GUÍA PARA LA ELABORACIÓN DE UN PLAN DE CONTINUIDAD DEL NEGOCIO EN LAS ENTIDADES VIGILADAS POR LA SUPERINTENDENCIA FINANCIERA DE COLOMBIA

AUTOR: JOHAAN ALBERTO MORENO OLIER

ASESOR TEMÁTICO : JONATHAN MEJIA ALVAREZ

ASESOR METODOLÓGICO: JORGE HENRY BETANCUR

UNIVERSIDAD DE MEDELLÍN

FACULTAD DE INGENIERÍA, PROGRAMA DE POSGRADOS

ESPECIALIZACIÓN EN RIESGOS FINANCIEROS

COLOMBIA

MEDELLÍN

2014

GUÍA PARA LA ELABORACIÓN DE UN PLAN DE CONTINUIDAD DEL NEGOCIO EN LAS ENTIDADES VIGILADAS POR LA SUPERINTENDENCIA FINANCIERA DE COLOMBIA

Comité evaluador

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE GRAFICAS

RESUMEN

En este trabajo se identifican y se explican de forma desglosada las actividades necesarias para diseñar, implantar y mantener un Plan de Continuidad del Negocio en las entidades vigiladas por la Superintendencia Financiera de Colombia (SFC). Este trabajo se fundamenta en las disposiciones del capítulo XXIII de la Circular Básica Contable y Financiera (C.E. 100 de 1995), en el que se dictan las reglas relativas a la administración del riesgo operativo, y en los lineamientos del estándar internacional en continuidad del negocio ISO 22301, que provee una guía para la creación y manejo para la administración de la continuidad del negocio.

Palabras clave: Plan, Guía, Continuidad.

ABSTRACT

This work identifies and explains in a disaggregated way the activities necessary to design, implement and maintain a Business Continuity Plan in the entities supervised by the Superintendencia Financiera de Colombia (SFC). This work is based on the provisions of Chapter XXIII of the Basic Accounting and Financial Circular (EC 100 of 1995), which dictate the rules for operational risk management, and international standard guidelines for business continuity ISO 22301, which provides guidance for the creation and management for managing business continuity.

Keywords: Plan, Guide, Continuity

INTRODUCCIÓN

El tema de este trabajo, está dirigido especialmente a las entidades vigiladas por la Superintendencia Financiera de Colombia.

En esta guía se identifican y explican de forma desglosada las actividades necesarias para diseñar, implantar y mantener un Plan de Continuidad del Negocio, basado en el estándar ISO 22301 norma que fue redactada por los principales especialistas en el tema y proporciona el mejor marco de referencia para gestionar la continuidad del negocio en una organización. En este sentido dentro de esta guía se abordaran aspectos tales como:

- Análisis de impactos en el negocio y evaluación de riesgos
- Estrategia de la continuidad del negocio.
- Establecimiento e implementación de procedimientos de continuidad del negocio.

Esta guía se elaboró teniendo en cuenta las diferentes fuentes información relacionada con los aspectos normativos y reglamentarios de la administración de riesgos para las entidades vigiladas por la Superintendencia Financiera de Colombia y la gestión de la continuidad del negocio propuesta por los estándares internacionales vigentes.

CAPÍTULO I PLANTEAMIENTO DEL PROBLEMA

En los últimos años, la Continuidad de Negocio se ha convertido en un tema importante dentro de la planeación que hacen las organizaciones. Mantenerse en el mercado hoy no sólo es cuestión de competitividad, estrategia de ventas o innovación. Es también entender los riesgos del entorno a los que está expuesta la empresa donde desarrolla sus actividades. Los constantes cambios mundiales en materia social, económica, política o ambiental, han hecho que las organizaciones cada vez más se vean expuestas a los riesgos propios del entorno donde desarrollan sus actividades. Así lo han entendido y en los últimos años muchas empresas han empezado a incorporar a sus estrategias, planes de actuación ante potenciales situaciones de emergencia, que puedan tener un impacto significativamente alto en sus operaciones normales y que coloquen en riesgo su permanencia en el mercado. Para ningún observador es extraño reconocer que en los últimos años las convulsiones de toda índole han ido en aumento, como la caída de las torres gemelas en Nueva York, el 11 de septiembre de 2001 que causó la muerte a más de 3.000 personas y un coletazo económico mundial. Dos años más tarde, en Agosto de 2003 un apagón sin precedentes afectó el nordeste de los Estados Unidos y Canadá, dejando durante horas en la oscuridad a 50 millones de personas. El 7 de julio de 2005, los atentados terroristas en el metro de Londres ocuparon los encabezados de las noticias mundiales. (Buitrago, 2009).

Colombia no ha sido ajena a estas situaciones y los datos así lo demuestran. El 25 de enero de 1999 un terremoto de 6.3 grados en la escala de Richter sacudió la región cafetera del país y dejó destrozadas varias ciudades como Armenia (Arboleda, 2013).

El 6 de diciembre de 1989 un camión bomba estalla frente a la sede del desarticulado Departamento Administrativo de Seguridad (DAS, entonces central de inteligencia del Estado), que causó la muerte a 63 personas y heridas a 660 más. El 15 mayo de 2012 un autobús cargado de explosivos estalla en la calle 74 con la avenida Caracas, muy cerca del

centro financiero de Bogotá, con un número aún indeterminado de muertos y heridos. (Agencia EFE, 2012).

Todas las anteriores referencias son una clara muestra de los incidentes a los que las organizaciones están expuestas. Si bien es cierto, que no se puede predecir su ocurrencia, es factible crear planes y estrategias para tratar de reducir su impacto. Hace poco más de 20 años el tema de respaldo o contingencia era desarrollado en la parte informática. Sin embargo, a través del tiempo el concepto se ha ampliado hasta llegar a lo que hoy se conoce como Business Continuity Plans (Planes de Continuidad de Negocio) o Disaster Recovery Plans (Planes de Recuperación ante Desastres) donde se pretende cubrir no solo la parte de datos e informática sino las actividades operacionales más representativas e importantes del negocio. (Buitrago, 2009).

Las consecuencias para una empresa que se vea afectada por una situación de desastre y no tenga planes de recuperación o de continuidad serían enormes; no sólo se vería afectada reputacional y financieramente sino que corre el riesgo de desaparecer. (Buitrago, 2009)

Para dar una idea de las consecuencias que podría afrontar una entidad, al no contar con un plan de continuidad que le permita mitigar el riesgo operativo y asegurar la continuidad de sus procesos, se exponen las siguientes cifras las cuales indican que de cada 100 empresas que afrontan un desastre, sin contar con un plan de continuidad, el 43% nunca reabre su negocio y desaparece del mercado, el 51% cierra en menos de 2 años y solo el 6% sobrevive a largo plazo (Del Pino, 2007).

En Colombia El 45% de las empresas no han implementado un plan de recuperación ante desastres en el lugar de trabajo y el 60% no tiene un plan de continuidad de operaciones comerciales. (Finanzas Personales, 2012)

Durante los últimos cuatro años las entidades vigiladas por la Superintendencia Financiera de Colombia han incurrido en sanciones pecuniarias que ascienden a 231 millones de pesos por no

cumplir con los aspectos normativos en relación a la administración de la continuidad del negocio (Superintendencia Financiera de Colombia, 2012).

PREGUNTA GENERAL

¿Qué aspectos se deben tener en cuenta para desarrollar un Plan de Continuidad del Negocio en las entidades vigiladas por la SFC?

PREGUNTAS ESPECÍFICAS

1 ¿Cuáles son las fases para desarrollar un Plan de Continuidad del Negocio en las entidades vigiladas por la SFC?

2 ¿Qué beneficios trae para una organización la implementación de un Plan de Continuidad del Negocio del Negocio en las entidades vigiladas por la SFC?

3 ¿Cuáles son las principales dificultades para implantar un Plan de Continuidad del Negocio en las entidades vigiladas por la SFC?

1.1 JUSTIFICACIÓN

Toda organización depende de sus recursos, del personal y de las tareas que día a día son ejecutadas con el fin de mantener los beneficios y la estabilidad. La mayoría de las organizaciones poseen bienes tangibles, empleados, sistemas y tecnologías de información, entre otros. Si alguno de estos componentes es dañado o deja de estar accesible por la razón que sea, la organización puede paralizarse. Cuanto mayor sea el tiempo de inactividad, mayor es la probabilidad de que tenga que comenzar desde cero. Incluso muchas organizaciones no son capaces de recuperarse después de ser víctima de algún desastre. Adicionalmente, en ocasiones existe la percepción errónea de interpretar como una falta de confianza o una señal de debilidad el hecho de que una organización anticipe que algún componente de su actividad de negocio puede fallar. Nada más lejos de la realidad.

