir objetivos de concientización y entrenamiento
- ✓ Desarrollar e implementar varios tipos de programas de entrenamiento
- ✓ Desarrollar programas de concientización
- ✓ Identificar otras oportunidades de educación

3.1.14. Plan de pruebas y Aseguramiento de la calidad

3.1.14.1. Pruebas

Antes las pruebas estaban centradas en el reinicio de la operatividad de los sistemas. Recientemente la industria de recuperación del negocio ha empezado adoptar una visión ampliada de las pruebas, una vista en la que todos los sistemas de información, los procesos de negocio y los departamentos de soporte de la organización deben participar.

El plan de pruebas tiene como objetivo verificar la efectividad y preparación de parte o toda la continuidad de la organización. Las pruebas, son actividades planeadas y programada con anticipación.

El plan de pruebas no busca conocer si el resultado es "satisfactorio" o fallido", este concepto podría causar en la gerencia una percepción equivocada de los objetivos de un plan de pruebas. Debe entenderse que cada ejercicio de pruebas es una oportunidad de mejorar los planes de la organización.

El mecanismo de cualquier prueba debe estar basado en un escenario pre-definido, objetivos, criterios de medición, procedimientos y una revisión exhaustiva de los resultados para realizar el mantenimiento respectivo que mejore la calidad del plan.

La prueba de los planes de continuidad sirve para determinar:

- ✓ Si la organización está lista.
- ✓ La habilidad de enfrentar una interrupción o desastre.
- ✓ Si la información respaldada y la documentación guardada en off-site son adecuados.
- ✓ Si los inventarios, tareas y procedimientos son adecuados para soportar el reinicio y la recuperación de las operaciones.
- ✓ Si los planes han sido mantenidos en el tiempo y actualizados de modo que reflejen las necesidades actuales.

3.1.14.1.1. Clasificación de las pruebas

Las pruebas se pueden clasificar por el momento en que se practican, por ser anunciadas o no anunciadas y por el tipo y alcance.

- ✓ Dos momentos de pruebas:
  - ✓ Pruebas iniciales del Plan de continuidad de negocio
  - ✓ Pruebas periódicas específicas de los componentes técnicos del plan y un posterior análisis de los resultados.
- ✓ Anunciadas o no anunciadas:
  - ✓ **Anunciadas** – sirven de introducción al proceso de pruebas y establece valores de ventanas de tiempos y performance que luego servirán para comparar. Son programadas por el equipo administrativo de continuidad de negocios y el coordinador de continuidad se encarga de revisar los planes con los participantes y de resolver algún problema encontrado en el plan de pruebas antes de ejecutarlo.
  - ✓ **No anunciadas** – sirven para determinar el nivel de preparación de la organización. Son programadas por el

equipo administrativo de continuidad de negocios, pero en este caso el coordinador no avisa a los participantes.

- ✓ Tipos y alcance, las que deben ejecutarse de manera secuencial y dentro de un año:

  - ✓ **Prueba de la respuesta a emergencias** – simula los pasos que se deben tomar inmediatamente después de un incidente que amenace la vida de los empleados o los activos de la empresa.
  - ✓ **Prueba paso a paso estructural** – se pre-define un escenario en el cual los equipos se desenvuelven ejecutando cada una de sus tareas. En este juego de roles por lo menos deben participar los líderes y sus backups.
  - ✓ **Prueba táctica simulada** – de un proceso o área funcional. Participan todos los miembros de la organización. El ambiente de desastre se simula tan real como sea posible, pero con los tiempos reducidos para lograr todas las actividades de 2 o 3 días en un solo día de trabajo.
  - ✓ **Prueba operacional** – múltiples procesos o áreas funcionales interrelacionadas. Similar al anterior, pero su alcance es mayor. Participan todos los equipos y afecta a todos los procesos de negocio e infraestructura

tecnológica. Los recursos que no estén disponibles localmente o pre-ubicados en el sitio alterno deberán ser tomados de las instalaciones del dispositivo de almacenamiento fuera del sitio o provistos por los proveedores. Debe ejecutarse antes de la prueba en producción.

- ✓ **Prueba en producción** – de uno o más procesos del negocio incluyendo la tecnología que los soporta. Sirve para validar las actividades de las organizaciones interrelacionadas, la utilidad de instalaciones de operación alternas y el servicio de soporte en aquellas ubicaciones. Debe tener cuidado de que la prueba no sea la causa de un desastre. Requiere la aprobación de la gerencia.

3.1.14.1.2. Escenarios de prueba

Sirven para enfrentar situaciones para las que la organización se ha preparado, está lista para responder y reaccionar a diferentes tipos de interrupciones.

Ejemplos de escenarios:

- ✓ Pérdida de toda una instalación – centro de datos.
- ✓ Pérdida de acceso a las áreas de producción.

- ✓ Pérdida de los equipos de producción.
- ✓ Desastre naturales o causados por el hombre.

3.1.14.1.3. Objetivos de la prueba

Los objetivos de una prueba deben incluir la evaluación y practica de las tareas del plan de continuidad.

Ejemplos:

- ✓ Volver a probar las partes del plan en las que se encontró alguna deficiencia en la última prueba.
- ✓ Probar con prioridad los sistemas, aplicaciones, procesos y operaciones sensibles al tiempo de recuperación que no hayan sido probados últimamente.
- ✓ Involucrar a los equipos de soporte que necesiten más entrenamiento para que mantengan familiaridad con sus tareas.
- ✓ Asegurarse de que las condiciones de prueba y los recursos están completamente definidos.

3.1.14.1.4. Procedimientos para la prueba

Debe existir relación entre los objetivos y los procedimientos. Algunos procedimientos sugeridos para cumplir con los objetivos son:

- ✓ Procedimiento de administración.
- ✓ Procedimiento de comunicaciones.
- ✓ Procedimiento de coordinación.
- ✓ Procedimiento de notificación.
- ✓ Procedimiento de operaciones.
- ✓ Procedimiento de organización.
- ✓ Procedimiento de asignación de personal.
- ✓ Procedimiento de asignación de recursos.
- ✓ Procedimiento de Recuperación.
- ✓ Procedimiento de reportes de estado.
- ✓ Procedimiento de situación de la continuidad.
- ✓ Procedimiento de seguridad.

3.1.14.1.5. Resultados de la prueba

Los líderes de los equipos deben documentar los resultados dentro de las 2 o 3 semanas después de terminada la prueba.

Los administradores de la continuidad del negocio revisarán los resultados y asignarán y coordinarán la corrección de los problemas encontrados. Luego se actualizará el plan para volver a ser revisado.

En algunos casos, se podría requerir volver a probar los resultados, esto se decidiría por un equipo que no haya participado de las pruebas, el cual puede ser interno o externo a la empresa.

Algunas consideraciones adicionales que se deben cumplir para optimizar el resultado del plan de pruebas son: Automatizar todo procedimiento de reanudación y recuperación, Identificar claramente los servicios y el soporte de los proveedores.

3.1.14.2. Aseguramiento de la calidad

Este componente es el más largo del plan, asegura la integridad de la información textual verificando que el contenido del plan es actualizado y mantenido en condiciones de uso aceptables.

Las tres formas de asegurar la calidad son: 1) Pruebas, 2) Entrenamiento y 3) Mantenimiento. Siempre se debe evaluar e implementar nuevas formas de obtener, actualizar y mantener información de los planes.

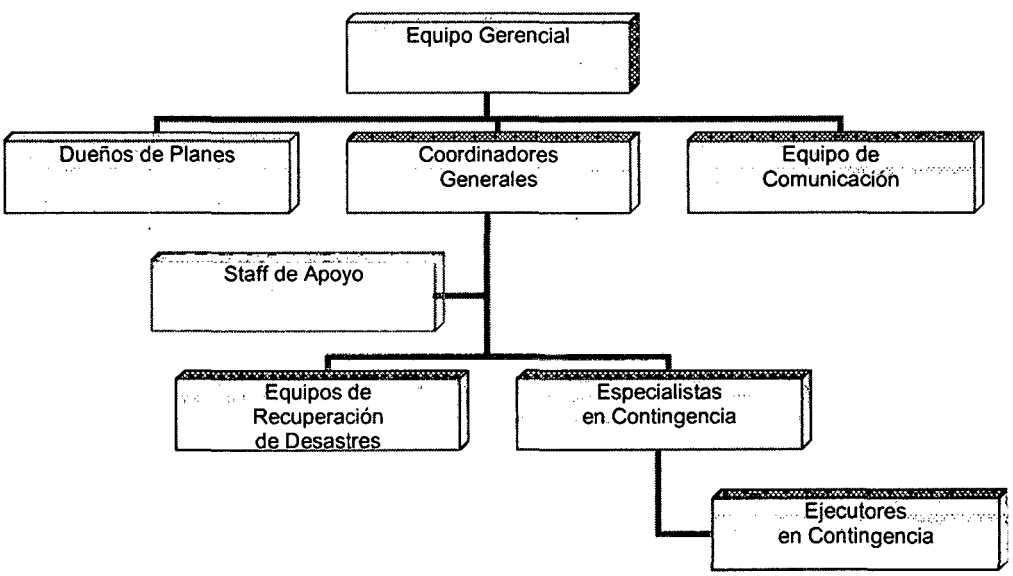
La responsabilidad recae en el jefe de departamento - propietario de cada plan, en los ejecutivos de División que son responsables por la calidad de todos los planes de la División, incluso la Alta Gerencia es responsable de la calidad de la capacidad de continuidad de la organización

3.1.15. Organización interna para la gestión de continuidad de negocio

3.1.15.1. Equipos

La administración de emergencias se debe adoptar como una disciplina formal. Esta visión, considera instaurar la Administración de la Continuidad de Negocios como disciplina corporativa, estableciendo un marco conceptual, uno normativo y uno organizacional que propulsen la asimilación de la disciplina y garanticen su vigencia en el tiempo.

Figura 25 Organización para Emergencias



Fuente: Informe Malcolm Baldridge

3.1.15.1.1. Equipo Gerencial de Continuidad de Negocios

Generalmente conformado por personal de Sistemas, Unidades de Negocios y Operaciones.

Su función es evaluar la situación de desastre e instruir al Equipo de Coordinadores Generales de los Planes el inicio de la "Situación de Contingencia", además de realizar el control de la recuperación del desastre. Igualmente, una vez superado el problema, declarará el final de la contingencia y retorno a operaciones normales.

- ✓ **Líder:** Gerente General Adjunto.
- ✓ **Líder Alterno:** Gerente de Banca de Servicio.
- ✓ **Miembros Permanentes:** Gerente de Sistemas y Organización, Gerente de Canales de Atención, Gerente de Procesos Centrales, Gerente de Producción de Sistemas.
- ✓ **Miembros Ad-Hoc:** Gerentes de las otras Bancas, Gerente de Mercado de Capitales.

3.1.15.1.2. Equipo de Coordinadores Generales de los Planes de Continuidad

Cada Área o División tiene un "Coordinador General" designado, responsable de:

- ✓ Mantener adecuadamente actualizados los Planes de Continuidad, Comunicación y sus anexos.

- ✓ Ejecutar adecuada y oportunamente el cronograma anual de pruebas para Continuidad de Negocios, definido por Administración de Riesgos.
- ✓ Efectuar recomendaciones de mejora a los planes en base a los resultados de las pruebas.
- ✓ Ejecutar, ante la eventualidad de un desastre, el Plan de Comunicaciones

3.1.15.1.3. Dueños de los Planes de Continuidad

Cada plan de Continuidad tiene un "Dueño" designado, que es el Gerente de la unidad o unidades responsables de ejecutar los planes. El "Dueño" será responsable de:

- ✓ Desarrollar Planes de Continuidad en su unidad, tanto para procesos críticos vigentes como para nuevos procesos críticos
- ✓ Asegurar el adecuado y oportuno mantenimiento de los Planes
- ✓ Asegurar la ejecución de pruebas periódicas
- ✓ Ante la eventualidad de un desastre:
  - ✓ Coordinar la ejecución del Plan de Recuperación de Desastres con el área correspondiente.
  - ✓ Coordinar la ejecución del Plan de Continuidad con los Equipos Ejecutores respectivos.
  - ✓ Proveer al Equipo de Coordinadores Generales, de información relevante respecto los Planes bajo su

responsabilidad, antes, durante y después del evento de desastre

3.1.15.1.4. Equipos ejecutores de Planes de Continuidad

El equipo para cada plan está conformado por las personas que son los usuarios responsables del proceso/transacción.

- ✓ Líder o Coordinador del Plan

Designado en el Plan de cada proceso crítico. Estará encargado de:

- ✓ Ejecutar el Plan de Recuperación de Desastres, en las funciones de su competencia.
- ✓ Ejecutar el Plan de Continuidad bajo su responsabilidad.
- ✓ Proveer al "Dueño" del Plan, de información relevante respecto al Plan antes, durante y después del evento de desastre.
- ✓ Proponer los ajustes pertinentes por cambios o mejoras, a los procedimientos del Plan de Continuidad y Recuperación de Desastres (Guía de Autonomías)

- ✓ Participantes

Personal operativo del Área (usuarios principales)

3.1.15.1.5. Equipos de Recuperación de Desastres

Encargados diseñar, mantener actualizados y ejecutar los planes de recuperación del recurso o recursos no disponibles o con fallas graves.

3.1.15.1.6. Equipo de Sistemas

Encargado de manejar la recuperación del desastre en los recursos tecnológicos, y coordinar las labores de recuperación de la carga de trabajo de las unidades involucradas.

- ✓ **Líder:** Gerente de Producción de Sistemas.
- ✓ **Participantes:** Equipos de Producción de Sistemas y Desarrollo de Sistemas

3.1.15.1.7. Equipos de Soporte

Encargados de apoyar en el manejo de la crisis, ejecución de la contingencia y recuperación, y la posterior evaluación de la contingencia

- ✓ Helpdesk

  Encargado de captar y distribuir información de manera masiva durante la contingencia.
- ✓ Marketing

  Encargado de la elaboración y asesoramiento en la difusión de comunicados para clientes y medios de comunicación.
- ✓ Procesos Administrativos y Financieros

  Encargado de gestionar la regularización de las diferencias en contingencia, generadas por retiros / cargos sin fondos / línea.

- ✓ Atención al Cliente

Encargado de procesar y analizar el impacto de la contingencia y proponer mejoras a los planes dentro del ámbito de la Calidad de Servicio al Cliente.

3.1.15.1.8. Equipo de Administración de Riesgos

Encargado de velar por la existencia y efectividad de los planes, diseñando la metodología de trabajo, programando pruebas, y analizando el resultado de las mismas. Asimismo, es responsable de coordinar y asesorar en la ejecución de los planes ante eventos catastróficos, realizando el análisis de impacto de los sucesos y proponiendo mejoras a los planes dentro del ámbito del Riesgo Operativo.

- ✓ **Líder:** Jefe de Administración de Riesgos de Operación
- ✓ **Participantes:** Funcionarios de Administración de Riesgos de Operación

3.1.15.1.9. Equipo de Auditoria

Encargado de auditar la existencia, el correcto mantenimiento, pruebas y ejecución de los Planes de Continuidad y Recuperación de Desastres

- ✓ **Líder:** Jefe del Servicio de Auditoría Operativa.
- ✓ **Participantes:** Funcionarios del Servicio de Auditoría Operativa

3.1.15.2. Tareas

En esta parte se definen las tareas o acciones a ser ejecutadas por el equipo. El desarrollo de las tareas para soportar los procesos de respuesta, reanudación, recuperación y restauración es el factor decisivo para saber si el plan contiene las acciones necesarias para responder a los incidentes y reanudar operaciones.

Los líderes de equipo que participarán activamente en la respuesta, reanudación, recuperación y restauración deben tener asignadas tareas de administración y coordinación, mientras que el líder alterno debe trabajar con el equipo para facilitar la finalización de las tareas. Las tareas que se asignen a un equipo deben ser consistentes con la experiencia y habilidad del empleado asignado en tal posición.

Las tareas deben ser desarrolladas de manera granular, y deben ser practicadas hasta que se vuelvan familiares.

3.1.15.3. Responsabilidades

Generalmente las responsabilidades son incluidas en la parte Introducción del Plan de Continuidad, suele ingresarse el nombre del puesto asignado y no el nombre de la persona y se listan las funciones describiendo la responsabilidad. En esta parte no se detallan las tareas y actividades específicas de la responsabilidad asignada.

Las funciones de los participantes en la estructura orgánica de la Administración de la Continuidad de Negocios, se agrupan de la siguiente manera:

- ✓ Responsabilidades Permanentes (Mantenimiento)

  Velar por la existencia, efectividad y actualización de los planes para los procesos críticos de su competencia, ejecutando simulacros y sesiones de capacitación de manera periódica, con la finalidad de:

  - ✓ Mantener entrenados a los ejecutores en los procedimientos de contingencia y recuperación de desastres.
  - ✓ Probar la efectividad de los procedimientos.
- ✓ Responsabilidades durante un desastre (Ejecución)
  - ✓ Analizar la información disponible, y determinar la activación, desactivación, o modificación de los planes de Continuidad (Contingencia y Recuperación). Asegurando la adecuada ejecución de los procedimientos.
- ✓ Responsabilidades después de un desastre (Documentación)
  - ✓ Coordinar el retorno a operaciones regulares, preparando y consolidando los informes de sucesos en contingencia por unidad. Finalmente, analizando los reportes y aprobando o proponiendo mejoras a los planes existentes.

3.1.15.3.1. Responsabilidades permanentes de los equipos

- ✓ **Equipo Gerencial**
  - ✓ Conoce y comprende los criterios especificados para la toma de decisiones del Plan de Continuidad de Negocios y Recuperación de Desastres.
  - ✓ Participa de las pruebas anuales como ente activo en los procedimientos de la Continuidad de Negocios.
  - ✓ Supervisa periódicamente, mediante la ejecución de comités trimestrales, los siguientes puntos:
  - ✓ El mantenimiento / actualización permanente de los Planes de Continuidad, Comunicación y Recuperación de Desastres.
  - ✓ El cumplimiento adecuado del cronograma anual de pruebas de los Planes de Continuidad, Comunicación y Recuperación de Desastres.
  - ✓ Aprueba de manera Ad-Hoc, en los casos que así lo amerite, las modificaciones a los Planes de Continuidad, Comunicación y Recuperación de Desastres.

- ✓ **Equipo de Coordinadores Generales**
  - ✓ Asegura el adecuado mantenimiento de los Planes de Continuidad, Comunicación y sus anexos.

- ✓ Coordina el Plan anual de pruebas de los planes de Contingencia, Comunicación y sus anexos, con el Servicio de Administración de Riesgos de Operación.
- ✓ Evalúa la efectividad de los Planes y efectuar recomendaciones de mejora a los planes, en base a los resultados de las pruebas

✓ **Dueños de Planes de Continuidad**

- ✓ Asegura la existencia de Planes de Continuidad en su unidad, tanto para procesos críticos vigentes como para nuevos procesos críticos.
- ✓ Mantiene debidamente actualizados los Planes, formatos y manuales de Continuidad conforme se identifiquen cambios en los procesos operativos del Área y/o en los componentes que los soportan.
- ✓ Instruye la ejecución, y evalúa las pruebas, incluyendo las necesidades de capacitación y entrenamiento de los ejecutores de procesos en contingencia.

✓ **Equipo de Marketing**

- ✓ Elabora y actualiza los comunicados que serán difundidos a clientes y medios de comunicación. Esto será preparado con anticipación a una posible contingencia tecnológica.
- ✓ Establece el Plan de medios o canales de Difusión de comunicados:

- ✓ **Comunicación Interna**:
  - ✓ Campaña de Difusión
  - ✓ Vía correo electrónico interno: Campaña de difusión, notificación de inicio y fin de situación de contingencia.
  - ✓ Folletos de publicidad: Campaña de Difusión.
- ✓ **Comunicación Externa:**
  - ✓ Anuncio en principales Diarios: Campaña de difusión
  - ✓ Videos en Agencias: Campaña de difusión, notificación de inicio y fin de situación de contingencia.
  - ✓ Conferencias de Prensa ante principales Medios de Comunicación: Notificación de inicio y fin de contingencia.

- ✓ **Equipo Helpdesk**
  - ✓ Participa en la ejecución del Plan anual de pruebas de los Planes de Continuidad y Recuperación.

- ✓ **Equipo de Recuperación de Desastres**
  - ✓ Mantiene debidamente actualizados los Planes, formatos y manuales de Recuperación de Desastres conforme se identifiquen cambios en los procesos operativos del Área y/o en los componentes que los soportan.
  - ✓ Coordina el Plan anual de pruebas, de los planes de Recuperación de Desastres de su competencia, con el Servicio de Administración de Riesgos de Operación.

- ✓ Ejecuta y evalúa las pruebas de los Planes, incluyendo las necesidades de capacitación y entrenamiento.

- ✓ **Equipo de Administración de Riesgos**
  - ✓ Diseña y difunde la metodología para la elaboración de Planes de Continuidad.
  - ✓ Analiza y define, en coordinación con los Dueños de los planes, el alcance mínimo de estos: en términos de procesos críticos a ser incluidos y escenarios a ser analizados.
  - ✓ Colabora en la evaluación de la efectividad de los Planes de Continuidad y Recuperación de Desastres, aportando propuestas de mejora que podrían ayudar a mejorarlos dentro de su ámbito de responsabilidad
  - ✓ Supervisa el mantenimiento / actualización permanente de los Planes de Continuidad y Recuperación de Desastres
  - ✓ Diseña y gestiona el plan anual de pruebas, estableciendo el cronograma e indicadores de las pruebas
- ✓ **Equipo de Auditoria**
  - ✓ Verifica la existencia y vigencia de los Planes de Continuidad y Recuperación de Desastres para procesos críticos. En este sentido Auditoria enfocará sus esfuerzos en los planes vigentes en el sistema normativo del

Banco, pudiendo eventualmente recomendar la creación de nuevos planes.

3.1.15.3.2. Responsabilidades durante el período de operación en contingencia

- ✓ **Equipo Gerencial**
  - ✓ Recibe el aviso de alerta del Líder del Equipo de Recuperación de Desastres, y sigue los procedimientos descritos en la cartilla de instrucciones en contingencia para el EGC.
  - ✓ Recibe y analiza permanentemente la información sobre la situación de desastre proporcionada por el Líder del Equipo de Recuperación de Desastres
  - ✓ Declara la Contingencia y el inicio de los Planes de Continuidad para la Unidad o Unidades que presentan la falla, utilizando para ello el Plan de Comunicaciones.
  - ✓ Requiere y analiza permanentemente información del desenvolvimiento de los Planes en las distintas Unidades, proporcionada por los Coordinadores Generales de los Planes. Realizando ajustes / cambios a los Planes de Continuidad de ser necesario (Guía de Autonomías).

- ✓ Declara el fin de la contingencia a la Unidad o Unidades en contingencia, utilizando para ello el Plan de Comunicaciones.
- ✓ Mantiene informada a la Alta Gerencia (Comité de Gestión) sobre la situación de desastre.

✓ **Equipo de Coordinadores Generales**

- ✓ Recibe el aviso de alerta de Helpdesk, y sigue los procedimientos descritos en la cartilla de instrucciones en contingencia para los Coordinadores Generales
- ✓ Instruye comunicación masiva reforzando la activación del nivel básico de atención, utilizando para ello el Plan de Comunicaciones
- ✓ Recibe y ejecutan las instrucciones de comunicación masiva de los miembros del EGC, utilizando para ello el Plan de Comunicaciones.
- ✓ Hace seguimiento a la Continuidad de Negocios, coordinando con los "Dueños" de planes la correcta ejecución de los mismos y los ajustes que estos pudiesen requerir.
- ✓ Hace seguimiento a la Recuperación de Desastres, coordinando con los Equipos de Recuperación de Desastres las acciones correspondientes.
- ✓ Obtiene, consolida y reporta periódicamente información relevante sobre la Continuidad de Negocios y

Recuperación de Desastres, requerida por el Equipo Gerencial para el análisis de la situación.

- ✓ Absuelve y resuelve, en segundo nivel, las dudas y/o problemas operativos que se puedan presentar en los Equipos Ejecutores, de acuerdo a lo normado en el Plan de Comunicaciones.
- ✓ Asesora al Equipo Gerencial en la toma de decisiones respecto a los Planes de Recuperación de Desastres y Continuidad de Negocios

✓ **Dueños de Planes de Continuidad**

- ✓ Recibe el aviso de alerta de su Coordinador General, y sigue los procedimientos descritos en la cartilla de instrucciones en contingencia para los Dueños de Planes.
- ✓ Verifica que los procesos se conduzcan conforme a lo previsto en los planes desarrollados y absuelven las dudas y/o problemas operativos que se puedan presentar en los Equipos Ejecutores
- ✓ Coordina los incidentes relevantes con el Equipo de Coordinadores Generales para el análisis de la situación

- ✓ **Equipos Ejecutores de Planes**

  - ✓ Recibe el aviso de alerta de Helpdesk, y sigue los procedimientos descritos en sus respectivos Planes de Continuidad y Recuperación de Desastres
  - ✓ Sigue la operativa descrita en el Plan de Continuidad y Recuperación de Desastres, reportando directamente al "Dueño" del Plan ó a su respectivo Coordinador General.

- ✓ **Equipo de Marketing**

  - ✓ Asesora a los ejecutivos del banco para las comunicaciones externas que sean necesarias, según lo normado en el Plan de Comunicaciones

- ✓ **Equipo Helpdesk**

  - ✓ Detecta y analiza la falla en primer nivel, siguiendo los procedimientos descritos en la cartilla de instrucciones en contingencia para Helpdesk
  - ✓ Da inicio al Plan de Comunicaciones de ser necesario
  - ✓ Atiende la línea de consulta de contingencia, dando información actualizada a los usuarios sobre el estado de la contingencia y absolviendo las dudas operativas que se puedan presentar en los Equipos Ejecutores, de acuerdo a lo normado en el Plan de Comunicaciones.

- ✓ **Equipo de Recuperación de Desastres**
  - ✓ Ejecuta, en coordinación con las unidades involucradas, las actividades del Plan de Recuperación de Desastres para la recuperación del servicio en el menor plazo posible.
  - ✓ Mantiene informado a Helpdesk y el Equipo Gerencial sobre el estado de la recuperación del desastre, de acuerdo al Plan de Comunicaciones.

3.1.15.3.3. Responsabilidades durante el período de operación en Normalización

- ✓ **Equipo Gerencial de Continuidad**
  - ✓ Instruye el inicio de las actividades de normalización, de acuerdo al Plan de Comunicaciones.
  - ✓ Recibe y analiza la información proporcionada por Administración de Riesgos, respecto del impacto financiero y de imagen, ocasionado por la contingencia y aplicación de los Planes de Continuidad y Recuperación de Desastres.
  - ✓ Vela por la actualización de los Planes en caso de haber surgido modificaciones y/o sugerencias de mejoras durante la situación de Contingencia y/o Recuperación de Desastres.

- ✓ **Equipo de Coordinadores Generales**
  - ✓ Recibe y ejecuta la instrucción de comunicación masiva de los miembros del Equipo Gerencial de Continuidad para el inicio de la normalización, utilizando para ello el Plan de Comunicaciones.
  - ✓ Coordina con las demás unidades y el Equipo de Recuperación de Desastres la ejecución de los Planes de Normalización de la carga de trabajo acumulada.
  - ✓ Consolida la información de los Dueños y Equipos Ejecutores respecto a la efectividad de los Planes de Continuidad y Recuperación de Desastres aplicados.

- ✓ **Dueños de Planes de Continuidad**
  - ✓ Asegura la adecuada ejecución de los Planes de Normalización de la carga de trabajo acumulada.
  - ✓ Evalúa y reporta a Administración de Riesgos y al Equipo Gerencial el impacto financiero y de imagen, ocasionado por la contingencia y la aplicación de los Planes de Continuidad y Recuperación de Desastres.
  - ✓ Evalúa la efectividad de los Planes de Continuidad y Recuperación de Desastres aplicados, en coordinación con el Equipo de Coordinadores Generales.
  - ✓ Propone y realiza los ajustes que se identifiquen como necesarios informando al Equipo Gerencial, en coordinación con el Equipo de Coordinadores Generales.

- ✓ **Equipos Ejecutores de Planes**
  - ✓ Ejecuta los Planes de Normalización de la carga de trabajo.
  - ✓ Verifica la correcta ejecución de las rutinas Batch para los procesos críticos de su responsabilidad, realizando los ajustes necesarios para no perjudicar a los clientes.
  - ✓ Colabora en la evaluación de la efectividad de los Planes de Continuidad y Recuperación de Desastres aplicados.

- ✓ **Equipo de Recuperación de Desastres - Sistemas**
  - ✓ Ejecuta el Plan de Normalización de la carga de trabajo en sistemas.
  - ✓ Coordina con los Equipos Ejecutores, el Plan de Normalización de la carga de trabajo acumulada.
  - ✓ Realiza las recomendaciones pertinentes para la optimización de los Planes de Continuidad y Recuperación de Desastres ejecutados.

- ✓ **Equipo de Marketing**
  - ✓ Evalúa el desempeño de la imagen institucional en los medios de comunicación y difusión durante la contingencia.

- ✓ Realiza recomendaciones al Equipo de Coordinadores Generales para mejorar el Plan de Comunicación de manera que sea más efectivo.

- ✓ **Equipo Helpdesk**
  - ✓ Guía a los usuarios en las actividades de retorno.

- ✓ **Equipo de Administración de Riesgos**
  - ✓ Prepara el informe de impacto de la contingencia, consolidando la información del Plan de Cobranzas, atención de reclamos y los informes de los Coordinadores Generales
  - ✓ Consolida las recomendaciones de mejora a los procedimientos de Continuidad y Recuperación de Desastres.
  - ✓ Evalúa la efectividad de los Planes de Continuidad y Recuperación de Desastres aplicados, y sugiere tareas correctivas que podrían ayudar a mejorarlos dentro de su ámbito de responsabilidad.

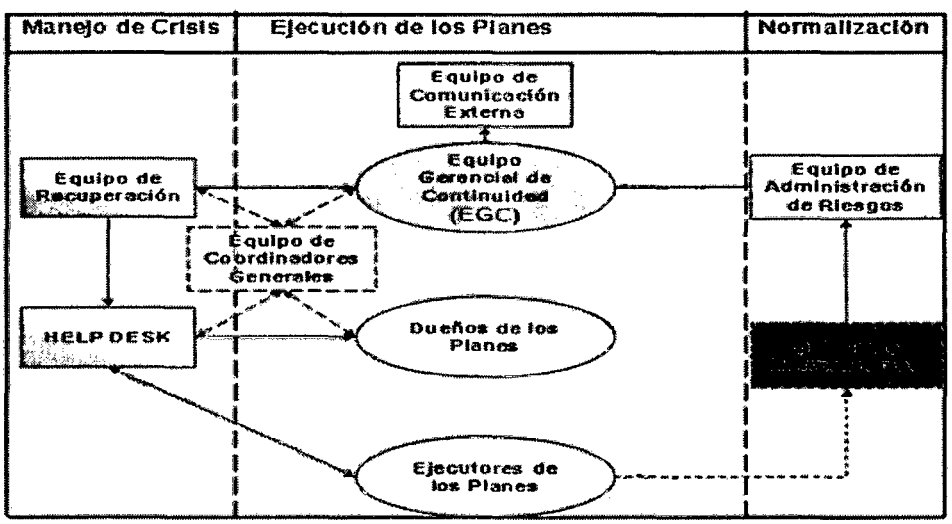
En la siguiente tabla y esquema, se ilustran las responsabilidades de los equipos definidos en el plan de continuidad y el flujo de comunicación entre estos equipos dentro de la organización.