Aparte de prevenir o minimizar las pérdidas para el negocio que un desastre puede causar, el objetivo principal de gestionar la continuidad del negocio en una organización es garantizar que ésta dispone de una respuesta planificada ante cualquier trastorno importante que puede poner en peligro su supervivencia.

Esta afirmación de por sí constituye un argumento irrefutable que explica la necesidad de instaurar en todas las compañías tales estrategias, independientemente de su tamaño y/o sector.

Además la implementación de un plan de continuidad puede aportar otros beneficios tales como:

a) Ser una ventaja competitiva frente a otras organizaciones: El hecho de mostrar que se toman medidas para garantizar la continuidad de negocio mejora la imagen pública de la organización y revaloriza la confianza frente a sus partes interesadas.

b) Gestionar de manera preventiva los riesgos: A través de la gestión de la continuidad, una organización es capaz de abordar la gestión proactiva de amenazas y riesgos que pueden impactar en sus operaciones.

c) Prevenir o minimizar las pérdidas de la organización en caso de desastre: La identificación proactiva de los posibles impactos e inconvenientes que una interrupción de sus actividades de negocio puede provocar.

d) Asegurar la "resiliencia" de las actividades de negocio ante interrupciones, aumentando la disponibilidad de los servicios dispuestos para el cliente.

e) Cumplir los requerimientos regulatorios: El numeral 3.1.3.1 del capítulo XXIII de la Circular Básica Contable y Financiera (C.E. 100 de 1995) establece que las entidades vigiladas por la Superintendencia Financiera de Colombia, de acuerdo con su estructura, tamaño, objeto social y actividades de apoyo, deben definir, implementar, probar y mantener un proceso para administrar la continuidad del negocio que incluya elementos como: prevención y atención de emergencias, administración de la crisis, planes de contingencia y capacidad de retorno a la operación normal.

f) Asignar de manera eficiente las inversiones en materia de seguridad: Todo plan de continuidad de negocio está diseñado conforme a un proceso previo de análisis de riesgos, el cual permite priorizar los mismos y fijar los esfuerzos y los presupuestos en las áreas más necesitadas.

1.2 OBJETIVOS

1.2.1 Objetivo general

Desarrollar una guía de implementación de cada una de las fases que componen un Plan de Continuidad del Negocio, basado en la norma ISO 22301, para las entidades vigiladas por la SFC.

1.2.2 Objetivos específicos

1. Exponer cada una de las fases que componen la implementación de un Plan de Continuidad del Negocio en las entidades vigiladas por la SFC.
2. Exponer los beneficios de contar con un Plan de Continuidad del Negocio en una entidad vigilada por la SFC.
3. Exponer las dificultades para implantar un Plan de Continuidad Plan de Continuidad del Negocio en una entidad vigilada por la SFC.

CAPÍTULO II MARCO TEÓRICO

2.1 Generalidades

2.1.1 Superintendencia Financiera de Colombia

La Superintendencia Financiera de Colombia, es un organismo técnico adscrito al Ministerio de Hacienda y Crédito Público, con personería jurídica, autonomía administrativa y financiera y patrimonio propio.

La Superintendencia Financiera de Colombia tiene por objetivo supervisar el sistema financiero colombiano con el fin de preservar su estabilidad, seguridad y confianza, así como, promover, organizar y desarrollar el mercado de valores colombiano y la protección de los inversionistas, ahorradores y asegurados. (SUPERINTENDENCIA FINANCIERA DE COLOMBIA, 2012)

- Historia

La Superintendencia Financiera de Colombia surgió de la fusión de la Superintendencia Bancaria de Colombia en la Superintendencia de Valores, según lo establecido en el artículo 1 del Decreto 4327 de 2005. La entidad es un organismo técnico adscrito al Ministerio de Hacienda y Crédito Público, con personería jurídica, autonomía administrativa y financiera y patrimonio propio.

  - Superintendencia Bancaria

La Superintendencia Bancaria de Colombia fue creada mediante el artículo 19 de la Ley 45 de 1923, año durante el cual se produjeron en nuestro país importantes reformas legislativas que permitieron la conformación de un marco institucional apropiado para el crecimiento y desarrollo de muchos sectores fundamentales de la economía nacional.

Hasta ese momento en Colombia, como en la mayoría de países del mundo, las entidades bancarias funcionaban sin mayores trabas, con escasas garantías para los derechos de sus

ahorradores y otros terceros interesados y mínima supervisión del Estado, ya que a pesar de que la inspección sobre dichos establecimientos estaba consagrada en la Ley 51 de 1918, en la práctica no se ejercía.

Con la mencionada Ley 45 se organizaron las distintas especialidades de la industria bancaria, estimulando la creación de secciones de ahorro y de secciones fiduciarias, y se estableció el campo de acción de cada una de dichas actividades, definiendo los principios de su funcionamiento, con requisitos acordes a los estándares internacionales de la época, los cuales se hicieron exigibles a todas las entidades que realizaran tales actividades.

Así mismo creó un sistema de inspección especializado a cargo de la Superintendencia Bancaria, organismo al que dotó de amplias facultades legales para vigilar el estricto cumplimiento de las leyes y reglamentos por parte de las entidades del sector.

Además, la Ley 45 de 1923, estableció un marco equilibrado de responsabilidades entre la función estatal de vigilancia, el comportamiento de los propietarios y administradores del sistema y la racionalidad del público ahorrador e inversionista, bajo las siguientes bases: necesidad de permiso o autorización estatal para la constitución de la personalidad bancaria y la apertura de nuevos establecimientos; prohibición a los bancos comerciales de ser propietarios de otras empresas o de bienes que no tuvieran que ver con su actividad principal, es decir, se restringió su actividad a la estrictamente bancaria; exigencia de un capital mínimo para poder operar; cumplimiento de condiciones de idoneidad, profesionalismo y experiencia, por parte de las personas interesadas en dedicarse a la actividad financiera y sometimiento al control y vigilancia del Estado, por conducto de la Superintendencia Bancaria.

De esta manera, se limitaron en forma taxativa las facultades de los bancos, para que su ejercicio se ajustara a las restricciones y limitaciones impuestas por las leyes. Además, se tipificaron las operaciones bancarias prohibidas, con el objeto de preservar la estabilidad financiera y la confianza pública.

Como resultado de la aplicación de las normas antes mencionadas, en los años siguientes desaparecieran muchos de los bancos locales y regionales, mediante procesos de adquisición o liquidación, dándole una mayor solidez al sistema bancario nacional, la cual le permitió superar la Gran Depresión que se inició en 1929 y continuó en los años siguientes.

En las décadas posteriores se presentó un permanente proceso de crecimiento y fortalecimiento de la Superintendencia, que procuró ajustar sus esquemas de supervisión a la rápida evolución de las instituciones vigiladas.

Esto le ha permitido afrontar con éxito varias situaciones de crisis que se han presentado en el sistema financiero, como la ocurrida a comienzos de los años 80, cuando el sector resultó seriamente debilitado, por las actuaciones irregulares de los administradores de varias de las más importantes entidades financieras, que utilizaron los recursos captados del público para adquirir el control de empresas y efectuar préstamos a personas y entidades vinculadas, sin contar con garantías adecuadas, situación que posteriormente llevó al encarcelamiento de varios reconocidos banqueros y a la fuga de otros.

Este proceso de modernización de la entidad y actualización de la legislación financiera tuvo un fuerte impulso en la década de los 90, con la expedición de la Ley 45 de 1990, la Ley 35 de 1993, el Decreto Ley 663 de 1993 (Estatuto Orgánico del Sistema Financiero) y sus posteriores modificaciones, en especial la Ley 510 de 1999, que convirtió a la Superintendencia en una entidad con personería jurídica, autonomía administrativa y financiera, así como patrimonio propio, le asignó funciones y le otorgó nuevas facultades.

Continuando con el proceso de modernización, la regulación del país se fue adaptando a los estándares internacionales de supervisión establecidos por el Comité de Basilea a través de la expedición de normas referentes al margen de solvencia, cupos individuales de créditos, la calificación de cartera de créditos y la constitución de provisiones, la valoración de inversiones a precios de mercado y la gestión de activos y pasivos.