Tabla 8 Responsabilidades y flujo de comunicación entre equipos

Manejo de crisis	Ejecución de los planes	Normalización
Equipo de recuperación	**Equipo de coordinadores generales**	**Equipo de administración de riesgos**
Ejecuta el plan de recuperación de desastres	Seguimiento a la recuperación y continuidad Asesoría en el manejo de los planes	Evalua e informa el impacto de la contingencia
HelpDesk	**Equipo gerencial de continuidad**	**Unidades de normalización**
Detecta y comunca eventos de desastre. Informa la situación del problema.	Declaración de contingencia Modificación de los planes	Reporta eventos ocurridos durante y despues de la contingencia.
	Dueño de los planes	
	Comunica eventos durante la contingencia	
	Ejecutores de los planes	
	Ejecuta planes de continuidad	

Fuente: Administración de Riesgos

Figura 26 Responsabilidades durante el período de operación en contingencia



Fuente: Administración de riesgos

3.1.16. Plan de Implementación

Si se requiere operar el sistema desde un centro alterno de recuperación, se deben seguir los siguientes pasos:

- ✓ La selección del centro de recuperación alterno dependerá del escenario de recuperación.
- ✓ Las instalaciones del centro alterno deben contar con la infraestructura (espacio físico, equipos, comunicaciones) y el soporte necesarios para la recuperación de un desastre.
- ✓ Se deben identificar los mecanismos de soporte y verificar que estos estarán disponibles para ser utilizados cuando se necesiten.

3.1.16.1. Quién desarrolla e implementa el plan?

El plan debe ser desarrollado e implementado por los dueños del negocio. Es recomendable contratar los servicios de una consultoría para asegurar que se cumplen con las mejores prácticas internacionales y que se cubren todos los puntos importantes de un plan de continuidad. Además de ser un tercer actor que brinda mayor confiabilidad a la gerencia al avalar el plan.

3.1.16.2. Criterios de evaluación de una consultoría

Para contratar los servicios de una consultoría que sirva de apoyo en el desarrollo del plan de continuidad, se deben considerar ciertos criterios de evaluación mínimos:

Tabla 9 Criterios de evaluación de consultoría para el desarrollo e implementación de un Plan de Continuidad de Negocios

CRITERIOS DE EVALUACION	PESOS
DEL POSTOR	**50**
1 Experiencia del postor	5
2 Experiencia de los consultores principales	30
3 % de involucramiento	15
DEL SERVICIO	**20**
4 Metodologia	5
5 Valor agregado	10
6 Plan de trabajo	3
ALCANCES	**30**
7 BIA Negocios	4
8 BIA TI	6
9 Planes de Recuperación	6
10 Planes de Prueba y Capacitación	6
11 Control de Cambios	8
PUNTAJE TOTAL	**100**

Fuente: Ejemplo - Proyecto DRP

El postor es el proveedor que brinda el servicio de consultoría para el desarrollo del plan de continuidad operativa del negocio.

Para la evaluación del postor se pueden considerar 3 aspectos:

- ✓ Criterios de evaluación del postor
- ✓ Criterios de evaluación del servicio
- ✓ Criterios de evaluación según el alcance definido

3.1.16.2.1. Criterios de evaluación del postor

Experiencia del postor, en el que se evalúa su experiencia en la práctica del Business Continuity Management (Administración de la continuidad de negocios), en base a los proyectos y referencias que presenten. Se debe tomar en cuenta si los consultores participantes estarán localmente y directamente relacionados en el desarrollo del plan, y si el postor que se presenta a la evaluación es la empresa invitada o es una empresa en representación.

Experiencia de los consultores principales, en el que se evalúa la experiencia de los consultores que se presentan, experiencia basada únicamente en la práctica del Business Continuity Management.

% de involucramiento, en el que se evalúa la participación directa, local de los consultores principales, tomando en cuenta el % de participación efectiva (presencial) durante el desarrollo e implementación del plan.

3.1.16.2.2. Criterios de evaluación del servicio

Metodología, en el que se evalúa la metodología utilizada por el postor, comparándola contra las mejores prácticas.

Valor agregado, en el que se evalúa el nivel de entregables propuestos por el postor que agregan un valor significativo al plan de continuidad operativa en general.

Plan de trabajo, en el que se evalúan los tiempos propuestos versus el cronograma para el desarrollo e implementación del plan, de modo que se adecuen a los plazos que el Banco haya considerado.

3.1.16.2.3. Criterios de evaluación del alcance

En cuanto a los criterios de evaluación del alcance, este dependerá de los puntos solicitados por el Banco para el desarrollo e implementación del plan de continuidad operativa. El postor debe cumplir como mínimo los puntos requeridos.

Para calificar a los postores, se podría utilizar tres valores para los puntajes:

- ✓ 1 = BAJO
- ✓ 2 = MEDIO
- ✓ 3 = ALTO

Por ejemplo, una calificación de postores podría verse de esta forma:

Tabla 10 Calificación para la evaluación de postores para la consultoría

POSTORES					
Postor 1		Postor 2		Postor 3	
Puntaje	Total	Puntaje	Total	Puntaje	Total
3	15	3	15	3	15
3	90	2	60	2	60
3	45	2	30	2	30
3	15	3	15	3	15
2	20	2	20	2	20
2	6	2	6	2	6
3	12	3	12	3	12
3	18	3	18	3	18
3	18	3	18	3	18
3	18	3	18	3	18
3	24	3	24	3	24
PUNTAJE TOTAL					
95.58		80.27		80.27	

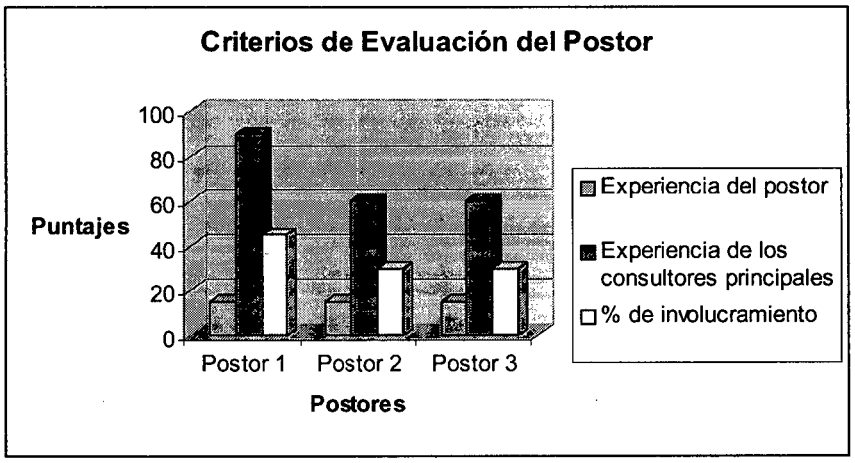
Fuente: Ejemplo - Proyecto DRP

En el que se observa que el Postor 1 es el proveedor que ofrece un mejor servicio en general.

3.1.16.3. Estructura de la propuesta del servicio de consultoría

La propuesta del servicio de consultoría debe contener el detalle de lo que el proveedor ofrece y además debe ser modular de manera que el Banco pueda decidir qué servicios tomar de los que son ofrecidos, o que pueda negociar alguno de los servicios retirando o agregando entregables.

Figura 27 Resultados de los criterios de evaluación del Postor



Fuente: Ejemplo - Proyecto DRP

3.1.17. Plan de mantenimiento

El propósito de esta sección es definir el esquema de actualización del Plan de Continuidad del Banco. El mantenimiento del Plan es de suma importancia ya que permite asegurar la exactitud de la información a recuperar y de los procedimientos que gobiernan esta recuperación; por

tal motivo se debe mantener actualizados el plan de prueba y el plan de implementación y además sincronizados con los cambios en el negocio. Todos los cambios en el negocio deben ser considerados para ser incluidos en el Plan de Continuidad. Los cambios relacionados con los Sistemas de Información son integrados en el plan a través del proceso de administración de cambios y problemas, y los cambios en el negocio a través de una revisión periódica.

Los cambios pueden ser:

- ✓ Cambios en la Organización. Cambios en la conformación de los equipos de trabajo definidos en el Plan, y en la estructura organizacional de la institución que afecten la vigencia de la información y las responsabilidades asociadas a los roles establecidos en los diferentes equipos de trabajo.

- ✓ Cambios en los Procedimientos de Recuperación. Cambios y/o modificaciones ocurridas en los procedimientos y flujos de recuperación.

- ✓ Cambios en las Aplicaciones Críticas. La vigencia de las aplicaciones críticas son consideradas como base para el Plan de Continuidad, las modificaciones que pudieran haber sufrido en el transcurso del tiempo deben verse reflejadas en el Plan de Continuidad.

No realizar un mantenimiento apropiado al plan queda demostrado en al número de problemas encontrados durante las pruebas. Es importante que los administradores funcionales que se encargan de firmar

los mantenimientos, vean las actualizaciones, cambios o revisiones para que puedan determinar si el plan podrá aprobar la prueba o incluso si podrá aprobar un verdadero desastre.

3.1.17.1. Administración de Cambios y Problemas

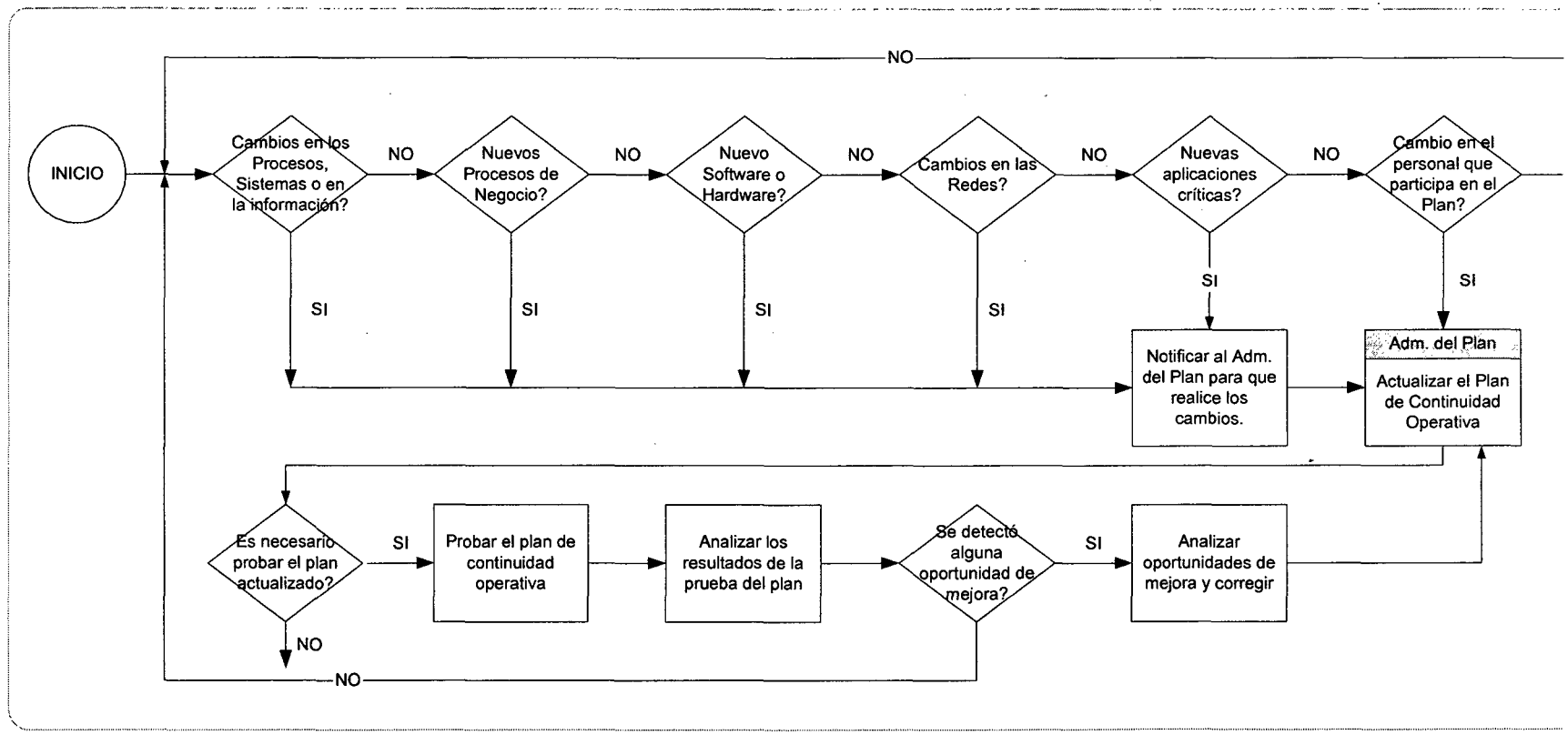
El Plan puede requerir actualización si se producen cambios o problemas en cualquiera de las siguientes situaciones:

- ✓ Resultados de una prueba del Plan Contingencia.
- ✓ Nuevas aplicaciones críticas.
- ✓ Aumento de la complejidad de las aplicaciones
- ✓ Compra de equipamiento nuevo.
- ✓ Cambios en el Hardware, Software, Redes de Telecomunicaciones, Sistemas Distribuidos, Aplicaciones, Datos, Personal, Formularios o suministros críticos.

El proceso de administración de cambios debe ser eficiente, todo cambio debe quedar documentado para poder proceder a la correcta actualización del plan si fuese necesario.

En el siguiente diagrama de flujo se pueden apreciar los procesos para el control de cambios en el plan de continuidad.

Figura 28 Flujo de procesos para la administración de un cambio en el plan de continuidad



Elaboración propia.

3.1.17.2. Tipos y alcance del mantenimiento

El mantenimiento típicamente está dividido según su alcance en "Programado", "No programado" y "Después de una prueba". Estos deben completarse en el curso de un año y repetirse anualmente para cumplir con las políticas establecidas y las pruebas programadas.

Algunas consideraciones para administrar el plan de mantenimiento:

- ✓ El número de planes escritos por la organización
- ✓ La frecuencia de os cambios organizacionales
- ✓ Frecuencia y tipo de pruebas programadas y ejecutadas
- ✓ Frecuencia de BIAs
- ✓ Tipo y alcance de los cambios de tecnología
- ✓ Impacto bajo operación normal versus esperado
- ✓ Disponibilidad de recursos

3.1.17.3. Disparadores de actualización

- ✓ Cambios en el personal clave.
- ✓ Cambios en el organigrama (Ej. Creación de nuevas posiciones)

- ✓ Cambios de dirección / teléfono de algún componente del equipo de recuperación.
- ✓ Cambios en cualquier equipo o dispositivo informático incluido dentro del esquema de recuperación.
- ✓ Cambio en algún procedimiento.
- ✓ Reubicación de instalaciones.
- ✓ Nuevos proveedores para los recursos críticos.
- ✓ Cambios en la configuración de los sistemas o los dispositivos de almacenamiento (Storage).
- ✓ Cambios en la configuración de comunicaciones o de las redes.

3.1.18. Herramienta para administrar el Plan de Continuidad de negocios

El documento del plan de continuidad debe cambiar al mismo tiempo en que cambia la organización, la vida de un plan puede ser mejor soportado si está almacenado en una base de datos relacional utilizando software diseñado específicamente para su administración.

Esta herramienta o software debe contar con:

- ✓ Flexibilidad para personalizar las vistas y reportes.
- ✓ Permitir la integración de múltiples planes.
- ✓ Administración por fases.
- ✓ Mantenimiento del plan y su activación.

La herramienta debe incluir plantillas que sirvan de ejemplo para empezar a desarrollar los planes inmediatamente. Las plantillas deben tener formatos y una guía que ayude a crear el plan directamente.

Debe permitir la importación de documentos que ya existían en la organización que hayan sido generados con otras herramientas.

La herramienta debe ser configurable, de manera que se pueda personalizar la terminología, el tamaño de los campos, etc. También debe contar con un módulo de seguridad que permita dar acceso al plan sólo a las personas autorizadas.

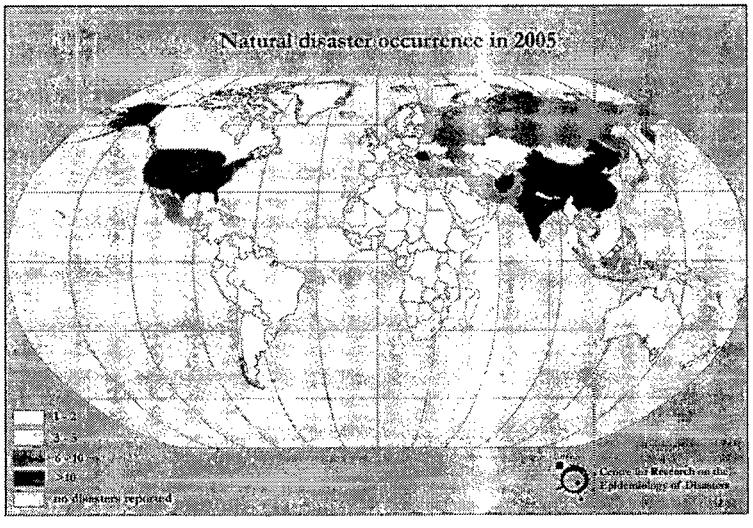
Una herramienta, para el desarrollo del plan de continuidad de negocios, ahorrará mucho tiempo y costos a la organización.

8.1. Descubrimiento de la Realidad

4.1.1. Riesgos que enfrenta el mundo

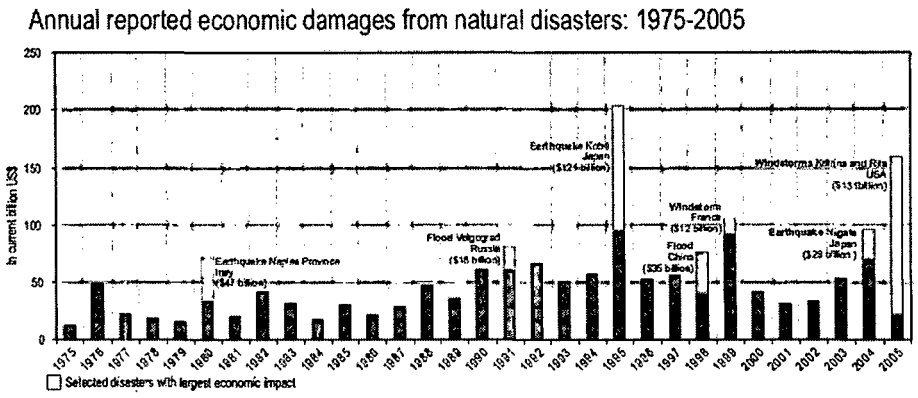
En la siguiente figura se muestra el número de desastres naturales ocurridos en el mundo en el año 2005, en este caso los desastres están clasificados de menor a mayor ocurrencia.

Figura 29 Número de desastres naturales en el mundo en el 2005



Pérdidas económicas a causa de los desastres:

Figura 30 Pérdidas económicas en el mundo



Muchas han sido las lecciones aprendidas a raíz de los primeros atentados con bomba en el World Trade Center y desastres naturales como el huracán Hugo. El factor clave fue sin embargo partir del hecho de que tales circunstancias se podían dar en algún momento y que por tanto debía planificarse de antemano el modo de actuar.

A lo largo de los últimos años las empresas de EEUU han sufrido desastres naturales y provocados por la mano del hombre, bien conocidos por todos, causando pérdidas que suman billones de dólares. Hace años el sur de California sufrió un gran terremoto, con repeticiones que sacudieron repetidamente sus valles. Donde la naturaleza se queda corta, el hombre llena el vacío. Los ataques terroristas con bomba del World Trade Center, resultaron en pérdidas de vidas humanas y daños valorados en cientos de millones de dólares. Las inundaciones en el medio oeste tuvieron un efecto igualmente devastador. Cuatro años antes

el Huracán Andrew asoló el Sur de Florida y partes del Sur de Louisiana, un terremoto causo grandes destrozos en la Bahía de San Francisco, luego fueron el Huracán Hugo en Charleston, Carolina del Sur, devastando sus alrededores.

¿Cuál es el grado de preparación de las empresas para estos desastres? La planificación de contingencias ante desastres en general y la planificación de contingencias informáticas en particular han sido puestas a prueba. Los desastres han demostrado que la capacidad de recuperarse ante ellos es crucial para la supervivencia de una empresa.

Deloitte & Touche, por ejemplo, fue capaz de trasladar todas sus operaciones desde el World Trade Center a otro centro de oficinas alternativo en la ciudad de Nueva York el mismo fin de semana tras el atentado con bomba. Lo que ha quedado muy claro es que las empresas deben implantar Planes de Contingencia ante Desastres (DRP) a todos los niveles de la empresa y que trasciende de los aspectos de procesamiento de datos propiamente dichos. La Dirección General debe comprender los principales riesgos para la empresa y las posibles consecuencias de un desastre. Un DRP adecuado identifica las necesidades de todos los departamentos e involucra personal de todas las áreas de la compañía. La responsabilidad para la obtención de un DRP no es únicamente de la Dirección Informática.

Quizás el desastre del World Trade Center, como ningún otro, evidenció de forma clara la necesidad de disponer de un DRP más allá de los sistemas informáticos. La cuestión no era únicamente mantener los sistemas en operación, sino cómo comunicarse con el cliente, los empleados y otros que interactúan con una empresa que de repente carece de los medios para ello, o incluso de las propias instalaciones donde se ubica. ¿Desde dónde se realizarán las transacciones el siguiente día laborable? ¿Cuál será la fuente de Cash Flow para el alquiler de instalaciones temporales, ordenadores y equipamiento de telefonía? Muchos negocios des-localizados han utilizado la telefonía móvil, que permite la comunicación sin cableado físico.

4.1.1.1. Desastres naturales en el mundo

4.1.1.1.1. Huracán Hugo - Charleston y Carolina del Sur

Después del Huracán Hugo, se realizó un estudio a 71 compañías del área de Charleston y Carolina del Sur. Todas las compañías del estudio habían declarado un volumen de ventas superior al millón de dólares. Las empresas fueron seleccionadas sobre un listado de Dun and Bradstreet.

Cada empresa recibió un cuestionario relativo a su plan de contingencia informático y factores relacionados, incluyendo su capacidad para procesar información crítica del sistema de gestión después de Hugo. Un total de 41 cuestionarios utilizables fueron remitidos y

posteriormente analizados. Dicho análisis reveló que 18 (44%) de las empresas disponía de un plan de contingencia informática antes del desastre, mientras que 23 empresas (56%) no disponían de él.

El estudio de las empresas del área de Charleston, no incidía sobre todos los aspectos de un DRP sino que lo hacía específicamente sobre los aspectos informáticos. El DRP informático es uno de los componentes más críticos del DRP y es especialmente relevante para los auditores externos. Las 23 empresas sin planes de contingencia informáticos tuvieron que enfrentarse a un sin fin de problemas tras el Huracán.

Parada informática. Todas las empresas sin el DRP informático, informaron sobre la parada de sus sistemas como resultado del huracán Hugo. Veinte empresas informaron sobre tiempos de parada entre 1 y 15 días, dos empresas estuvieron paradas de 16 a 60 días y una afirmó tener sus sistemas parados durante 2 a 4 meses.

Con los sistemas inoperantes y sin plan de contingencia para recuperar rápidamente las actividades normales de procesamiento de datos, las empresas tuvieron que enfrentarse al problema de cómo recuperar la información crítica de gestión.

Capacidad para procesar información contable. Las 23 empresas sin plan de contingencia tuvieron varios problemas asociados con el tiempo de parada. Muchas empresas fueron incapaces de procesar información

crítica de contabilidad mientras tenían los sistemas parados. Sólo 5 empresas fueron capaces de procesar toda su información contable. 4 empresas fueron capaces de procesar parte de la información y 14 de ellas no pudieron procesar nada.

Tabla 11 Tiempos de parada por el Huracán Hugo:

Tiempo de Parada	Número	Porcentaje
1-15 días	20	87%
16-60 días	2	9%
2-4 meses	1	4%
Total	23	100%

Tabla 12 Capacidad de Proceso de Datos tras el Huracán Hugo:

Datos Procesados	Número	Porcentaje
Todos los datos	5	22%
Algunos datos	4	17%
Ningún dato	14	61%
Total	23	100%

4.1.1.1.2. Desastres provocados por el hombre en el mundo

4.1.1.1.2.1. Las Torres, atentado 1

Durante el atentado con bomba en el aparcamiento del World Trade Center de Nueva York hace una década, las pérdidas materiales fueron escasas, hubo grandes destrozos en los sótanos del edificio pero las plantas superiores quedaron intactas. No obstante se dieron dos circunstancias que representaron la banca rota y el cierre definitivo de decenas de compañías; la primera: se trataba de una atentado terrorista; la segunda: las características de los edificios, edificios de alto riesgo (rascacielos) que debían ser desalojados e inspeccionados por los servicios de seguridad, mientras duraran las investigaciones. El resultado fue, que durante un periodo que osciló entre uno y dos meses aproximadamente, numerosos centros de procesamiento de datos con la más moderna tecnología quedaron totalmente aislados, sin posibilidad de que nadie pudiera entrar en ellos. El motivo fue que las torres fueron "selladas" durante ese periodo para facilitar las tareas de desescombro, los trabajos de investigación y poder garantizar los umbrales mínimos de seguridad para los miles de ocupantes en ambas torres.

El restablecimiento de la seguridad, fue el causante de que numerosas empresas no tuvieran acceso a su mayor activo "perfectamente preservado": la información. Como consecuencia muchas

de las empresas que no disponían de los datos fuera de los límites físicos del edificio, no tuvieron acceso a la información básica para gestionar la tesorería, atender a los clientes, etc. En los casos donde no existía el DRP o éste no incluían la hipótesis de "pérdida de acceso", significó la desaparición de la compañía.

4.1.1.1.2.2. Las Torres, atentado 2

Años más tarde durante los atentados del 11 de setiembre, en las mismas torres los DRPs eran una realidad, los daños materiales fueron asombrosos, sin embargo resaltó la supervivencia de aquellos que disponían de un Plan de Contingencia frente a los que no habían hecho nada al respecto, los primeros y tras un breve lapso de tiempo, (desde horas a unos pocos días) estaban dando servicio desde los respectivos centros de respaldo alternativos.

Algunos datos que ilustran la magnitud del desastre:

- ✓ 14,600 empresas en el World Trade Center y alrededores fueron afectados.
- ✓ 13.4 millones de pies cuadrados de espacio en seis edificios fueron destruidos.
- ✓ 36 millas de nuevo cableado tuvo que ser instalado por Consolidated Edison.
- ✓ 652 compañías ocupando 28.6 millones de pies cuadrados fueron permanentemente desplazados por la destrucción.

- ✓ 200,000 líneas de comunicación Verizon fueron afectadas por fallos en la red.
- ✓ 12,000 clientes de Consolidated Edison perdieron el suministro eléctrico.

4.1.1.1.2.3. Dos bancos, dos resultados

Un gran banco internacional localizado en el séptimo piso de la Torre Norte del World Trade Center quedó reducido a un montón de escombros humeantes el 11 de septiembre. Los altos ejecutivos y otros empleados anduvieron atolondrados por haber perdido compañeros, amigos y parejas. Pero cuando se recuperaron de su trauma, los supervivientes trabajaron juntos para asegurar que las necesidades de los clientes del banco se cumplían. Aunque los 85 servidores del banco, incluyendo doce que proporcionaban aplicaciones críticas para importantes transacciones financieras, fueron destruidos, el banco había trabajado con EDS para configurar servidores de seguridad que estaban situados en el norte de New Jersey. Este local de seguridad permitió que el banco estuviera dispuesto a funcionar en menos de dos horas evitando así severas multas y pérdidas. Los ejecutivos del banco dicen que si EDS no hubiera tenido éxito en poner en marcha el área de recuperación de desastres del norte de New Jersey tan rápido como lo hizo, el banco no se hubiera recuperado nunca.

Al contrario del buen resultado de los planes de seguridad corporativa y de continuidad del negocio puestas en marcha por el banco con EDS, un plan desarrollado por otra gran institución financiera también localizada en el WTC no funcionó tan bien: la empresa había dispuesto sus servidores de seguridad y locales de emergencia separados de las Torres gemelas por sólo unos pocos bloques de edificios y allí las explosiones y fuegos de los ataques los destruyeron.

El número de empresas que no estaban preparadas para la eventualidad de un desastre como el del 11 de setiembre fueron la mayoría. La triste realidad fue esa, como en el caso de las 143 compañías que simplemente desaparecieron en los meses y años que siguieron al atentado con bomba del año 1993 en el WTC, muchas compañías que vivieron la tragedia del 11/09 que no hayan tenido un plan de continuidad simplemente no verán el final de la década. Estas compañías aprenderán sus lecciones acerca de la importancia de un plan de recuperación de desastres de la manera más dura, además del dolor y la angustia por la triste memoria de tan horrible evento.

4.1.1.1.2.4. Sabotaje de las comunicaciones en Colombia

A principios de 1993, 16 trabajadores de la compañía de telecomunicaciones estatal Telecom fueron acusados, en aplicación de la legislación antiterrorista, de delitos relacionados con una huelga realizada en abril de 1992. La huelga privó a Colombia de servicio telefónico durante siete días y retrasó los planes gubernamentales de privatizar Telecom.

La base de los cargos contra los trabajadores de Telecom fue el presunto sabotaje del sistema informático de la empresa para impedir que técnicos ajenos a ella pudieran operarlo durante la huelga. Aunque el código penal civil recoge los delitos de sabotaje y daños contra propiedades del Estado, el Fiscal General de la Nación dictaminó que el caso debía verse ante los tribunales regionales especiales. La legislación antiterrorista define como terrorista a todo "el que provoque o mantenga en estado de zozobra o terror a la población o a un sector de ella, mediante actos que pongan en peligro la vida, la integridad física o la libertad de las personas o las edificaciones o medios de comunicación... valiéndose de medios capaces de causar estragos". En octubre de 1993, el Tribunal Nacional conmutó los cargos de "terrorismo" por "disrupción de comunicaciones", en aplicación del código penal ordinario. Los trabajadores quedaron en libertad bajo fianza al cabo de nueve meses de detención.

4.1.2. Riesgos que enfrenta el Perú

Como en cualquier otra parte del mundo, el Perú no está a salvo de sufrir interrupciones a causa de los desastres naturales, pero también sufre desastres provocados por el hombre, recordando los causados por el terrorismo.

4.1.2.1. Desastres naturales en el Perú

Geográficamente, el Perú está ubicado en la costa Occidental de América del Sur formando parte del denominado Círculo de Fuego del Pacífico. Asimismo, debido a la presencia en el Perú de la Cordillera Andina y a su localización en las zonas tropical y subtropical, permite que frecuentemente se encuentre expuesto a la amenaza de diversos desastres naturales generados por fenómenos geodinámicos internos y externos potencialmente destructivos (sismos, lluvias, huaycos, erupciones volcánicas, etc.). Fuente: ENTORNO TECTÓNICO Y AMENAZA SÍSMICA EN PERÚ JANICE HERNÁNDEZ TORRES Escuela Profesional de Ingeniería Geofísica Universidad Nacional de San Agustín.