- Superintendencia de Valores

La Comisión Nacional de Valores fue creada mediante la Ley 32 de 1979, con el objetivo de "estimular, organizar y regular el mercado público de valores", entendiendo por tal el conformado por la emisión, suscripción, intermediación y negociación de los documentos emitidos en serie o en masa, respecto de los cuales se realizara oferta pública, y que otorgaran a sus titulares derecho de participación, de crédito, de tradición o representativos de mercancía.

La entidad comenzó a operar en 1980, en un momento en el cual la confianza del público inversionista en el mercado bursátil estaba gravemente afectada por hechos tales como las grandes pérdidas sufridas por los ahorradores de algunos fondos de inversión y las pugnas por obtener el control de importantes empresas del país.

Las funciones iniciales de la Comisión Nacional de Valores, establecidas en el artículo 9º de la Ley 32 de 1979, no incluían la inspección, vigilancia o control sobre ninguno de los agentes del mercado, centrándose en la administración del Registro Nacional de Valores e Intermediarios; la autorización de las ofertas públicas de los documentos emitidos en serie o en masa y la determinación de las características de la información que debía suministrarse al mercado y de las condiciones para la realización de operaciones a través de bolsa, principalmente.

Posteriormente, con el fin de fortalecer y especializar la supervisión del mercado bursátil, el Decreto 2920 de 1982 trasladó a la Comisión Nacional de Valores el control y vigilancia administrativo de las bolsas de valores, de los comisionistas de bolsas, de los corredores independientes de valores y de las sociedades administradoras de fondos de inversión, con las mismas facultades que antes tenía la Superintendencia Bancaria.

En los años siguientes, diversas normas otorgaron a la Comisión Nacional de Valores la vigilancia de las sociedades administradoras de depósitos centralizados de valores, las

sociedades calificadoras de valores y los fondos de garantía que se constituyan en el mercado público de valores y los fondos mutuos de inversión.

En 1991, la nueva Constitución Nacional dispuso en su artículo transitorio 52, que la Comisión Nacional de Valores tendría el carácter de Superintendencia, y ordenó al Gobierno Nacional la adecuación de la institución a su nueva naturaleza. Mediante el Decreto 2115 de 1992, expedido por el Presidente de la República en ejercicio de las atribuciones conferidas en los Artículos Transitorios 20 y 52 de la Constitución Política, reestructuró la entidad, que pasó a denominarse Superintendencia de Valores.

En el artículo 2º del mencionado decreto 2115 se dispuso que la Superintendencia asumiría el control sobre los emisores de valores, con el fin primordial de velar por la calidad, oportunidad y suficiencia de la información que éstos deben suministrar y presentar al público, proteger los intereses de los inversionistas y verificar que quienes participen en el mercado público de valores ajusten sus operaciones a las normas que lo regulan.

En virtud de lo anterior, cesó la vigilancia que hasta la entrada en vigencia del Decreto 2115 de 1992 ejercía la Superintendencia de Sociedades sobre los emisores de valores de los sectores agroindustrial, minero, industrial, comercial y de servicios, con excepción de los fondos ganaderos y las sociedades que se encontraban en concordato o en proceso de liquidación, las cuales continuarían rigiéndose por las disposiciones que regulaban tales procesos a la fecha de promulgación del referido Decreto.

- Integración de las dos entidades en la Superintendencia Financiera de Colombia

Ante el acelerado desarrollo del mercado financiero, el Gobierno Nacional consideró necesario evaluar si la estructura del actual sistema de regulación y supervisión del mercado, en cabeza de la Superintendencia Bancaria, respecto de los establecimientos financieros y de seguros, y de la Superintendencia de Valores, respecto de los participantes en el mercado de

valores, resultaba adecuada para garantizar un sistema financiero estable, eficiente y competitivo, que brindara un ambiente de protección al consumidor.

En el estudio realizado con tal propósito por expertos internacionales, se concluyó que era necesario revisar la estructura del mercado financiero nacional, la regulación que lo regía y la supervisión que se ejercía sobre éste, con el fin de adecuarlos a las necesidades y realidades económicas vigentes.

Para el efecto, se efectuó una profunda revisión del conjunto normativo aplicable al sistema financiero colombiano, con el propósito de eliminar arbitrajes y disposiciones obsoletas, así como obtener una regulación moderna, clara y coherente que ofreciera seguridad jurídica al supervisor, al sistema y a los consumidores.

Se encontró que la existencia de supervisores diferentes había promovido arbitrajes regulatorios en temas contables, de desarrollo de los negocios y de suministro de información a los consumidores. Un ejemplo de ello se presentaba en el caso de las carteras colectivas, que eran vigiladas por la Superintendencia Bancaria cuando eran estructuradas y administradas por las sociedades fiduciarias; mientras que cuando eran estructuradas y administradas por sociedades comisionistas de bolsa o sociedades administradoras de inversión, se encontraban vigiladas por la Superintendencia de Valores.

Adicionalmente, se hizo necesaria la revisión del diseño del proceso de elaboración de la regulación, de tal forma que se definieran con claridad las competencias de las distintas autoridades, para garantizar su acción coordinada, evitar la proliferación de disposiciones y propiciar la participación de los distintos sectores interesados.

Por otra parte, en relación con la supervisión, se concluyó que los considerables cambios que durante la última década había sufrido el mercado financiero, en su estructura, la dinámica de las operaciones y los riesgos implícitos en éstas, hacían que la existencia de dos supervisores, sobre agentes cuyas actividades con frecuencia estaban bajo el ámbito de las

dos superintendencias, como es el caso de los intermediarios financieros, muchos de los cuales ejercían además la intermediación de valores, invertían en forma protagónica en los escenarios bursátiles de negociación y participaban como emisores en el mercado de valores, hacían necesaria la integración de la supervisión, reconociendo el cambio en las actividades, la evidente integración de los mercados y los crecientes riegos a los cuales están expuestos los diferentes participantes en el sistema.

Así, se materializó la integración de las superintendencias de Valores y Bancaria, en la Superintendencia Financiera de Colombia, como un nuevo supervisor que reemplazó a los dos anteriores. No se trató de que una superintendencia asumiera las funciones de la otra, sino de crear un nuevo esquema de supervisor, que responda a las nuevas realidades del sistema financiero colombiano.

La estructura organizacional y funcional de la Superintendencia Financiera de Colombia se basa en la efectiva y eficiente supervisión de los principales riesgos a los que están expuestas las entidades del sistema, tales como los riegos de crédito, operativo, de mercado y de lavado de activos. Adicionalmente se tuvo en cuenta que los activos del sistema están concentrados en unos pocos grupos o conglomerados financieros, integrados por instituciones de diferente naturaleza, que exigen una supervisión altamente especializada, comprensiva y consolidada, que permita lograr economías de escala, concentrada en el seguimiento de las operaciones y exposiciones entre entidades del mismo grupo o conglomerado y que advierta oportunamente situaciones que puedan derivar en problemas del conglomerado o sistémicos. (SUPERINTENDENCIA FINANCIERA DE COLOMBIA, 2012).

- Entidades vigiladas por la Superintendencia Financiera de Colombia

La Superintendencia Financiera de Colombia (SFC) tiene como misión preservar la confianza pública de los ciudadanos y la estabilidad del sistema financiero, mantener la integridad, eficiencia y transparencia del mercado de valores y demás activos financieros, de

igual manera, velar por el respeto de los consumidores financieros. Así, ejerce la inspección, vigilancia y control de quienes realizan la actividad financiera, bursátil, aseguradora y cualquier otra relacionada con el manejo o inversión de recursos recibidos (captados) del público.

De acuerdo con las leyes colombianas vigentes, las únicas entidades legalmente autorizadas para la captación, manejo, aprovechamiento o inversión de recursos del público, son las sometidas a la inspección, vigilancia y control de la Superintendencia Financiera de Colombia, a saber: los bancos; las compañías de financiamiento comercial; las corporaciones financieras; las cooperativas financieras; los organismos cooperativos de grado superior de carácter financiero; las entidades oficiales especiales; las sociedades fiduciarias; las secciones de ahorro y crédito de las cajas de compensación; las sociedades administradoras de fondos de pensiones y de cesantía; las sociedades comisionistas de bolsa independientes; comisionistas de bolsa de valores y de bolsas agropecuarias, agroindustriales y de otros productos básicos; las sociedades administradoras de inversión; los fondos mutuos de inversión; los emisores de valores inscritos en el Registro Nacional de Valores y Emisores y las sociedades de capitalización, según las modalidades que la ley expresamente establece para cada tipo de entidad. Así mismo, las únicas entidades autorizadas para la realización de operaciones de seguros son las compañías y cooperativas de seguros sometidas a la inspección, vigilancia control y de esta Superintendencia.