En los siguientes cuadros se muestran estadísticas de los desastres naturales ocurridos en el Perú:

Tabla 13 Los 10 desastres naturales – vidas humanas

Top 10 Natural Disasters - number killed:

Disaster type	Date	No Killed
Earthquake	31-May-70	66,794
Epidemic	18-Aug-91	8,000
Slides	Dec-41	5,000
Slides	10-Jan-62	2,000
Epidemic	31-Jan-91	1,726
Earthquake	10-Nov-46	1,400
Epidemic	Jan-92	690
Slides	18-Mar-71	600
Slides	25-Apr-73	500
Flood	Jan-83	364

Tabla 14 Los 10 desastres naturales – afectados

Top 10 Natural Disasters - number affected:

Disaster type	Date	No Affected
Earthquake	31-May-70	3,216,240
Drought	23-Aug-90	2,200,000
Extreme Temperature	Jun-04	2,137,467
Extreme Temperature	7-Jul-03	1,839,888
Earthquake	Mar-72	1,575,000
Drought	14-Jul-92	1,100,000
Flood	Jan-83	700,000
Drought	1983	620,000
Flood	24-Dec-97	580,750
Earthquake	23-Jun-01	349,978

Tabla 15 Los 10 desastres naturales – daños económicos

Top 10 Natural Disasters - economic damage:

Disaster type	Date	Damage US* (000's)
Flood	Jan-83	988,800
Earthquake	31-May-70	530,000
Drought	14-Jul-92	250,000
Slides	10-Jan-62	200,000
Earthquake	23-Jun-01	200,000
Drought	1983	151,800
Drought	23-Aug-90	36,000
Earthquake	5-Apr-86	22,000
Slides	25-Apr-74	21,700
Earthquake	Mar-72	20,000

Tabla 16 Desastres naturales

Summarized Table of Natural Disasters in Peru from 1913 to 2006

	# of Events	Killed	Injured	Homeless	Affected	Total Affected	Damage US$ (000's)
Drought	7	0	0	0	4,226,104	4,226,104	447,800
avg per event		0	0	0	603,729	603,729	63,971
Earthquake	36	70,109	154,395	300,701	5,121,146	5,576,242	805,100
avg per event		1,947	4,289	8,353	142,254	154,896	22,364
Epidemic	9	10,672	79,725	0	234,528	314,253	0
avg per event		1,186	8,858	0	26,059	34,917	0
Extreme Temperature	4	471	1,800,000	0	2,180,055	3,980,055	0
avg per event		118	450,000	0	545,014	995,014	0
Flood	39	2,430	2,985	300,125	2,868,656	3,171,766	1,019,800
avg per event		62	77	7,696	73,555	81,327	26,149
Insect Infestation	1	0	0	0	0	0	0
avg per event		0	0	0	0	0	0
Slides	26	9,735	83	8,626	49,600	58,309	224,700
avg per event		374	3	332	1,908	2,243	8,642
Volcano	2	0	0	0	4,161	4,161	0
avg per event		0	0	0	2,081	2,081	0
Wave / Surge	1	7	2	750	0	752	0
avg per event		7	2	750	0	752	0
Wild Fires	1	0	0	0	1,000	1,000	0
avg per event		0	0	0	1,000	1,000	0
Wind Storm	2	119	0	0	86,682	86,682	0
avg per event		60	0	0	43,341	43,341	0

Fuente EM-DAT: The OFDA/CRED International Disaster Database, www.em-dat.net - Université catholique de Louvain - Brussels – Belgium)

Las sequías en la sierra sur, los aluviones en el Callejón de Huaylas, los terremotos y tsunamis, los huaycos e inundaciones asociados al fenómeno de El Niño, constituyen las amenazas que mayor daño han causado al país. Sin embargo, la suma de numerosos pequeños desastres causados por los friajes, sismos locales o inundaciones, ha provocado un efecto bastante mayor sobre las poblaciones.

4.1.2.1.1. Sequías

Las sequías han afectado gravemente la vida de las poblaciones de la sierra sur y central del país. Los departamentos golpeados por las sequías han sido Ayacucho, Cusco y Puno. Las migraciones procedentes de la sierra sur del país en los años 60 se asociaron a este fenómeno que afectó la vida de los campesinos.

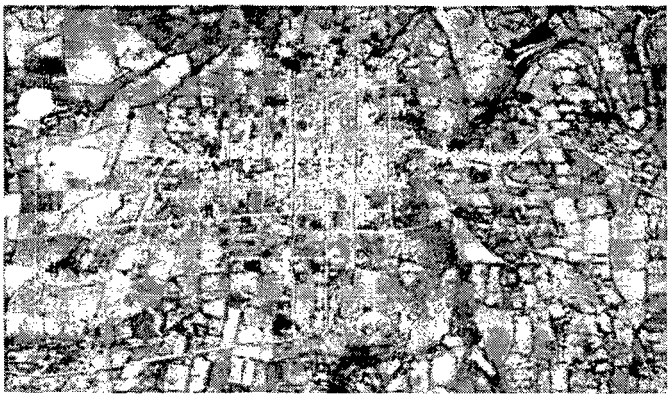
4.1.2.1.2. Aluviones

Los aluviones en el Callejón de Huaylas causaron la destrucción de Huaraz (1941), la desaparición de Ranrahirca (1962) y Yungay (1970). La región Áncash fue sacudida en 1970 por uno de los sismos más destructivos registrados en el país, con una magnitud de 7,8 en la escala de Richter. El área afectada por este movimiento sísmico tuvo un radio de 160 kilómetros. Según el Indeci, este evento causó 67 mil muertes, 150 mil heridos, 800 mil habitantes quedaron sin hogar y casi tres millones de personas fueron afectadas. El 95% de las viviendas, especialmente las de

adobe, quedó completamente en ruinas, colapsó todo el sistema de alcantarillado y la actividad agrícola se paralizó. Tras el terremoto se produjo el desprendimiento de una de las paredes del lado este del nevado Huascarán generando un alud de grandes proporciones que barrió por completo las ciudades de Yungay y Ranrahirca. Las pérdidas materiales ocasionadas por el violento sismo fueron superiores a los US$2.000 millones.

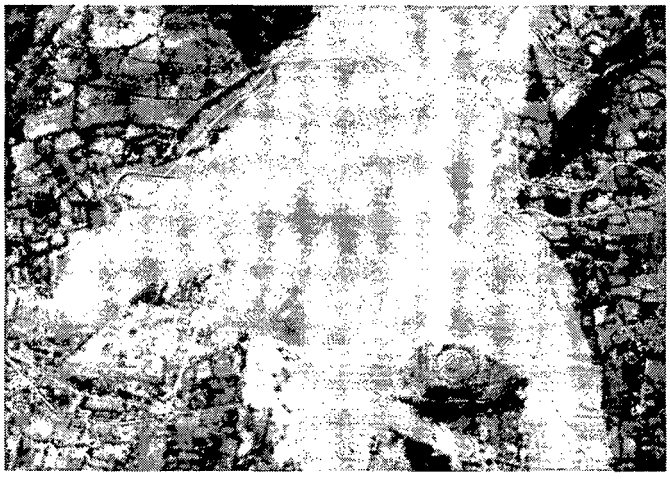
Yungay antes del aluvión

Figura 31 Yungay antes del aluvión



Yungay después del aluvión

Figura 32 Yungay después del aluvión



4.1.2.1.3. Terremotos

Lo conocido acerca de los terremotos que acaecieron en el antiguo Perú, data prácticamente desde la conquista española. Se pueden encontrar relatos sobre los daños y pérdidas humanas, pero diversos factores como lo agreste del territorio, la escasa densidad de población, la falta de medios de comunicación, las preocupaciones de los conquistadores por su afianzamiento en estas nuevas tierras, y además el poco conocimiento científico de la época, no permitieron tener mayor información para confeccionar un catálogo sísmico-geográfico.

Los datos son incompletos y se encuentran esparcidos en diversas obras inéditas o poco conocidas. El historiador don José Toribio Polo (1904), analizando todas esas fuentes, estimó que se habían producido más de 2,500 temblores en territorio peruano, desde la conquista hasta fines del siglo XIX y advirtió que por varias causas no se anotaron muchos de los sismos en el período de 1600 a 1700.

Lo que sí se sabe es que los daños materiales fueron cuantiosos debido a que las construcciones eran inadecuadas para resistir los violentos movimientos del suelo. Se construía aprovechando los materiales de cada región y de acuerdo con las condiciones climáticas, primando las construcciones de adobe y de quincha en la costa, las de piedra en las regiones altas, como en Arequipa donde se construyó con sillar, un tufo volcánico fácil de manejar.

A mediados del Siglo XVII, Lima, principal metrópoli de la América del Sur, había desarrollado una fisonomía peculiar; calles rectas, edificaciones de ladrillo y adobe con balcones de madera, y setenta templos y campanarios.

El terremoto de 1687 destruyó toda Lima y aunque fue reconstruida por el Virrey don Melchor de Navarra y Rocafull, Duque de La Palata, volvió a ser íntegramente destruida por el gran sismo de 1746, que acompañado de un tsunami arrasó el puerto del Callao. El Virrey don José Manso de Velasco realizó con éxito la tarea de reconstrucción según los planos del cosmógrafo francés Luis Godín.

En ese período otras incipientes ciudades del Perú fueron igualmente destruidas por formidables movimientos sísmicos; Arequipa lo fue sucesivamente en 1582, 1600 y 1784; la ciudad imperial del Cuzco en 1650; Trujillo en 1619 y 1725. Durante el siglo XIX sucedieron varios sismos; uno de los principales por su intensidad fue el de 1868, que devastó Arequipa, Tacna y Arica. Este movimiento fue seguido de un tsunami que puso en conmoción a todo el Océano Pacífico, llegando a las alejadas playas del Japón, Nueva Zelandia y Australia.

En el presente siglo, ocurrieron terremotos que afectaron a Piura y Huancabamba (1912), Caravelí (1913), Chachapoyas (1928), Lima (1940), Nazca (1942), Quiches, Ancash (1946), Satipo (1947), Cuzco (1950), Tumbes (1953), Arequipa (1958-1960), Lima (1966), Chimbote y Callejón de Huaylas (1970), Lima (1974).

Según la información que cubre un período de más de cuatrocientos años, los sismos han dejado en el Perú un saldo aproximado de ochenta mil muertos, decenas de millares de heridos y una destrucción material valuada en el orden de decenas de miles de millones de soles.

Después de la gran catástrofe de 1970, el Gobierno nombró una comisión (CRYRZA) para que realizara estudios técnicos de toda la zona afectada como base de una labor planificadora del desarrollo regional urbano y de vivienda.

Lista de terremotos ocurridos en el Perú:

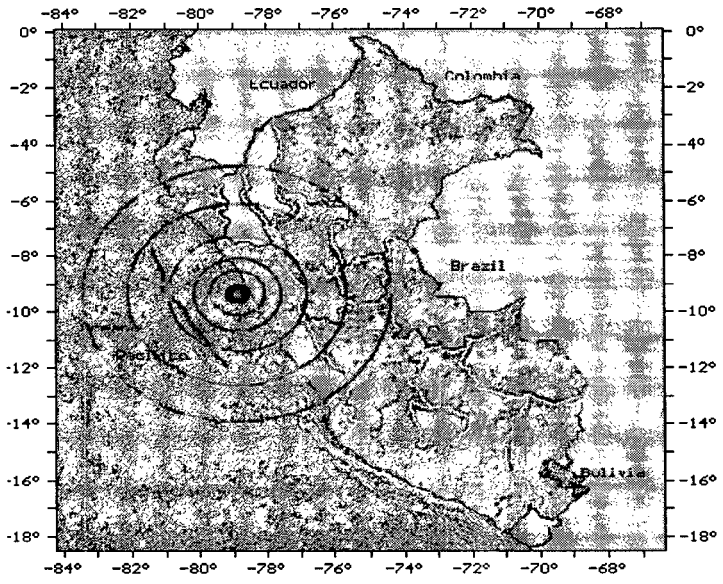
Tabla 17 Terremotos en el Perú

Fecha	Ubicación	Magnitud
1966 10 17	Near the Coast of Peru	8.1
1970 05 31	Peru	7.9
2001 06 23	Near Coast of Peru	8.4
2001 07 07	Near Coast of Peru	7.6
2002 10 12	Peru-Brazil border region	6.8
2005 09 26	Northern Peru	7.5
2006 10 20	Near the Coast of Central Peru	6.5

Fuente: U.S. Geological Survey Earthquake Hazards Program

Terremoto de 1970

Figura 33 Terremoto en el Perú 1970



Fuente: Instituto Geofísico del Perú

Percepción del sismo fuera del área principal:

Al Norte fue sentido fuertemente en Tumbes, con grado III MM. En Guayaquil, Ecuador. Al Norte y Nor Este, causó pánico en Jaén, Moyobamba e Iquitos. Al Este y Sur Este, Grado IV-V en Huánuco. Al Sur y Sur Este Grado VI MM en Lima. Fuerte en Pisco e Ica. No fue sentido en Abancay, Arequipa y el Cuzco.

El sismo ocurrió a las 15:30 del día domingo 31 de Mayo de 1970, fue uno de los terremotos más catastróficos en la historia del Perú. El número de víctimas fue de 50 mil personas, 20 mil desaparecidos y 150 mil quedaron heridos según el informe de la Comisión de Reconstrucción y Rehabilitación de la zona afectada.

La mortalidad se debió en su mayoría a la gran avalancha que siguió al terremoto y que sepulto al pueblo de Yungay.

La región mas afectada, de topografía variable, quedo comprendida entre la costa y el río Marañon al Este, limitada por los paralelos 8° a 10.5° Lat. Sur que abarco prácticamente todo el departamento Ancash y el sur del departamento de La Libertad.

En la región costera quedó destruida Casma, ciudad de viejas construcciones de adobe. Sufrió grandes daños Chimbote, ciudad industrial y pesquera, casas de diversidad de estructuras. Menor destrucción se apreció en Trujillo y Huarmey.

Los daños fueron severos en el Callejón de Huaylas, sobre todo en Huaraz. Según señala Berg y Husid (1970): "en medio de tanto desastre, algunos edificios de hormigón armado y edificios de albañilería soportaron muy bien".

Gran destrucción se observó en las construcciones rurales de los pueblos y caseríos situados en las vertientes de la Cordillera Negra asi como en los ubicados en el lado oriental de la Cordillera Blanca.

Se produjeron intensidades de VIII MM, en los sedimentos fluviales y fluvio-aluviales de la Costa. Sin embargo Lomnitz (1970) estima que en

algunos sedimentos poco consolidados y saturados de agua, entre Casma y Chimbote, la intensidad puede haber llegado al grado IX. En la zona del Callejón de Huaylas fue de grado VII-VIII. En Huarmey VII y en Trujillo VI-VII.

Figura 34 Huaraz después del terremoto de 1970

Huaraz después del terremoto.

Daños ocasionados por la catástrofe, fuente: CRYRZA

- ✓ 60,000 viviendas destruidas.
- ✓ De 38 poblaciones, 15 quedaron con las viviendas destruidas en más de un 80%. El resto, sufrió daños de consideración.
- ✓ En 18 ciudades con un total de 309,000 habitantes y en 81 pueblos con una población de 59,400 personas, los alcantarillados quedaron inhabilitados.
- ✓ 6,730 aulas fueron destruidas.

- ✓ La capacidad de energía eléctrica de Ancash y La Libertad quedó reducida a un 10%, por los serios daños causados a la Central Hidroeléctrica de Huallanca.
- ✓ Quedaron dañadas las facilidades para irrigar 110,000 hectáreas.
- ✓ El 77% de los caminos de La Libertad y Ancash, se interrumpieron así como el 40% de los existentes en Chancay y Cajatambo.

Tabla 18 Desastres naturales en el Perú – estadísticas

Intensidad	Muertos	Heridos	Viviendas destruidas	Afectados	Pérdidas económicas
7,8 escala Richter	75.000	150.000	95%	2'800.000	US$2.000 millones

Fuente: Clasificación de fenómenos y desastres naturales. Atlas de peligros naturales del Perú.

Las ciudades de Lima, Arequipa, Cusco, Ica, Tacna y Áncash son las que han sufrido en mayor grado la furia destructiva de los terremotos. En Tacna y Áncash se registraron dos terremotos de grado XI en la escala MSK (grado 8 en escala de Richter).

Regiones que registraron terremotos:

(+) Sismos más fuertes registrados de intensidad XI (MSK), modificada de Mercalli.

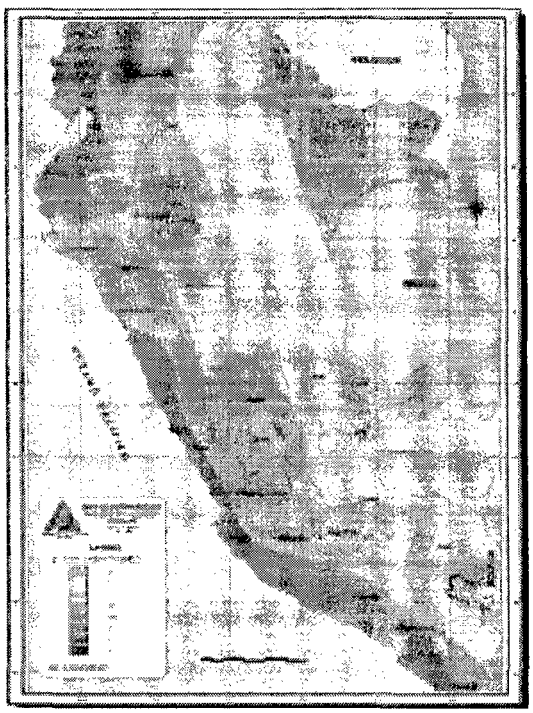
Tabla 19 Terremotos por departamento en el Perú

Región	Número de terremotos
Lima y Callao (+)	36
Arequipa	26
Cusco	16
Ica	12
Tacna (+)	10
Áncash (+)	8
Ayacucho	7
Piura	7
Apurímac	7
Junín	7
San Martín	6
Cajamarca	4
Moquegua	3
Amazonas	2
Tumbes	2
Puno	2
Huánuco	1
Pasco	1
TOTAL	158

Fuente: Mapa de intensidades macrosísmicas máximas. Instituto Geofísico del Perú.