Las citadas entidades autorizadas para captar recursos del público deben constituirse exclusivamente bajo la forma de sociedades anónimas o de cooperativas financieras. Así las cosas, en nuestro país ninguna sociedad colectiva, en comandita, de responsabilidad limitada o empresa unipersonal puede contar con autorización legal para captar recursos del público y, mucho menos, una persona natural.

Las cooperativas de ahorro y crédito, las cooperativas multiactivas con sección de ahorro y crédito y las cooperativas integrales con sección de ahorro y crédito sometidas a la inspección, vigilancia y control de la Superintendencia de la Economía Solidaria, se encuentran autorizadas para desarrollar la actividad financiera exclusivamente con sus asociados o cooperados.

A continuación se muestra un listado de las entidades vigiladas por la Superintendencia financiera de Colombia, con corte al 31 de agosto 2013 (SUPERINTENDENCIA FINANCIERA DE COLOMBIA, 2012)

Tabla 1: Tipos de entidades vigiladas por la Superintendencia Financiera de Colombia

TIPO DE ENTIDAD	TOTAL ENTIDADES VIGILADAS
Administradoras de sistemas de pago de bajo valor	6
Almacenes generales de depósito	4
Banco de la república	1
Bolsas agropecuarias	1
Bolsas de valores	1
Cámara de riesgo central de contraparte	1
Cámaras de compensación de las bolsas agropecuarias	1
Comisionistas de bolsas de valores	27
Compañías de financiamiento	22
Compañías de seguros de vida	19
Compañías de seguros generales	24
Cooperativas de seguros	2
Corporaciones financieras	5
Entidades administradoras del régimen solidario de prima media	6
Entidades cooperativas de carácter financiero	6
Establecimientos bancarios	22
Fondos de garantías	1
Fondos mutuos de inversión vigilados	40
Instituciones oficiales especiales	11
Oficinas de representación del mercado de valores del exterior	14

TIPO DE ENTIDAD	TOTAL ENTIDADES VIGILADAS
Oficinas de representación en Colombia de organismos financieros del exterior	51
Oficinas de representación en Colombia de reaseguradoras del exterior	14
Oficinas de representación en Colombia sin establecimiento de comercio	12
Oficinas de representación sin establecimientos de comercio de sociedades fiduciarias	2
Organismos cooperativos de grado superior	1
Organismos de autorregulación	1
Proveedores de precios para valoración	2
Sociedades administradoras de depósitos centralizados de valores	1
Sociedades administradoras de fondos de pensiones y cesantía	5
Sociedades administradoras de inversión	4
Sociedades administradoras de sistemas de compensación y liquidación de divisas	1
Sociedades administradoras de sistemas de negociación de valores y de registro de operaciones sobre valores	4
Sociedades administradoras de sistemas de negociación y registro de divisas	3
Sociedades calificadoras de valores	3
Sociedades comisionistas de bolsas agropecuarias	22
Sociedades corredoras de seguros	50
Sociedades de capitalización	3
Sociedades de intermediación cambiaria y servicios financieros especiales	2
Sociedades fiduciarias	27
Titularizadoras	2
Totales	**424**

Fuente: www.superfinanciera.com

2.1.2 Capítulo XXIII de la Circular Básica Contable y Financiera (C.E. 100 de 1995)

Las Entidades sometidas a la inspección y vigilancia de la Superintendencia Financiera de Colombia (SFC) están cobijadas por una normatividad que se encuentra en algunas circulares tales como, la Circular Básica Jurídica (C.E. 007 de 1996) y Circular Básica Contable y Financiera (C.E. 100 de 1995), esta última circular en su capítulo XXIII incorpora las reglas relativas a la administración del riesgo operativo, recordemos que este trabajo está fundamentado en este capítulo por lo tanto a continuación abordaremos algunos aspectos del mismo. (SUPERINTENDENCIA FINANCIERA DE COLOMBIA, 2012)

- Consideraciones generales de la norma

En desarrollo de sus operaciones, las entidades sometidas a la inspección y vigilancia de la Superintendencia Financiera de Colombia (SFC) se exponen al Riesgo Operativo (RO).

Por tal razón, dichas entidades deben desarrollar, establecer, implementar y mantener un Sistema de Administración de Riesgo Operativo (SARO), acorde con su estructura, tamaño, objeto social y actividades de apoyo, estas últimas realizadas directamente o a través de terceros, que les permita identificar, medir, controlar y monitorear eficazmente este riesgo.

Dicho sistema está compuesto por elementos mínimos (políticas, procedimientos, documentación, estructura organizacional, el registro de eventos de riesgo operativo, órganos de control, plataforma tecnológica, divulgación de información y capacitación) mediante los cuales se busca obtener una efectiva administración del riesgo operativo. (SUPERINTENDENCIA FINANCIERA DE COLOMBIA, 2012)

- Ámbito de aplicación

Todas las entidades sometidas a la inspección y vigilancia de la SFC, deben adoptar un Sistema de Administración de Riesgo Operativo (SARO), con excepción de las Oficinas de Representación de instituciones financieras y reaseguradoras del exterior. (SUPERINTENDENCIA FINANCIERA DE COLOMBIA, 2012).

- Riesgo Operativo (RO)

Se entiende por Riesgo Operativo, la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos. Esta definición incluye el riesgo legal y reputacional, asociados a tales factores. (SUPERINTENDENCIA FINANCIERA DE COLOMBIA, 2012)

- Sistema de Administración de Riesgo Operativo (SARO)

Conjunto de elementos tales como políticas, procedimientos, documentación, estructura organizacional, registro de eventos de riesgo operativo, órganos de control, plataforma tecnológica, divulgación de información y capacitación, mediante los cuales las entidades vigiladas identifican, miden, controlan y monitorean el riesgo operativo. (SUPERINTENDENCIA FINANCIERA DE COLOMBIA, 2012).

- Etapas de la Administración del Riesgo Operativo

En la administración del riesgo operativo, las entidades deben desarrollar las siguientes etapas:

a) Identificación

En desarrollo del SARO las entidades deben identificar los riesgos operativos a que se ven expuestas, teniendo en cuenta los factores de riesgo. (SUPERINTENDENCIA FINANCIERA DE COLOMBIA, 2012)

b) Medición

Una vez concluida la etapa de identificación, las entidades deben medir la probabilidad de ocurrencia de los riesgos operativos y su impacto en caso de materializarse. (SUPERINTENDENCIA FINANCIERA DE COLOMBIA, 2012)

c) Control

Las entidades deben tomar medidas para controlar los riesgos inherentes a que se ven expuestas con el fin de disminuir la probabilidad de ocurrencia y/o el impacto en caso de que se materialicen (SUPERINTENDENCIA FINANCIERA DE COLOMBIA, 2012).

1) Administración de la continuidad del negocio: De acuerdo con su estructura, tamaño, objeto social y actividades de apoyo, las entidades deben definir, implementar, probar y

mantener un proceso para administrar la continuidad del negocio que incluya elementos como: prevención y atención de emergencias, administración de la crisis, planes de contingencia y capacidad de retorno a la operación normal. (SUPERINTENDENCIA FINANCIERA DE COLOMBIA, 2012).

2) Plan de continuidad del negocio: Conjunto detallado de acciones que describen los procedimientos, los sistemas y los recursos necesarios para retornar y continuar la operación, en caso de interrupción. (SUPERINTENDENCIA FINANCIERA DE COLOMBIA, 2012)

d) Monitoreo

Las entidades deben hacer un monitoreo periódico del perfil de riesgo y de la exposición a pérdidas. (SUPERINTENDENCIA FINANCIERA DE COLOMBIA, 2012)

2.1.3 Plan de Continuidad del negocio

Las entidades vigiladas por la SFC tienen el deber de cumplir con la administración de la continuidad del negocio, para esto es necesario que cuenten con un plan de continuidad del negocio que les permita retornar y continuar la operación, en caso de interrupción. (SUPERINTENDENCIA FINANCIERA DE COLOMBIA, 2012)

- Objetivos de un plan de continuidad del negocio.