Mapa de distribución de máximas intensidades sísmicas

Figura 35 Mapa de distribución de intensidad sísmica en el Perú



Fuente: CISMID

4.1.2.1.4. Tsunamis

Si bien los tsunamis son menos frecuentes, han dejado secuelas importantes en las principales ciudades y puertos costeños.

Tsunamis en el Perú:

Tabla 20 Tsunamis en el Perú

Año	Zona impactada	Víctimas mortales	Hechos ocurridos
1586	Costa de Lima	22	Intensidad VIII. Olas inundaron 10km².
1664	Costa de Pisco	70	Intensidad VI. Mar inundó ciudad sureña.
1687	Callao	200	Intensidad IX. Destruyó Lima.
1716	Pisco	n.d.	Intensidad IX. Epicentro cerca de Camaná.
1746	Callao	7	El más letal que se conoce. Diecinueve barcos destruidos. Chancay y Huacho destruidos. Olas de siete metros de altura y se internaron 1,5km.
1806	Callao	n.d.	Produjo olas de seis metros de altura.
1868	Desde Trujillo (norte del Perú) hasta Arica y Concepción (Chile)	No se registró víctimas	Nave de guerra fue varada 400m tierra adentro. El epicentro del sismo fue en Arica. Algunas olas alcanzaron 21 metros de altura en Concepción.
1946	Perú, Chile, Ecuador y Colombia hasta Alaska y Hawai	n.d.	n. d.
1974	Callao	No se registró víctimas	También inundó fábricas en las bahías de Chimú y Tortugas (Áncash). En Lima destruyó cultivos.
1996	Chimbote	15	Intensidad 6,9 escala Richter.
1996	Nasca	No se registró víctimas	Intensidad de 6,4 en la escala Richter. El epicentro se produjo a 93km de la costa de Nasca. El puerto de San Juan de Marcona fue afectado.
2001	Camaná	86	Intensidad de 6,9 en la escala de Richter. Epicentro en el mar a 82 km de Camaná. Se generaron tres olas grandes. La más grande de 8,14 metros de altura.

Fuente: Dirección de Hidrografía y Navegación. Marina de Guerra del Perú. Departamento del Medio Ambiente.

- ✓ Tsunami del 1746

El sismo del 28 octubre de 1746 y el Tsunami que lo siguió dejó el Puerto del Callao literalmente bajo las aguas. Se tuvo que ejecutar una reconstrucción de la capital del Perú.

A las diez y media de la noche, el mar se hinchó, y bramó con furia. Media hora más tarde el mar inundó el puerto, y las tierras situadas mas allá, hasta mas de una legua. De 23 navíos en el puerto, se hundieron 19, y 4 fueron arrojados tierra dentro. La luz se había ido. Al siguiente día no

existia ya Callao. De 7,000 personas que formaban la población de Callao, sobrevivieron unos 100. Todo quedó cubierto de escombros; sólo 25 casas quedaron de pie. Hasta el 29 de noviembre, es decir por espacio de mas de un mes, se experimentaron unos 60 temblores, entre los que hubo algunos violentísimos.

El Callao fue destruido por dos olas, una de las cuales alcanzó más de 7 metros de altura. Este maremoto causó la muerte de 5 á 7 mil habitantes y es probablemente el maremoto más fuerte registrado a la fecha. Diecinueve barcos, incluidos los de guerra, fueron destruidos o encallados; uno de ellos fue varado aproximadamente 1.5 Km tierra adentro. En otros puertos también hubo destrucción especialmente Chancay y Huacho.

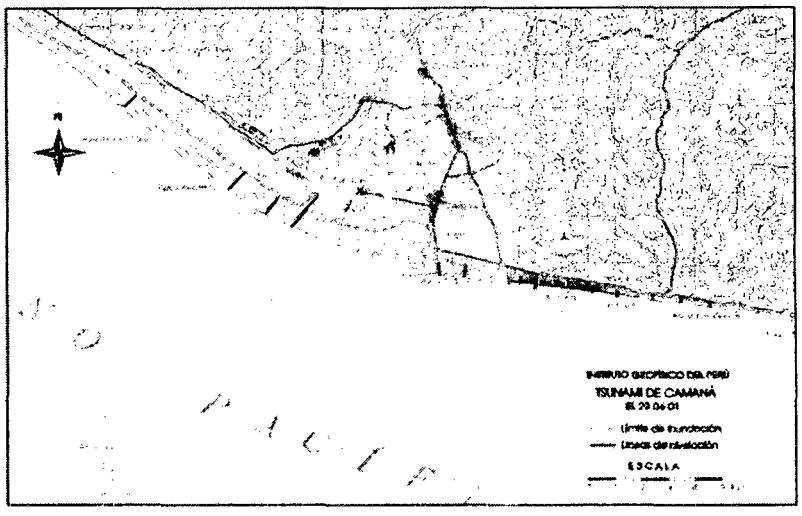
- ✓ Tsunami del 2001

El 23 de junio del 2001 se produjo un sismo de magnitud 8.4, con epicentro ubicado a 82 km al noroeste del distrito de Ocoña, departamento de Arequipa, Perú. Como consecuencia de este sismo se originó un tsunami que afectó la zona sr del Perú, desde Ocoña al norte, hasta Matarani al sur.

Este tsunami originó tres olas consecutivas, llegando la primera luego de 20 minutos aproximadamente de producido el sismo principal, siendo la tercera ola la que causó mayor daño.

Límites de inundación del Tsunami:

Figura 36 Límites de inundación del Tsunami del 2001 en el Perú



4.1.2.1.5. Huaycos e inundaciones

El Fenómeno de El Niño ha dejado efectos desastrosos bajo la forma de una cadena de huaycos e inundaciones en distintas partes del país, con un impacto negativo en la economía. Los más intensos y destructivos fueron el de 1982/83 y el de 1997/98. Las pérdidas económicas originadas por ambos se calculan en US$6.000 millones, un 10% del PBI.

El Estado, con el fin de estar preparado ante una nueva ocurrencia atmosférica, ha formado el Comité de Estudio Nacional del Fenómeno El Niño (ENFEN), participando de igual manera en un programa de monitoreo conocido como Proyecto Naylamp, una iniciativa regional para el estudio integral del fenómeno.

Las consecuencias de El Niño 1982/1983:

Tabla 21 El Niño 1982/1983

Consecuencias	Sectores afectados	Pérdidas económicas
Sociales	Vivienda, educación.	US$ 218 millones
Productivas	Agropecuario, pesquero, comercio, industria.	US$ 2.533 millones
En infraestructura	Transporte, energía.	US$ 532 millones
TOTAL		US$ 3.283 millones

Fuente: Atlas de Peligros Naturales del Perú. Instituto Nacional de Defensa Civil.

Los desastres más importantes causados por los huaycos e inundaciones no han correspondido necesariamente a los fenómenos de El Niño más intensos; en 1987 Chosica fue afectada por varios huaycos que provocaron la desaparición de doscientas personas y destruyeron medio millar de viviendas. La inundación de Chimbote en 1972 causó grandes estragos al igual que las inundaciones del Callao a mediados de los años 90.

En la localidad de Tamburco, provincia de Abancay (Apurímac), se originó en 1997 uno de los deslizamientos de mayores proporciones pocas veces visto; desaparecieron 220 personas, hubo 50 heridos y un centenar de viviendas destruidas. En 1996, un sismo en el sur provocó el deslizamiento de los relaves mineros sobre el río Acarí, causando un

grave impacto ambiental. En el 2004 un movimiento sísmico en Nazca destruyó cientos de viviendas y escuelas.

4.1.2.1.6. Friaje

En julio del 2002 toda la sierra central, sierra sur y selva sur fueron afectadas por un inesperado fenómeno atmosférico de origen antártico que produjo graves consecuencias: más de 29 mil hectáreas de cultivos perdidos, 8 millones 409 mil cabezas de ganado (entre camélidos, ovinos, vacunos) perdidas por muerte o enfermedad. El friaje dejó un total de 6.457 personas con infecciones respiratorias agudas (IRAS) y 80 fallecidos.

4.1.2.2. Desastres provocados por el hombre en el Perú

4.1.2.2.1. Incendios

El 23 de mayo del año 2,000 ocurrió un incendio en el local del Instituto Geofísico del Perú ubicado en la Calle Calatrava 216, Urb. Camino Real – La Molina, Lima, Perú.

Figura 37 Incendio en el Instituto Geofísico del Perú

Fotos: El Comercio y Expreso

Problemas ocasionados por el incendio:

Pérdida total del material bibliográfico de Ciencias de la Tierra existente en la Biblioteca Central del IGP. Textos con temas de Geofísica en general, colecciones de revistas especializadas en Geofísica y Geología, Tesis de diferentes grados y de diversos autores nacionales y extranjeros que realizaron trabajos en el país, especialmente de todo el grupo francés (geólogos y geofísicos), textos universitarios de diferentes campos de la geofísica, artículos, volúmenes de Congresos y reuniones de trabajo nacional e internacional.

Pérdida parcial en el Banco de Datos. El fuego ha destruido un 25% del ambiente físico asignado a esta área. Las PCs (6 en total) fueron dañadas parcialmente por el fuego pero el agua las dejó inservibles. La base de datos sísmicos almacenada en CDs, fue destruida por el fuego en un 20%; sin embargo, las fuentes originales de los datos se encontraban almacenadas en otra oficina a buen resguardo. Por lo tanto, solo es cuestión de tiempo lograr recuperar toda esta información en el formato adecuado. Toda la documentación impresa en papel, sobre los

trabajos que se venían realizando, así como el avance logrado por los jóvenes investigadores, se perdió o se dañó con el agua.

El Servicio de Emergencia Sísmica Nacional se detuvo totalmente durante el incendio; sin embargo, apenas concluida la participación de la Compañía de Bomberos se reinició el funcionamiento de este servicio. Muestra de ello, el CNDG-IGP informó sobre la ocurrencia de un sismo de magnitud 4.4, ocurrido a las 08:14 a.m. (Hora Local), el mismo que afectó a la ciudad de Tumbes con una intensidad de II-III MM. A las 15:00 horas del mismo día (lunes 22 de Mayo), se restableció el Servicio de Emergencia Sísmica con el control total de la Red Sísmica Nacional.

4.1.3. Administración de Riesgos en el Sistema Bancario Peruano

La Superintendencia de Banca, Seguros y AFP en su ley general para el sistema financiero indica el marco de regulación y supervisión del sistema financiero nacional. Ver **¡Error! No se encuentra el origen de la referencia.** para mayor información.

Al año 2014, el sistema bancario peruano lo conforman 16 bancos comerciales, también llamada Banca Múltiple, considerando que el Scotiabank compró las acciones de los Bancos Wiese y Sudamericano, terminando su fusión a mayo del 2006, momento en el que tomó la denominación de Scotiabank Perú. Además a partir de octubre del 2006 inició operaciones un nuevo competidor, el HSBC.

1. Banco de Comercio
2. Banco de Credito del Perú
3. Banco Interamericano de Finanzas
4. Banco Financiero
5. BBVA Banco Continental
6. Citibank del Perú
7. Interbank
8. Scotiabank
9. Banco GNV
10. Banco Falabella
11. Banco Ripley
12. Banco Santander
13. Banco Azteca
14. Deutsche Bank
15. Banco Cencosud
16. ICBC Perú Bank

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

Los desastres en el Perú si ocurren y pueden ocurrir en cualquier momento. Los Bancos deben prepararse para enfrentar desastres, eventos, interrupciones y no sólo para cumplir con las regulaciones.

Si los millones de dólares que se gastan en tecnología anualmente para mantener un nivel competitivo es un indicador de cuanta resiliencia se tiene en tecnología, entonces fallar en la implementación de un plan de recuperación de desastres es un indicador de la negligencia de la organización. No contar con un plan de continuidad y recuperación de desastres pone en alto riesgo la supervivencia del negocio.

No existe mucha información en el Perú sobre continuidad de negocios, el tema es algo confuso ya que hay muchas instituciones internacionales que definen de manera diferente los conceptos sobre recuperación, contingencia, seguridad y continuidad. No se tienen ejemplos que se puedan aplicar a la realidad nacional.

La regulación peruana aún no está alineada completamente a los estándares y normas internacionales de continuidad. Esta debe exigir y al

mismo tiempo brindar más apoyo e información a los Bancos para asegurar la continuidad operativa del sistema bancario en el Perú.

Las clasificadoras de riesgos, incluyen muy escuetamente el riesgo operacional, este es un tema en el que aún no se percibe mucha experiencia. Estas deben incluir en sus reportes, información mas detallada acerca del riesgo operativo de los Bancos, de manera que brinden información de mejor calidad y transparencia.

En los Bancos, las tecnologías de información son un factor primordial en la continuidad de negocios, son la base sobre la cual se soportan todas las operaciones y procesos críticos.

El presente trabajo recoge las mejores prácticas de las diferentes instituciones que desarrollan el tema de continuidad de negocios, adaptándolas de una manera simple y esquematizada, se recomienda desarrollar un plan de continuidad operativa de negocios siguiendo las pautas brindadas en este trabajo, y/o consultando las referencias indicadas.

Plantear varios escenarios de desastre, de manera que sirvan de base para determinar las alternativas viables de reanudación y recuperación de las operaciones y procesos del negocio. El plan debe cubrir el peor escenario de desastre, de manera que la ocurrencia de escenarios menores quede cubierta.

CAPÍTULO VI: GLOSARIO DE TERMINOS

A continuación se enuncian las siguientes definiciones:

Sistema. - Estructura organizativa, procedimientos, procesos y recursos necesarios para implantar una de los procesos.

Procedimiento. - Forma específica de llevar a cabo una actividad.

Proyecto. - Conjunto de tareas y actividades relacionadas con un mismo objetivo, los cuales se ordenan y ejecutan con un principio y un fin claramente definidos. La diferencia fundamental con los procesos y procedimientos estriba en la no repetitividad de los proyectos.

DRP. - Disaster Recovery Planning. Planes de recuperación de desastres.

PCN. - Planes de continuidad del negocio sin Sistemas, procedimientos de operación alternativos que prescinden de las herramientas usuales (entre ellas las de TI) para continuar operando de la mejor manera durante eventos de desastre.

ARO. - Administración de Riesgos de Operación.

BCM. - Business Continuity Management. Modelo de gestión de continuidad de negocios.

BCI. - Business Continuity Institute. Instituto encargado de promover la administración de continuidad de negocios.

DRII. - Disaster Recovery Institute International.

BIA. - Business Impact Analysis. Análisis de Impacto al Negocio.

BCP. - Business Continuity Planning. Planes de continuidad de negocios.

CAPÍTULO VII: REFERENCIAS BIBLIOGRÁFICAS

(1) McGrawHill. Metodología de la investigación.
3ra Edición. 2003

(2) Strohl Systems. Business Continuity Planning Guide
USA 2002.

(3) Instituto de continuidad de negocios – Business Continuity Institute – BCI http://www.thebci.org/

(4) Instituto de recuperación de desastres - Disaster Recovery Internacional Institute – DRII http://www.drii.org/

(5) Super Intendencia de Banca y Seguros http://www.sbs.gob.pe/

(6) Paper sobre Continuidad de negocios. Autores: Kerry Schmitt, Al Decker, Dan Starta (Cap. 2. - Dos Bancos, dos resultados).