Juan Gaspar Martínez en su libro El plan de continuidad de negocio: Una guía práctica para su elaboración (2010) propone que dicho plan debería hacer frente a estos objetivos específicos:

a) Aumentar la probabilidad de continuidad de las funciones críticas de la organización en caso de que un incidente interrumpa las operaciones en las que se apoyan.

b) Proporcionar un enfoque organizado y consolidado para dirigir actividades de respuesta rápida y recuperación ante cualquier incidente o interrupción de trabajo imprevista, evitando confusión y reduciendo la situación de tensión.

c) Proporcionar una respuesta rápida y apropiada a cualquier incidente imprevisto, reduciendo así los impactos resultantes de interrupciones de trabajo a corto plazo.

d) Recuperar las funciones críticas del negocio de manera oportuna, aumentando la capacidad de la organización para recuperarlas ante un incidente que haya dejado las instalaciones dañadas o destruidas.

e) Aumentar la probabilidad de continuidad de los servicios de la organización en caso de que un incidente interrumpa sus operaciones normales.

f) Reducir el tiempo de recuperación, y como consecuencia, las pérdidas económicas, directas e inducidas, como resultado de un desastre.

g) Reducir el impacto, tangible o intangible, en las áreas funcionales como consecuencia de una interrupción de los servicios.

h) Realizar la recuperación de las funciones críticas, mediante el desarrollo de los procedimientos necesarios para reducir la duración de la recuperación, minimizar el coste de la recuperación, evitar la confusión y reducir el riesgo de errores y evitar la duplicación de esfuerzos. (Martínez, 2006)

- Fases de un plan de continuidad del negocio

Las diferentes metodologías que sirven para estructurar un plan de continuidad del negocio cuentan con unas etapas en común, estas son:

- Diseño del Plan y establecimiento de la Política de Continuidad de Negocio.

Comprende la identificación de las actividades que deben ser realizadas de forma previa para comenzar el proceso de desarrollo e implantación del Plan de Continuidad.

En esta fase, la entidad que decide abordar un plan continuidad de negocio debe averiguar qué se va a hacer y por qué.

Una tarea clave de esta fase es designar un coordinador/líder que se encargará de gestionar y supervisar el proceso de elaboración e implantación del plan de continuidad de negocio.

En paralelo, y con el fin de formalizar un marco de actuación que determine los objetivos, y el alcance (actividades de negocio incluidas) del plan, así como las funciones y responsabilidades del mismo, debe elaborarse la política de continuidad de la organización, normalmente es la figura citada en el apartado anterior el encargado de diseñar y elaborar esta política.

Generalmente la citada política es entendida como un documento sencillo, claro y conciso que establece a alto nivel (estratégico) los objetivos, el alcance y las responsabilidades en la gestión de la continuidad de negocio en la organización.

Finalmente el coordinador o equipo de continuidad debe aplicar sus habilidades de gestión de proyectos para programar y desarrollar los siguientes componentes del plan de trabajo: tareas a llevar a cabo para satisfacer los objetivos descritos en la política de continuidad, responsables de ejecutar tales tareas, tiempos de ejecución, hitos, presupuestos, plazos e indicadores de éxito. (INTECO, 2010)

- Conocimiento de los procesos de negocio de la organización y análisis de riesgos

En esta fase se identifican los productos y servicios clave de la entidad, los recursos clave que soportan estas actividades y los riesgos a los que está expuesta.

Identificados los objetivos y el alcance de la gestión de continuidad de negocio a través de la citada Política de Continuidad de Negocio, la entidad debe:

a) Entender la organización mediante la identificación de productos y servicios clave, así como las actividades y recursos críticos que los soportan.

b) Estimar el impacto y las consecuencias de los posibles fallos en esas actividades y recursos críticos.

c) Identificar y valorar los riesgos que podrían interrumpir la entrega de los productos y servicios de la empresa, así como de los recursos sobre los que están soportados.

En esta etapa es importante considerar que toda la entidad es un ente complejo de personas, tareas, departamentos, mecanismos de comunicación y relaciones con proveedores externos, los cuales pueden prestar servicios críticos que deben ser considerados. Uno de los desafíos más grandes en la continuidad del negocio es entender todas las complejidades e interrelaciones existentes de una organización.

En esta fase es necesario que la entidad realice el esfuerzo de identificar y valorar el impacto que podría tener en la organización si una actividad se paraliza, así como el tiempo de interrupción que puede ser soportado por la empresa hasta que las pérdidas no sean asumibles.

En este punto es necesario destacar que el impacto total asociado a la interrupción de alguna actividad de la organización depende de varios factores:

Tabla 2: Factores de interrupción de las actividades en las organizaciones

TIPOS DE IMPACTO	DESCRIPCIÓN DEL IMPACTO
Operativos	Actividades de negocio que dejan de estar en funcionamiento o el coste de las horas de trabajo perdidas por los empleados
Económicos	Costes directos o indirectos como por ejemplo el lucro cesante o el daño emergente
Regulatorios o contractuales	Sanciones por incumplimiento legal o penalizaciones por incumplimiento del contrato con clientes
Imagen	Relación de aspectos más intangibles y por tanto más difíciles de valorar como la imagen, la fiabilidad y la reputación de la organización frente a clientes, proveedores y accionistas

Fuente: INTECO

Otro aspecto importante dentro de esta fase es la identificación y priorización de las actividades y recursos críticos, se deben tener en cuenta aquellos que, en caso de pérdida, tendrían el mayor impacto sobre la actividad empresarial en el menor tiempo posible y, por tanto, necesitarían ser restaurados con mayor inmediatez.

Dentro de esta fase aparecen dos parámetros muy específicos que están estrechamente relacionados con la recuperación estos son el Tiempo de Recuperación Objetivo (RTO) y el Punto de Recuperación Objetivo (RPO).

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

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

Del estudio de los procesos, el cálculo del impacto y de la identificación de las actividades surge el comúnmente denominado Análisis de Impacto en el Negocio (BIA). El BIA constituye la base para elaborar un plan de continuidad de negocio y consiste en describir qué pérdidas potenciales tendrá la entidad si alguna actividad del negocio se interrumpe.

En esta etapa también es importante determinar cuál es la probabilidad de ocurrencia de un desastre o de una interrupción severa de los servicios o actividades críticas. Es por esto que se realiza el análisis de riesgos que consiste en identificar las amenazas sobre los servicios o actividades y su probabilidad de ocurrencia, las vulnerabilidades asociadas a cada servicio y el impacto que las citadas amenazas pueden provocar sobre la disponibilidad de los mismos.

Independientemente de la metodología o de las herramientas empleadas para el análisis de riesgos, el resultado del proceso permite identificar y priorizar aquellos que pueden provocar una interrupción de las actividades de negocio de la entidad o de los recursos críticos sobre los cuales dichas actividades están soportadas. (INTECO, 2010)

- Medidas preventivas

Esta fase plantea la posibilidad de aplicar medidas de seguridad preventivas y proactivas con la intención, en la medida de lo posible, de evitar o gestionar los incidentes graves, sin necesidad de activar el plan de continuidad de negocio a no ser que sea estrictamente necesario.

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

a) Reduzcan la probabilidad de que las actividades críticas sufran interrupciones.

b) Disminuyan el tiempo de una eventual interrupción.

c) Limiten el impacto que una paralización de las actividades críticas pueda provocar en la organización.

d) Incrementen la fortaleza del negocio mediante la eliminación de puntos de fallo únicos (accesos, procesos, clientes, etc.) (INTECO, 2010)

- Estrategias de recuperación

En base a los resultados del BIA y del análisis de riesgos, el objetivo perseguido en esta fase consiste en identificar las alternativas de recuperación de las actividades críticas de la organización en los marcos de tiempo definidos y aceptados.

La organización debe tener en cuenta los posibles daños potenciales a la hora de revisar y seleccionar las diferentes soluciones o alternativas de recuperación de sus actividades críticas, considerando adicionalmente los siguientes factores:

a) La cuantía económica asociada a la implantación de la estrategia de recuperación, la cual suele constituir uno de los mayores inconvenientes a la hora de adquirir una solución de recuperación.

b) Los beneficios que proporciona la citada estrategia.

c) El Tiempo de Recuperación Objetivo (RTO).

d) La pérdida máxima de información que una empresa se puede permitir (RPO).

En esta etapa es importante tener en cuenta los siguientes aspectos con respecto a la selección de las estrategias de recuperación:

a) La elección de las diferentes alternativas de recuperación depende de las necesidades de la organización: tiempos de recuperación objetivo (RTO), costes, recursos humanos/técnicos, etc.

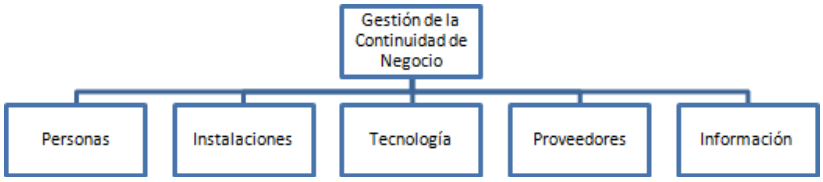
b) Lo más común y recomendable es adoptar una combinación de las estrategias de recuperación para los distintos recursos críticos.

c) El tiempo de recuperación objetivo (RTO) definido por la organización para sus actividades críticas siempre debe ser menor al tiempo máximo permitido de interrupción.

d) El coste de las estrategias de recuperación será generalmente mayor cuanto menor sea el tiempo de recuperación objetivo (RTO).

Una vez analizadas y seleccionadas las estrategias de recuperación que serán empleadas como respaldo en caso de interrupción de las actividades críticas de negocio, es necesario plasmar todas las soluciones y pasos a abordar en un plan (entendido como un conjunto de procedimientos, funciones y actividades que permitirá el restablecimiento de las citadas actividades en unos plazos razonables). (INTECO, 2010)

Grafica 1: Recursos organizacionales sobre los cuales se diseñan las estrategias de recuperación



Fuente: INTECO

- Desarrollo e implantación del plan de continuidad

Una vez que las estrategias han sido definidas, deben ser documentadas y puestas en marcha por los encargados de la continuidad de negocio de la entidad.

En esta fase se pretende:

a) Gestionar la respuesta a incidentes: asegurar la existencia de mecanismos que alerten de la existencia de eventos adversos y actúen frente a los mismos.

b) Asegurar la continuidad de actividades críticas: garantizar que la ejecución del plan descansa sobre las figuras y/o equipos necesarios (desde su activación hasta la vuelta a la normalidad de las actividades), y que se dispone o se puede disponer de los medios materiales para llevarlas a cabo (INTECO, 2010).

- Mantenimiento del plan de continuidad

Los objetivos perseguidos en esta fase son:

a) Inculcar y promocionar una cultura de continuidad de negocio en la entidad de forma que paulatinamente se convierta en un proceso crítico a gestionar bajo un ciclo de mejora continua.

b) Bajo el citado ciclo, mejorar la eficiencia y la solidez del plan o planes de continuidad de negocio.

c) Transmitir fiabilidad a empleados, clientes, accionistas sobre la capacidad de la entidad para superar posibles interrupciones de sus operaciones.

d) Minimizar la probabilidad y el impacto de las interrupciones.

e) Adaptar el plan de continuidad a los cambios organizativos y de negocio que sufren las empresas, revisando periódicamente los análisis de riesgos, los Análisis de Impacto en el Negocio (BIA) y los contactos y responsabilidades asignados que deben mantenerse actualizados en las estrategias y los procedimientos. (INTECO, 2010)

2.1.4 Estándar internacional en continuidad del negocio ISO 22301

Cabe recordar que este trabajo tomará como referencia el nuevo estándar de continuidad del negocio ISO 22301 para desarrollar la guía para la elaboración de un plan de continuidad del negocio en las entidades vigiladas por la Superintendencia Financiera de Colombia.

- Antecedentes

El nuevo estándar ISO 22301 tiene por nombre “Seguridad de la Sociedad: Sistemas de Continuidad del Negocio”. Este modelo aparece como producto de una evolución de lineamientos, buenas prácticas y estándares en continuidad del negocio.

El lineamiento más antiguo es el NFPA 1600, publicado en 1995, el cual estableció una serie de conjuntos de criterios para la gestión de desastres, emergencias y programas de

continuidad para las organizaciones. En 1997 el Disaster Recovery Institute International (DRII), publicó las "Prácticas Profesionales para la Gestión del Negocio".

En 2006, se publicó el lineamiento BS 25999-1, el cual describió de manera concreta el ciclo de vida de la continuidad del negocio. Su enfoque representó las opciones continuas del programa de continuidad del negocio en la organización.

En el año 2007, se publicó el estándar BS 25999-2:2007, el primer estándar internacional certificable y auditable. Fue elaborado con el objetivo de definir los requisitos para un enfoque de sistemas de gestión para la gestión de la continuidad del negocio basado en buenas prácticas, para su uso por organizaciones grandes, medianas y pequeñas que operan en los sectores industrial, comercial, público y de beneficencia.

En el mismo año se publicó el ISO/PAS 22399, el cual generó los lineamientos genéricos para una organización interesada en desarrollar un sistema de gestión con criterios para el desempeño de preparación ante incidentes y continuidad operacional.

En el año 2008, se publicó el lineamiento ISO/IEC 24762 que desarrolló guías para la provisión de información y comunicación frente a la recuperación de desastres. Ese mismo año, se publicó el BS 25777, un código de buenas prácticas sobre gestión de la continuidad.

Una norma que, emparentada con la BS 25999 sobre continuidad de negocio, definió un código de buenas prácticas sobre continuidad centrado en las infraestructuras TIC de las organizaciones.

En el año 2010, se publicó el "ASIS/BSI Busines Continuity Management Standard." Este lineamiento, basado en el BS 25999 (parte 1 y 2), especifica los requerimientos para un sistema de gestión de continuidad del negocio, para permitir a las organizaciones identificar, desarrollar e implementar políticas, objetivos, capacidades, procesos y programas para poder atender eventos alteradores que pudieran paralizar a la organización.

En 2011, se publicó el PAS 200, "Gestión de Crisis - Lineamiento y Buena Práctica". Es un lineamiento diseñado para ayudar a las empresas a tomar pasos prácticos para mejorar su habilidad de manejar crisis. También en el año 2011, se publicó el lineamiento ISO/IEC 27031, el cual describe los conceptos y principios de tecnología de información y comunicación (ICT) para preparar a una organización para la continuidad del negocio. Es aplicable a todo tipo de empresa.

Finalmente, en el año 2012, la Organización Internacional para la Normalización (ISO) publicó el estándar "Seguridad de la Sociedad: Sistemas de Continuidad del Negocio-Requisitos". Este estándar certificable y auditable capta los principales conceptos de los demás lineamientos publicados desde 1995.

El estándar ISO 22301:2012 "Seguridad de la Sociedad: Sistemas de Continuidad del Negocio-Requisitos" aplica el ciclo Plan-Do-Check-Act (PDCA por sus siglas en inglés) para la planificación, establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y la mejora continua de su efectividad. El modelo ha sido creado con consistencia con otros estándares de gestión, tales como: ISO 9001:2008, ISO 27001:2005, ISO 20000-1:2011, ISO 14001:2004 y con el ISO 28000:2007. (Servat, 2012)

Grafica 2: Evolución de los estándares en continuidad del negocio

Fuente: Servat, A. (2012) Nuevo estándar internacional en continuidad del negocio.

- Requisitos y Beneficios

El nuevo estándar ISO 22301 incluye la recuperación o continuidad de las actividades del negocio en el evento de cualquier interrupción. De manera general, debe ser manejado a través de actividades como definición de alcance, evaluación de riesgos, estrategia de continuidad del negocio, objetivos de continuidad del negocio planificación de desarrollo, capacitación, ejercicios, pruebas, revisión y desarrollo continuo. Incluso si la entidad nunca ha experimentado un incidente serio, establecer un plan de continuidad basado en ISO 22301, ayuda a definir los procesos clave del negocio y las interrupciones que pudieran resultar de cualquier amenaza.

ISO 22301 entrega un conjunto integral de controles basados en las Buenas Prácticas. Igualmente el estándar define la capacidad estratégica y táctica de la entidad para planificar y responder a los incidentes e interrupciones del negocio con el fin de continuar las operaciones en un nivel aceptable previamente definido.

El estándar es genérico y ofrece lineamientos a entidades para poner en marcha sus planes de continuidad. A través del estándar ISO 22301, una entidad puede preparase para lo peor y dar los pasos para mejorar su flexibilidad. Para la implementación de un plan de continuidad efectivo, el proceso debería incluir una Evaluación de Riesgos (RA) y un Análisis de Impacto Empresarial (BIA). Ambas son partes inherentes de la ISO 22301 y componente esencial para ayudar a identificar y priorizar actividades, dependencias y recursos en apoyo de los productos y servicios principales. El proceso de internalizar un RA y un BIA también mejora el entendimiento de lo que una falla en cualquiera de estas actividades podría impactar en la organización.