8.1. Escala de intensidades de Mercalli modificada

ESCALA DE MERCALLI

Escala I.- No se advierte sino por unas pocas personas y en condiciones de perceptibilidad especialmente favorables.

Escala II.- Se percibe sólo por algunas personas en reposo, particularmente las ubicadas en los pisos superiores de los edificios.

Escala III.- Se percibe en los interiores de los edificios y casas. Sin embargo, muchas personas no distinguen claramente que la naturaleza del fenómeno es sísmica, por su semejanza con la vibración producida por el paso de un vehículo liviano. Es posible estimar la duración del sismo.

Escala IV.- Los objetos colgantes oscilan visiblemente. Muchas personas lo notan en el interior de los edificios aún durante el día. En el exterior, la percepción no es tan general. Se dejan oír las vibraciones de la vajilla, puertas y ventanas. Se sienten crujir algunos tabiques de madera. La

sensación percibida es semejante a la que produciría el paso de un vehículo pesado. Los automóviles detenidos se mecen.

Escala V.- La mayoría de las personas lo perciben aún en el exterior. En los interiores, durante la noche, muchas personas despiertan. Los líquidos oscilan dentro de sus recipientes y aún pueden derramarse. Los objetos inestables se mueven o se vuelcan. Los péndulos de los relojes alteran su ritmo o se detienen. Es posible estimar la dirección principal del movimiento sísmico.

VI.- Lo perciben todas las personas. Se atemorizan y huyen hacia el exterior. Se siente inseguridad para caminar. Se quiebran los vidrios de las ventanas, la vajilla y los objetos frágiles. Los juguetes, libros y otros objetos caen de los armarios. Los cuadros suspendidos de las murallas caen. Los muebles se desplazan o se vuelcan. Se producen grietas en algunos estucos. Se hace visible el movimiento de los árboles y arbustos, o bien, se les oye crujir. Se siente el tañido de las campanas pequeñas de iglesias y escuelas.

Escala VII.- Los objetos colgantes se estremecen. Se experimenta dificultad para mantenerse en pie. El fenómeno es percibido por los conductores de automóviles en marcha. Se producen daños de consideración en estructuras de albañilería mal construidas o mal proyectadas. Sufren daños

menores (grietas) las estructuras corrientes de albañilería bien construidas. Se dañan los muebles. Caen trozos de estuco, ladrillos, parapetos, cornisas y diversos elementos arquitectónicos. Las chimeneas débiles se quiebran al nivel de la techumbre. Se producen ondas en los lagos; el agua se enturbia. Los terraplenes y taludes de arena o grava experimentan pequeños deslizamientos o hundimientos. Se dañan los canales de hormigón para regadío. Tañen todas las campanas.

Escala VIII.- Se hace difícil e inseguro el manejo de vehículos. Se producen daños de consideración y aún el derrumbe parcial en estructuras de albañilería bien construidas. En estructuras de albañilería especialmente bien proyectadas y construidas sólo se producen daños leves. Caen murallas de albañilería. Caen chimeneas en casas e industrias; caen igualmente monumentos, columnas, torres y estanques elevados. Las casas de madera se desplazan y aún se salen totalmente de sus bases. Los tabiques se desprenden. Se quiebran las ramas de los árboles. Se producen cambios en las corrientes de agua y en la temperatura de vertientes y pozos. Aparecen grietas en el suelo húmedo, especialmente en la superficie de las pendientes escarpadas.

Escala IX.- Se produce pánico general. Las estructuras de albañilería mal proyectadas o mal construidas se destruyen. Las estructuras corrientes de albañilería bien construidas se dañan y a veces se derrumban totalmente. Las estructuras de albañilería bien proyectadas y bien construidas se dañan seriamente. Los cimientos se dañan. Las estructuras de madera son removidas de sus cimientos. Sufren daños considerables los depósitos de agua, gas, etc. Se quiebran las tuberías (cañerías) subterráneas. Aparecen grietas aún en suelos secos. En las regiones aluviales, pequeñas cantidades de lodo y arena son expelidas del suelo.

Escala X.- Se destruye gran parte de las estructuras de albañilería de toda especie. Se destruyen los cimientos de las estructuras de madera. Algunas estructuras de madera bien construidas, incluso puentes, se destruyen. Se producen grandes daños en represas, diques y malecones. Se producen grandes desplazamientos del terreno en los taludes. El agua de canales, ríos, lagos, etc. sale proyectada a las riberas. Cantidades apreciables de lodo y arena se desplazan horizontalmente sobre las playas y terrenos planos. Los rieles de las vías férreas quedan ligeramente deformados.

Escala XI.- Muy pocas estructuras de albañilería quedan en pie. Los rieles de las vías férreas quedan fuertemente

deformados. Las tuberías (cañerías subterráneas) quedan totalmente fuera de servicio.

Escala XII.- El daño es casi total. Se desplazan grandes masas de roca. Los objetos saltan al aire. Los niveles y perspectivas quedan distorsionados.

8.2. SBS - Resolución N° 006-2002: Reglamento para la Administración de los Riesgos de Operación

Lima, 4 de enero de 2002

Resolución S.B.S.

N° 006-2002

El Superintendente de Banca y Seguros

CONSIDERANDO:

Que, es objetivo de esta Superintendencia propender a que las empresas supervisadas cuenten con un sistema de control de riesgos que les permita identificar, medir, controlar y reportar los riesgos que enfrentan con la finalidad de proteger los intereses del público de acuerdo a lo señalado en el artículo 347° de la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca, Seguros y AFP, Ley N° 26702, y sus modificatorias, en adelante Ley General;

Que, entre los riesgos que enfrentan las empresas supervisadas en el desarrollo de sus actividades se encuentran los riesgos de operación, los cuales pueden generarse por deficiencias o

fallas en los procesos internos, en la tecnología de la información, en las personas o por ocurrencia de eventos externos;

Que, resulta necesario establecer criterios mínimos prudenciales para que las empresas supervisadas realicen de manera adecuada la gestión de dichos riesgos;

Estando a lo opinado por las Superintendencias Adjuntas de Banca, Seguros y Asesoría Jurídica; y,

En uso de las atribuciones conferidas por los numerales 7 y 9 del artículo 349° de la Ley General y por la Resolución SBS N° 1028-2001 del 27 de diciembre de 2001;

RESUELVE:

Artículo Primero.- Aprobar el Reglamento para la Administración de los Riesgos de Operación, que forma parte integrante de la presente Resolución.

Artículo Segundo. - La presente Resolución entra en vigencia al día siguiente de su publicación en el Diario Oficial ¨ El Peruano".

Regístrese, comuníquese y publíquese,

SOCORRO HEYSEN ZEGARRA

Superintendente de Banca y Seguros (e)

REGLAMENTO PARA LA ADMINISTRACION DE LOS RIESGOS DE OPERACION

CAPITULO I

DISPOSICIONES GENERALES

Alcance

Artículo 1º.- Las disposiciones de la presente norma son aplicables a las empresas señaladas en los artículos 16° y 17° de la Ley General, al Banco Agropecuario, a la Corporación Financiera de Desarrollo S.A. (COFIDE), al Banco de la Nación, a la Fundación Fondo de Garantía para Préstamos a la Pequeña Industria (FOGAPI) y a las derramas y cajas de beneficios que se encuentren bajo la supervisión de esta Superintendencia, en adelante empresas.

Definiciones

Artículo 2º.- Para los efectos de la presente norma deben considerarse los siguientes términos:

a. Administración de riesgos: Proceso que consiste en identificar, medir, controlar y reportar los riesgos que la empresa enfrenta.
b. Directorio: Toda referencia al directorio, entiéndase realizada también a cualquier órgano equivalente.

c. Información: Cualquier forma de registro electrónico, óptico, magnético o en otros medios, susceptible de ser procesada, distribuida y almacenada.

d. Proceso: Conjunto de actividades, tareas y procedimientos organizados y repetibles.

e. Proceso crítico: Proceso considerado indispensable para la continuidad de las operaciones y servicios de la empresa, cuya realización podría ser razonablemente desarrollada por la empresa supervisada.[1]

f. Reglamento del Sistema de Control Interno: Reglamento del Sistema de Control Interno aprobado mediante la Resolución SBS Nº 1040-99 del 26 de noviembre de 1999.

g. Servicios críticos provistos por terceros: Servicios relacionados a procesos críticos provistos por terceros, cuya realización podría ser razonablemente desarrollada por la empresa supervisada. 1

h. Superintendencia: Superintendencia de Banca, Seguros y AFP.

i. Tecnología de información: Incluye los sistemas informáticos y la tecnología asociada a dichos sistemas.

j. Riesgo legal: Posibilidad de ocurrencia de pérdidas financieras debido a la falla en la ejecución de contratos o acuerdos, al incumplimiento no intencional de las normas, así como a factores externos, tales como cambios regulatorios, procesos judiciales, entre otros[2]

Riesgos de operación

---

[1] Literales e. y g. sustituidos mediante Resolución SBS N° 240-2005 del 08/02/2005

[2] Literal incorporado mediante Resolución SBS N° 240-2005 del 08/02/2005

Artículo 3º.- Las empresas deben administrar adecuadamente los riesgos de operación que enfrentan. Entiéndase por riesgos de operación a la posibilidad de ocurrencia de pérdidas financieras por deficiencias o fallas en los procesos internos, en la tecnología de información, en las personas o por ocurrencia de eventos externos adversos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y el de reputación.[3]

Responsabilidad del Directorio y la Gerencia

Artículo 4º.- El Directorio es responsable del establecimiento de políticas y procedimientos generales para identificar, medir, controlar y reportar apropiadamente los riesgos de operación. Asimismo, será también su responsabilidad el velar por el cumplimiento de las referidas políticas y procedimientos y de las disposiciones contenidas en el presente Reglamento. Corresponderá a la Gerencia General la implementación de las políticas y procedimientos generales establecidos por el Directorio.

Unidad de riesgos

Artículo 5º.- De conformidad con lo dispuesto en el Reglamento del Sistema de Control Interno, la Unidad de Riesgos será la encargada de la administración de los riesgos de operación que enfrenta la empresa, pudiendo comprender a alguna unidad especializada para la evaluación de dicho riesgo.

[3] Artículo sustituido mediante Resolución SBS N° 240-2005 del 08/02/2005

Asimismo, para dicho fin, la unidad de riesgos o, de ser el caso, la unidad especializada, deberá contar con la infraestructura adecuada, así como con los recursos humanos, técnicos y logísticos que le permitan el apropiado cumplimiento de sus funciones, de acuerdo a la dimensión y estructura de la empresa, la naturaleza de sus operaciones y servicios y la complejidad de los mismos.

Entre las funciones de la referida unidad responsable se incluirán por lo menos las siguientes:

a. Preparación y evaluación de políticas para la administración de los riesgos de operación.
b. Desarrollo de metodologías para la evaluación cuantitativa y/o cualitativa de los riesgos de operación.
c. Evaluación de los riesgos de operación, de forma previa al lanzamiento de nuevos productos y ante cambios importantes en el ambiente operativo o informático.
d. Consolidación y desarrollo de reportes e informes sobre la administración de los riesgos de operación por proceso, o unidades de negocio y apoyo.
e. Identificación de las necesidades de capacitación y difusión para una adecuada administración de los riesgos de operación.
f. Otras necesarias para el desarrollo de su función.

Manual de organización y funciones

Artículo 6°.- De conformidad con las disposiciones contenidas en la presente norma y en el Reglamento del Sistema de Control Interno, la empresa deberá disponer de una estructura organizacional y administrativa que le permita una adecuada administración de los riesgos de operación. Dicha estructura deberá establecerse de manera que exista independencia entre la unidad de riesgos y aquellas otras unidades de negocio, así como una clara delimitación de funciones, responsabilidades y perfil de puestos en todos sus niveles. Estos aspectos deberán encontrarse recogidos en el manual de organización y funciones de la empresa.

Manuales de políticas y procedimientos

Artículo 7°.- Las políticas y procedimientos establecidos para la administración de los riesgos de operación deberán estar claramente definidos en los manuales de políticas y procedimientos; asimismo, deberán ser consistentes con el tamaño y naturaleza de la empresa y con la complejidad de sus operaciones y servicios.

Manual de control de riesgos

Artículo 8°.- El manual de control de riesgos deberá contener una sección especial sobre los riesgos de operación. Dicha sección deberá contemplar por lo menos los siguientes aspectos:

a. Políticas para la administración de los riesgos de operación.

b. Funciones y responsabilidades de las unidades de negocio y de apoyo en la administración de los riesgos de operación.

c. Descripción de la metodología aplicada para la medición y evaluación de los riesgos de operación.

d. La forma y periodicidad con la que se deberá informar al Directorio y a la Gerencia General, entre otros, sobre la exposición a los riesgos de operación de la empresa y de cada unidad de negocio.

e. El proceso para la aprobación de propuestas de nuevas operaciones, productos y servicios que deberá contar, entre otros aspectos, con una descripción general de la nueva operación, producto o servicio de que se trate, los riesgos identificados y las acciones a tomar para su control.

CAPITULO II

ADMINISTRACION DE LOS ASPECTOS QUE ORIGINAN LOS RIESGOS DE OPERACION

Procesos internos

Artículo 9°.- Las empresas deberán administrar apropiadamente los riesgos asociados a los procesos internos implementados para la realización de sus operaciones y servicios, de tal forma que se minimice la posibilidad de pérdidas financieras relacionadas al diseño inapropiado de los procesos críticos, o a políticas y procedimientos inadecuados o

inexistentes que puedan tener como consecuencia el desarrollo deficiente de las operaciones y servicios o la suspensión de los mismos.

En tal sentido, podrán considerarse entre otros, los riesgos asociados a las fallas en los modelos utilizados, los errores en las transacciones, la evaluación inadecuada de contratos o de la complejidad de productos, operaciones y servicios, los errores en la información contable, la inadecuada compensación, liquidación o pago, la insuficiencia de recursos para el volumen de operaciones, la inadecuada documentación de transacciones, así como el incumplimiento de plazos y costos planeados.

Tecnología de información

Artículo 10º.- Las empresas deberán administrar apropiadamente los riesgos asociados a la tecnología de información, de tal modo que se minimice la posibilidad de pérdidas financieras derivadas del uso de inadecuados sistemas informáticos y tecnologías relacionadas a ellos, que pueden afectar el desarrollo de las operaciones y servicios que realiza la empresa al atentar contra la confidencialidad, integridad y disponibilidad de la información.

Para este fin, las empresas podrán considerar los riesgos vinculados a las fallas en la seguridad y continuidad operativa de los sistemas informáticos, los errores en el desarrollo e implementación de dichos sistemas y la compatibilidad e integración de los mismos,

problemas de calidad de información, la inadecuada inversión en tecnología, así como las fallas en la adecuación a los objetivos del negocio, entre otros aspectos.

Personas

Artículo 11°.- Las empresas deben administrar apropiadamente los riesgos asociados a las personas de la empresa, de tal modo que se minimice la posibilidad de pérdidas financieras asociadas a inadecuada capacitación del personal, negligencia, error humano, sabotaje, fraude, robo, paralizaciones, apropiación de información sensible, lavado de dinero y similares.

Eventos externos

Artículo 12°.- Las empresas deberán considerar en la administración de los riesgos de operación la posibilidad de pérdidas derivada de la ocurrencia de eventos ajenos al control de la empresa que pudiesen alterar el desarrollo de sus actividades, afectando los aspectos que dan origen a los riesgos de operación referidos en los artículos 9°, 10° y 11° del presente Reglamento. En tal sentido, entre otros factores, se podrán tomar en consideración los riesgos que implican las contingencias legales, las fallas en los servicios públicos, la ocurrencia de desastres naturales, atentados y actos delictivos, así como las fallas en servicios críticos provistos por terceros.