ISO 22301 mejora cualquier negocio asegurando un plan de continuidad planificado y efectivo en todos los niveles, incluyendo:

a) La completa identificación y comprensión por parte de la organización, de los procesos críticos del negocio y el impacto de una interrupción.

b) El aumento de los niveles de flexibilidad y de capacidad de recuperación y la sobrevivencia continua de la entidad.

c) Ventaja sobre los competidores menos flexibles.

d) Comunicar un mensaje positivo a la prensa y a las partes interesadas en condiciones de crisis.

e) Mejorar el perfil de riesgo en la mente de las aseguradoras, resultando en primas más bajas de los seguros.

f) Cumplimiento de las expectativas de organismos reguladores, aseguradoras, socios comerciales y partes interesadas.

g) Disminución significativa del impacto financiero de los incidentes, interrupciones o desastres mayores.

h) Aumenta la oportunidad de sobrevivencia tanto de la organización como de los empleados.

i) Mantener la reputación y posiblemente mejorarla, mediante un enfoque profesional para la gestión de las interrupciones.

j) Respuestas ordenadas y oportunas a incidentes e interrupciones del negocio, con el fin de continuar las operaciones en un nivel aceptable previamente definido y de acuerdo a los acuerdos contractuales.

k) Motiva la coordinación entre los equipos y la organización.

l) Demuestra el compromiso gerencial sobre la gestión de riesgos como un todo con evidencia visible y documentada. (SGS América Latina, 2013).

CAPÍTULO III METODOLOGÍA DE LA INVESTIGACIÓN

3.1 DISEÑO METODOLÓGICO

En este punto del trabajo se expondrá la metodología o procedimiento ordenado que se seguirá para establecer lo significativo de los hechos y fenómenos hacia los cuales está encaminado el interés del trabajo de grado formulado.

3.2. MÉTODO

En la Guía para la elaboración de un plan de continuidad del negocio en las entidades vigiladas por la Superintendencia Financiera de Colombia se aplicó el método Analítico- Sintético. En su fase de análisis se encuentra el estudio de la información que proveen los libros y mejores prácticas respecto al tema en cuestión. El trabajo ha sido segregado en varios temas, los cuales se han investigado de forma separada pero de manera secuencial. En cuanto a la fase de síntesis se ejecutó mediante la obtención de un conocimiento global del plan de continuidad con base en el entendimiento de cada una de sus fases.

3.3 ENFOQUE

Este trabajo concentra un alto componente cualitativo, debido a que incorpora elementos a través de los cuales se pretende priorizar la observación, análisis e interpretación del objeto de investigación. A través de la técnica "Información documental" la cual permite, mediante la recopilación de información, conocer y comprender el objeto de investigación estudiado, a través de un conjunto de recursos bibliográficos, principalmente la norma ISO 22301. Por medio de esta técnica se generaran distintas formas de interpretar y diseñar los aspectos claves del problema tratado.

3.4 ALCANCE

El alcance de este trabajo de grado se define como descriptivo dado que su propósito es el desarrollo de una Guía para la elaboración de un plan de continuidad del negocio en las entidades vigiladas por la Superintendencia Financiera de Colombia, donde se muestren cada una de las etapas que componen dicho plan.

3.5 FUENTE Y TÉCNICAS

Para la Guía para la elaboración de un plan de continuidad del negocio en las entidades vigiladas por la Superintendencia Financiera de Colombia se utilizaron las siguientes fuentes y técnicas

3.5.1 Fuentes primarias

a) Recolección directa.

b) Informantes clave.

c) Observación.

d) Mediciones.

3.5.2 Fuentes secundarias

a) Documentos.

b) Informes.

c) Otras investigaciones.

d) Páginas electrónicas.

3.5.3 Técnicas

a) Entrevistas.

b) Mediciones.

c) Estudios de caso.

d) Estudio de documentos.

3.6 DISEÑO

El diseño del trabajo de grado Guía para la elaboración de un plan de continuidad del negocio en las entidades vigiladas por la Superintendencia Financiera de Colombia es de carácter no experimental transeccional pues, no se pretende construir situaciones ni manipular variables, dado que el objetivo de este tipo de diseño es observar una situación y proporcionar una visión de la misma en un momento dado, para este caso en particular se exponen las diferentes fases para la elaboración de un plan de continuidad.

3.7 UNIDAD DE ANÁLISIS

La unidad de análisis está conformada por las instituciones sometidas a la vigilancia de la Superintendencia Financiera de Colombia (SFC) tales como, los bancos; las compañías de financiamiento comercial; las corporaciones financieras; las cooperativas financieras; los organismos cooperativos de grado superior de carácter financiero; las entidades oficiales especiales; las sociedades fiduciarias; las secciones de ahorro y crédito de las cajas de compensación; las sociedades administradoras de fondos de pensiones y de cesantía; las sociedades comisionistas de bolsa independientes; comisionistas de bolsa de valores y de bolsas agropecuarias, agroindustriales y de otros productos básicos; las sociedades

administradoras de inversión; los fondos mutuos de inversión; los emisores de valores inscritos en el Registro Nacional de Valores y Emisores y las sociedades de capitalización.

3.8 ANÁLISIS DE LA INFORMACIÓN

a) Tabulación.

b) Clasificación

c) Categorización.

d) Análisis estadístico.

e) Graficación.

f) Comparaciones.

g) Contrastación con la teoría.

CAPÍTULO IV RESULTADOS

Con respecto a la información encontrada en la revisión de la literatura, concretamente la norma internacional ISO 22301, a continuación se exponen las fases para la implementación de un Plan de Continuidad del Negocio

4.1 CONTEXTO DE LA ORGANIZACIÓN

Las entidades vigiladas por la Superintendencia Financiera de Colombia (SFC) tienen un contexto interno que incluye misión, visión, políticas, objetivos, estrategias, metas, roles y responsabilidades, estructura, normatividad entre otros. De igual forma interactúa con su medio por lo cual se puede indicar que tienen un contexto externo en el cual deben considerarse aspectos como la competencia, regulaciones legales que apliquen, economía, política, tecnología, cultura y los demás aspectos que se consideren necesarios. La importancia de entender estos aspectos es saber que requiere ser protegido y cuáles son las limitaciones existentes para esta protección. Para determinar el contexto de una entidad vigilada por la Superintendencia Financiera de Colombia es recomendable emplear documentación existente en la entidad relacionada con calidad, seguridad, planeación estratégica y continuidad que brinden información que permitan posicionar a la entidad con respecto a su medio. También es importante realizar entrevistas con altos mandos, encuestas con el personal, visitas a instalaciones y las demás que se consideren necesarias. Esta etapa tiene cuatro objetivos fundamentales:

a) Conocer los alcances y limitaciones de la entidad.

b) Determinar las situaciones que pueden afectar a la entidad a nivel interno y externo.

c) Establecer los diferentes aspectos que requiere proteger la entidad.

d) Establecer el nivel de aceptación de riesgo. (Ramírez, A., Ortiz, Z. 2011:56 - 66)

4.1.1 Entendimiento del negocio.

La esperanza de que una organización recupere sus actividades tras un desastre es muy baja si no dispone previamente de un buen conocimiento acerca de cómo funciona. Ante esta afirmación, es frecuente la postura de muchas organizaciones al pensar que "obviamente, una compañía conoce cómo funciona". Pero si se analiza este asunto detenidamente, muchas de ellas se sorprenderían de lo verdaderamente complicado que resulta entender y asimilar su funcionamiento al nivel de detalle que es requerido para poder reconstruir sus actividades en caso de que sea necesario. Cada miembro de la organización conoce sus funciones y sus responsabilidades al detalle, aunque si se tiene en cuenta que cada actividad de negocio está constituida por información, funciones, redes, personas, tiempo, interdependencias, etc., difícilmente se puede identificar a alguien que sea capaz de explicar todos y cada uno de los procesos de negocio de su organización.

La entidad vigilada debe conocer cuál es su ámbito de negocio y los procesos que le permiten desarrollar su actividad, en este sentido la entidad debe tener pleno conocimiento de los procesos del negocio y el apoyo de los mismos en las tecnologías de la información, de las personas clave para la entidad, de los productos y servicios, de la estrategia de negocio y de las metas de la entidad vigilada. (INTECO, 2010)

4.1.2 Necesidades y expectativas de los interesados

Las partes interesadas son individuos y otras entidades que aportan valor a la entidad vigilada por la Superintendencia Financiera de Colombia, o que de otro modo están interesados en las actividades de la entidad o afectados por ellas. La satisfacción de las necesidades y expectativas de las partes interesadas contribuye al logro del éxito del Plan de continuidad del negocio. Además, las necesidades y expectativas de las partes interesadas como entes individuales son diferentes, pueden estar en conflicto con las de otras partes

interesadas, o pueden cambiar rápidamente. Los medios por los que se expresan y se satisfacen las necesidades y expectativas de las partes interesadas pueden adoptar una amplia variedad de formas, incluyendo la colaboración, la cooperación, la negociación, la contratación externa, o el cese total de una actividad.