CAPITULO III

REQUERIMIENTOS DE INFORMACION

Informe anual a la Superintendencia

Artículo 13º.- Las empresas deberán presentar a la Superintendencia, dentro de los noventa (90) días calendario siguientes al cierre de cada ejercicio anual, un informe referido a la evaluación de los riesgos de operación que enfrenta la empresa por proceso o unidad de negocio y apoyo. Dicho informe deberá contemplar por lo menos los siguientes aspectos:

a. Metodología empleada para la administración de los riesgos de operación.
b. Identificación de los riesgos de operación por proceso o unidad de negocio y apoyo.
c. Evaluación de los riesgos de operación identificados.
d. Medidas adoptadas para administrar los riesgos de operación materiales identificados y plazos para su aplicación. Dichas medidas podrán ser, entre otras:
   - Evitar el riesgo
   - Reducir su probabilidad de ocurrencia
   - Reducir las consecuencias
   - Transferir el riesgo
   - Retener el riesgo

e. Funcionarios responsables de las actividades de control de riesgo identificadas.
f. Plan de actividades de la Unidad de Riesgos en lo referente a la administración de los riesgos de operación.

Mediante Oficio Múltiple, la Superintendencia podrá definir posteriormente la estructura mínima del informe anual, informes periódicos de situación, asi como su presentación por medios electrónicos.[4]

Información adicional

Artículo 14º.- La Superintendencia podrá requerir a la empresa cualquier otra información que considere necesaria para una adecuada supervisión de los riesgos de operación de la empresa.

Asimismo, la empresa deberá tener a disposición de esta Superintendencia todos los documentos a que hace mención el presente Reglamento, así como la información de auditoría o revisiones realizadas por la casa matriz en caso de las empresas cuya matriz no se encuentre en el país.

[4] Párrafo incorporado mediante Resolución SBS N° 240-2005 del 08/02/2005

CAPITULO IV

COLABORADORES EXTERNOS

Auditoría Interna

Artículo 15º.- La Unidad de Auditoría Interna deberá evaluar el cumplimiento de los procedimientos utilizados para la administración de los riesgos de operación, así como de lo dispuesto en el presente Reglamento. Asimismo, la Unidad de Auditoría Interna deberá incluir la referida evaluación en las actividades permanentes del Plan Anual y deberá realizar los informes y recomendaciones que se deriven de la misma.

Auditoría Externa

Artículo 16º.- Las sociedades de auditoría externa deberán incluir en su informe sobre el sistema de control interno comentarios dirigidos a indicar si la entidad cuenta con políticas y procedimientos para la administración de los riesgos de operación, considerando el cumplimiento de lo dispuesto en el presente Reglamento.

Empresas Clasificadoras de Riesgo

Artículo 17º.- Las empresas clasificadoras de riesgo deberán tener en cuenta las políticas y procedimientos establecidos por la empresa para la administración de los riesgos de operación en el proceso de clasificación de las empresas supervisadas.

Servicios provistos por terceros

Primera.- Las empresas son responsables de asegurar el cumplimiento de la normatividad emitida por la Superintendencia, aun en aquellos casos en que ciertas funciones sean realizadas por terceros. En este sentido, además del cumplimiento de lo dispuesto en la presente Resolución, las empresas deberán asegurarse de que los contratos suscritos con proveedores de servicios críticos a la empresa, incluyan cláusulas que faciliten una adecuada revisión de la respectiva prestación, por parte de las empresas, la Unidad de Auditoría Interna, la Sociedad de Auditoría Externa, así como por parte de la Superintendencia o la persona que ésta designe.

Medidas adicionales

Segunda.- La Superintendencia podrá disponer la adopción de medidas adicionales a las previstas en el presente Reglamento con el propósito de atenuar la exposición a los riesgos de operación que enfrentan las empresas.

Sanciones

Tercera.- En caso de incumplimiento de las disposiciones contenidas en el presente Reglamento la Superintendencia aplicará las sanciones correspondientes de conformidad con lo establecido en el Reglamento de Sanciones.

Plazo y Plan de Adecuación

Cuarta.- Las empresas contarán con un plazo de adecuación a las disposiciones de la presente norma que vencerá el 30 de junio de 2003. A dicha fecha las empresas deberán tener a disposición de este organismo de control los Manuales de Políticas y Procedimientos, el Manual de Organización y Funciones, el Manual de Control de Riesgos y los contratos de servicios críticos provistos por terceros a que se refiere la primera disposición final y transitoria del presente reglamento, adecuados a las disposiciones comprendidas en el mismo.

Para el ejercicio 2002 las empresas no se encuentran obligadas a presentar el informe anual a que se refiere el artículo 13° del presente reglamento. Sin embargo, en un plazo que no excederá del 30 de junio de 2002 deberán remitir a este organismo de control un plan de adecuación a las disposiciones contenidas en la presente norma. Dicho plan deberá incluir un diagnóstico preliminar de la situación existente en la empresa, las acciones previstas para la total adecuación y el cronograma de las mismas, así como los funcionarios responsables del cumplimiento de dicho plan.

Reglamento de Auditoría Interna

Quinta.- Toda referencia realizada al término riesgo informático en el Reglamento de Auditoría Interna, aprobado mediante la Resolución SBS N° 1041-99, deberá ser entendida como referida a los riesgos de operación, de acuerdo con lo dispuesto en la presente norma.

8.3. Ejemplo de Objetivos del Plan de continuidad operativa

Los objetivos del Plan de Continuidad Operativa son:

a. Asegurar que la recuperación de operaciones en caso de Contingencia cumpla con los siguientes criterios:

- ✓ Activación del Centro Alterno en un tiempo menor a una (1) hora.
- ✓ Reanudación de las operaciones On-Line (transacciones en línea), considerando la incorporación del mayor número de oficinas, agencias y canales de distribución electrónica.

b. Organizar los grupos de personas responsables por el proceso de recuperación de operaciones de la institución.

c. Identificar las actividades, procedimientos y tareas necesarias para la recuperación de operaciones.

d. Mantener el control de las operaciones en modalidad de Contingencia, permitiendo el flujo de información sobre el estado de las actividades de recuperación.

Permitir el retorno al centro de cómputo primario, una vez que la situación de contingencia haya sido superada.

8.4. Ejemplo de Alcance del Plan de continuidad operativa

Alcance del Plan de Continuidad Operativa:

Este Plan describe la activación de la contingencia en los siguientes escenarios:

Escenarios de contingencia	***Activación de contingencia***
Desastre en el Centro de datos Primario	Centro de datos Secundario
Desastre en el Centro de datos Primario y Secundario	Centro de datos fuera de la región

La activación del Centro Alterno permite la recuperación de los servicios vitales del negocio del Banco, estos servicios son:

Servicios Críticos
Atención en agencias - Ventanillas.
Cajeros Automáticos.
Sistema de verificación de Firmas.
Atención del Help-Desk.
Servicio transaccional para Empresas.
Servicio de Call Center para Atención al Cliente.
Sistema de autenticación y autorización de transacciones de tarjetas, incluyendo puntos de venta.

Las aplicaciones a recuperar que soportan estos servicios vitales, son las siguientes:

Aplicaciones Críticas	*Plataforma*
Cuentas Corrientes	Mainframe
Ahorros	Mainframe
Tarjetas de Crédito	Mainframe
Operaciones Generales	Mainframe
Base de datos de clientes	Mainframe
Administración de Tarjetas de Crédito	Mainframe

Aplicaciones Críticas	*Plataforma*
Procesos core del Banco	Mainframe
Base de datos de Firmas	Cliente/Servidor
Sistema para transacciones Interbancarias	Cliente/Servidor
Sistema para transacciones con Empresas	Cliente/Servidor
Sistema del Call Center	Cliente/Servidor
Reportes de Clientes	Mainframe
Papeles Comerciales	Mainframe
CTS	Mainframe

Desarrollo paso a paso

Tal como se indicó en el esquema del Capítulo III, los pasos para ejecutar un BIA son:

1. Definir las premisas y el alcance que guiarán el proyecto para el cual se desarrolla el BIA. El alcance consiste en definir las operaciones, funciones o líneas de negocio que participarán en las entrevistas. En esta definición se debe tener en cuenta si se incluye o no a las subsidiarias y/o segmentos del negocio en otra ubicación geográfica.

Para definir las premisas, se describen las circunstancias que impactan en las condiciones en las que el BIA será desarrollado. Las premisas son importantes para definir los escenarios, los objetivos, las razones por las que se analiza o no cierto segmento de la empresa.

2. Desarrollar entrevistas o cuestionarios para recopilar información necesaria para cuantificar el impacto y los riesgos. Las preguntas deben tener relación a la variedad de impacto, riesgos y vulnerabilidades que deben resultar de una interrupción importante del negocio. Cada pregunta debe tener un set de respuestas predefinidas que serán seleccionadas por los entrevistados.

3. Identificar los destinatarios de las entrevistas, quienes serán los responsables por la información brindada. Decidir qué departamentos y quiénes participarán en las entrevistas. Probablemente se envíe mas de un cuestionario a un mismo departamento, dependerá del tamaño y complejidad de la encuesta.

4. Notificar a los destinatarios que serán entrevistados y cómo deben prepararse para este. Comentar a los destinatarios acerca del proyecto de análisis de impacto en el negocio y de su importante participación. Explicar qué es un BIA, por qué se está ejecutando y por qué los escogieron para ser entrevistados.

5. Distribuir los cuestionarios y las instrucciones.

6. Revisar las respuestas devueltas para asegurarse de que las preguntas fueron respondidas correctamente. Asegurarse de que todas las preguntas fueron respondidas, y de que no se malinterpreto alguna de las preguntas.

7. Conducir entrevistas de seguimiento para aclarar ambigüedades o problemas en la interpretación. Si la revisión anterior muestra que algunas preguntas no fueron respondidas como se esperaba, se puede llamar al entrevistado para revisar con él estas preguntas. De esta manera se puede discutir con mayor detalle permitiéndoles sustentar sus respuestas y se obtiene mayor información.

8. Modificar las respuestas de los encuestados en base al seguimiento realizado. Las respuestas de los entrevistados sólo deben ser modificada si es necesario y con la aprobación del entrevistado.

9. Analizar y verificar la información final una vez devuelta. Reflejar lo encontrado en reportes y gráficos.

10. Preparar un reporte para la gerencia en base al análisis de la información. La información encontrada no es útil hasta que se genere un reporte adecuado y se entreguen recomendaciones.

El reporte debe identificar las operaciones y funciones más críticas. También debe describir y cuantificar el impacto financiero y operacional. Éste debe ser mostrado en gráficos y cuadros que visualmente puedan demostrar lo encontrado, tampoco debe llenarse de cuadros para no complicar el reporte, con tres o cuatro gráficos o cuadros es suficiente para explicar el punto.

11. Presentar recomendaciones de lo encontrado en el BIA a la gerencia. Es la base para desarrollar la estrategia, consta de suficiente información de manera que resulta cómodo para la gerencia tomar decisiones.

8.6. Matriz de comunicaciones

"Logo de la empresa"

MATRIZ DE COMUNICACIONES

Plan de Continuidad: "I "Nombre del Plan"
Escenario:

Elaborado por: "Nombre de quien elaboró el flujo"
Fecha última actualización: "Fecha"

Tipo de Comunicación	Medio	Responsable	Frecuencia	Disparador	Descripción de la comunicación	Audiencia

8.7. SBS - Extracto de la Ley No 26702, Ley General del Sistema Financiero

TEXTO CONCORDADO DE LA LEY GENERAL DEL SISTEMA FINANCIERO Y DEL SISTEMA DE SEGUROS Y ORGANICA DE LA SUPERINTENDENCIA DE BANCA Y SEGUROS

LEY No 26702

TÍTULO PRELIMINAR

PRINCIPIOS GENERALES Y DEFINICIONES

Artículo 1º.- ALCANCES DE LA LEY GENERAL.

La presente ley establece el marco de regulación y supervisión a que se someten las empresas que operen en el sistema financiero y de seguros, así como aquéllas que realizan actividades vinculadas o complementarias al objeto social de dichas personas.

Salvo mención expresa en contrario, la presente ley no alcanza al Banco Central.

Artículo 7º.- NO PARTICIPACIÓN DEL ESTADO EN EL SISTEMA FINANCIERO.

El Estado no participa en el sistema financiero nacional, salvo las inversiones que posee en COFIDE como banco de desarrollo de

segundo piso, en el Banco de la Nación, en el Banco Agropecuario y en el Fondo MIVIVIENDA S.A.

DISPOSICIONES FINALES Y COMPLEMENTARIAS

DÉCIMO SEXTA:

El Fondo de Garantía para la Pequeña Industria - FOGAPI, se encuentra sujeto a los factores de ponderación de riesgos, patrimonios efectivos, límites y niveles de provisiones, establecidos por esta ley, así como a la supervisión de la Superintendencia. El plazo de adecuación será de 90 días.

DÉCIMO SÉTIMA:

Los bancos multinacionales constituidos al amparo del Decreto Ley 21915 y que se encuentren en operaciones, que no opten por adecuarse a las normas generales contenidas en la presente Ley, se regirán por las normas siguientes:

1. Sólo pueden ser accionistas de los bancos multinacionales las instituciones financieras de inversión o de crédito, seguros, reaseguros, públicos o privados, de reconocida solvencia en su país de origen.

2. El capital suscrito mínimo de los bancos multinacionales es de cincuenta millones de dólares americanos o su equivalente en otras monedas de libre convertibilidad. El capital pagado no puede ser inferior al cincuenta por ciento de dicha suma.

3. Los bancos multinacionales se constituyen con la participación del capital extranjero y tienen por objeto promover y participar en todo tipo de operaciones bancarias y financieras, de inversión y desarrollo de negocios, servicios y otras actividades afines, en el país y en el exterior.

4. Los bancos constituidos como multinacionales se consideran extranjeros y sus inversiones y créditos en el país como tales, cuando se efectúen con recursos originados en el exterior.

5. Los bancos multinacionales, pueden realizar operaciones activas y pasivas propias de empresas bancarias o financieras en el mercado interno, siempre que asignen de su capital social, en efectivo, un capital no menor al mínimo legal exigido para las empresas bancarias, y mantener tales recursos en el país.

6. Para el establecimiento, traslado y cierre de sucursales o agencias de bancos multinacionales dentro del país, se requiere autorización previa de la Superintendencia, la que se otorga teniendo en cuenta las condiciones económicas y financieras generales y locales y previo informe del Banco Central. En el caso de sucursales o agencias en el exterior, sólo es necesario comunicar el hecho a la Superintendencia.

7. Los libros y registros contables requeridos por las disposiciones legales peruanas deben ser llevados por los bancos multinacionales en español, pudiendo serlo además en el idioma extranjero que establezcan sus estatutos.

8. La contabilidad debe reflejar en cuentas separadas las operaciones, ingresos y gastos que se deriven de las actividades extra territoriales, y aquéllas que se realicen en el país.

9. Las operaciones efectuadas en el mercado interno se registran en moneda nacional, pudiendo mantenerse las operaciones en moneda extranjera en registros auxiliares en la moneda de origen.

10. Los estados financieros consolidados pueden ser elaborados y presentados en la moneda que establezca el respectivo estatuto.

11. En caso de que el banco multinacional tuviera su oficina principal en otro país, le será de aplicación lo dispuesto en el artículo 292° de la presente ley.

12. Cuando el banco multinacional tenga su oficina principal en el Perú, se regirá, en el orden que se indica, por:

a) Las normas contenidas en esta disposición final;

b) Las demás normas contenidas en la presente ley;

c) Las disposiciones contenidas en su estatuto.

13. Cuando el banco multinacional tenga su oficina principal fuera del Perú, y tenga una sucursal en el Perú, se regirá, en el orden que se indica, por:

a) Tratándose de las materias extraterritoriales que no comprometan al ahorro del público, por las normas contenidas en su estatuto social;

b) Tratándose de las materias que comprometan al ahorro del público, por las normas contenidas en la presente ley;

14. Cuando el banco multinacional tenga su oficina principal fuera del Perú, se regirá, en el orden que se indica, por:

a) Las normas contenidas en su estatuto social;

b) Las normas contenidas en esta disposición final, en todo lo que atañe a la información que debe presentar a la Superintendencia, así como a las autorizaciones que debe solicitar de este último Organismo;

c) En caso de que, en el país donde tenga su oficina principal, el banco multinacional no se encontrara sujeto a un mecanismo de supervisión equivalente al que establece la presente ley, la Superintendencia podrá asumir esa supervisión.

15. Los bancos multinacionales deberán presentar a la Superintendencia toda información y documentación que este Organismo les solicite.