Tabla 3. Ejemplos de partes interesadas y sus necesidades y expectativas.

PARTE INTERESADA	NECESIDADES Y EXPECTATIVAS
Clientes	Calidad, precio y desempeño en la entrega de los productos
Propietarios/accionistas	Rentabilidad sostenida Transparencia
Personas en la organización	Buen ambiente de trabajo Estabilidad laboral Reconocimiento y recompensa
Proveedores y aliados	Beneficios mutuos y continuidad
Sociedad	Protección ambiental Comportamiento ético Cumplimiento de los requisitos legales y reglamentarios

Fuente: Norma técnica colombiana NTC-ISO 9004 tercera actualización

La elaboración de un Plan de Continuidad del Negocio exitoso depende en gran medida del entendimiento y la satisfacción de las necesidades actuales y futuras, así como de las expectativas presentes y potenciales de los clientes. Para entender y satisfacer las necesidades y expectativas de las partes interesadas las entidades vigiladas deberán considerar como mínimo los siguientes aspectos.

a) Identificar las partes interesadas y mantener una respuesta equilibrada a sus necesidades y expectativas.

b) Traducir las necesidades y expectativas en los requerimientos.

c) Comunicar los requerimientos a la entidad y a las partes interesadas.

d) Determinar las características claves del producto o servicio para los clientes o usuarios.

e) Considerar la relación de la entidad vigilada con la sociedad.

f) Identificar los requerimientos obligatorios y legales. (Esponda, Palavicini y Navarrete 2001).

4.1.3 Regulaciones y requerimientos de Ley

Las entidades vigiladas deberían establecer procedimientos que le permitan constituir y ajustar en su Plan de Continuidad del Negocio a todos los requisitos legales y reglamentarios aplicables que se refieren a la continuidad de sus operaciones. La información acerca de estos requisitos deberá documentarse, actualizarse y comunicarse a los empleados y otras partes interesadas. (ISO, 2011)

4.1.4 El alcance y ámbito de aplicabilidad del sistema.

Un paso clave que la entidad debe abordar cuando decide impulsar un plan de continuidad de negocio es decidir acerca del alcance del mismo. En ocasiones el plan de continuidad exigido es demasiado extenso si se aplica a toda la entidad y termina fracasando. Por ello, es importante determinar qué áreas, procesos de negocio o productos/servicios de la entidad serán incluidos en el plan. Incluso en los casos en los que la institución tenga varias sedes, será necesario establecer un alcance geográfico. En este sentido, algunas preguntas que deben contemplarse cuando las entidades tratan de determinar el alcance de su estrategia de continuidad son:

a) ¿Cuáles son las actividades más importantes y críticas de la entidad?

b) ¿Qué impacto tendría una interrupción los servicios o de los procesos de la empresa?

c) ¿Durante cuánto tiempo puedo permitirme que la entrega de mis productos o servicios esté interrumpida? (INTECO,2010)

Al definir el alcance del Plan de continuidad del Negocio la entidad vigilada también deberá tener en cuenta las limitaciones presupuestarias con el ánimo de ajustar dicho alcance a estas limitaciones.

Por otro lado es necesario que la entidad vigilada documente y explique claramente los diferentes aspectos (productos, servicios, actividades, recursos y relaciones con las partes interesadas) que excluye del alcance de su Plan de Continuidad asegurándose de que la exclusión de dichos aspectos no perjudica el rendimiento y la efectividad del Plan de Continuidad. (ISO, 2011)

4.1.5 Definición del proceso de Continuidad del Negocio

La entidad deberá establecer un proceso para el Plan de Continuidad del Negocio en el cual se identifiquen plenamente los siguientes aspectos:

a) Un objetivo que explique de forma breve y concisa la finalidad del proceso.

b) El alcance que corresponda a la delimitación del proceso es decir, en donde comienza y en donde termina el proceso.

c) El líder del proceso quien será el responsable de su funcionamiento, resultados y de su mejora continua.

d) Los insumos de diferente índole como datos, productos e información que son fundamentales para el desarrollo del proceso.

e) El resultado final que entrega el proceso para garantizar la continuidad y eficiencia del sistema.

f) Los proveedores que suministran las entradas al proceso.

g) Los actores o grupos de interés que reciben los productos del proceso.

h) Las personas, bienes materiales, financieros o técnicos con los que se cuenta para alcanzar el objetivo del proceso. (ISO, 2000)

4.2 GERENCIA DEL PLAN

4.2.1 Liderazgo del Plan

En este punto es muy importante designar un líder que gestione y supervise el proceso de elaboración e implantación del plan de continuidad de negocio. Esta persona deberá trabajar en conjunto con las diferentes áreas de la entidad para identificar el alcance y los objetivos del plan de continuidad, así como las actividades de negocio que son catalogadas como críticas. Adicionalmente, el perfil de este líder no tiene que estar necesariamente ligado a las áreas de tecnología, tal y como se asume en algunas ocasiones pues, se tiene la falsa idea de que los procesos de continuidad de negocio están constituidos principalmente por componentes tecnológicos.

El líder designado para la gestión y supervisión del desarrollo e implementación del plan de continuidad de negocio, debe contar con las siguientes competencias:

a) Liderazgo.

b) Conocimiento de la entidad y de sus actividades de negocio.

c) Capacidad de comunicación con todas las áreas del negocio.

d) Capacidad para gestionar proyectos, planificar, definir recursos necesarios, realizar seguimiento y reportar a las áreas pertinentes. (INTECO, 2010)

4.2.2 Compromiso de la administración

La alta dirección de la entidad vigilada debe estar comprometida con el Plan de Continuidad del Negocio y debe evidenciar tal compromiso a través de los siguientes aspectos:

a) Cumplir con los requisitos legales aplicables.

b) Establecer una política de continuidad del negocio y unos objetivos alineados con las estrategias de la entidad.

c) Designar una o más personas con la autoridad y las competencias para ser responsables del funcionamiento efectivo del Plan de Continuidad de negocio.

d) Establecer roles, responsabilidades y competencias para los involucrados en el Plan de Continuidad.

e) Asegurar la disponibilidad de los recursos.

f) Establecer una comunicación efectiva que informe acerca de la importancia del cumplimiento de la política y los objetivos de la continuidad del negocio.

g) Propiciar la realización de auditorías internas al Plan de Continuidad del Negocio

h) Adelantar revisiones de la efectividad del Plan de Continuidad del Negocio.

i) Direccionar y apoyar la mejora continua.

j) Participar activamente en las pruebas del Plan de Continuidad del Negocio.

k) Incluir el Plan de Continuidad como tema permanente en las reuniones de la administración. (ISO, 2011)

4.2.3 Política del Plan de Continuidad del Negocio

Con el objetivo de establecer un marco de actuación que determine los objetivos, y el alcance del plan, así como las funciones y responsabilidades de los empleados involucrados en el mismo, la entidad vigilada debe elaborar una política de continuidad. La política debe ser sencilla, clara y concisa y debe establecer a nivel estratégico los objetivos, el alcance y las responsabilidades en la gestión de la continuidad de negocio de la entidad vigilada, con el fin de evitar interpretaciones erróneas. (INTECO, 2010)

La política establecida debe cumplir como mínimo con lo siguiente:

a) Estar acorde con el tamaño, la naturaleza y la complejidad de la entidad vigilada.

b) Incluir las obligaciones legales y regulatorias del Plan de Continuidad.

c) Debe ser comunicada y entendida por cada uno de los actores involucrados en el Plan de Continuidad del Negocio.

d) Estar disponible para las partes interesadas.

e) Proporcionar orientación sobre el alcance y los límites del Plan de Continuidad de Negocio.

f) Establecer los criterios para el tipo y la magnitud de los incidentes que activarán el Plan de Continuidad del Negocio.

g) Ser revisada periódicamente o cuando sucedan cambios significativos.

h) Especificar la periodicidad de las pruebas.

i) Establecer los niveles de servicio en un evento de interrupción.

j) Definir los integrantes del Comité de continuidad. (ISO, 2011)

4.2.4 Roles y Responsabilidades

La alta dirección de la entidad debe asegurar la asignación y comunicación de los roles y las responsabilidades dentro del Plan de Continuidad del Negocio, en este sentido se debe establecer la estructura organizacional que define los equipos que componen el plan de continuidad, esta estructura tiene el objetivo de identificar los responsables de la recuperación de los procesos definidos como críticos y la adecuada atención de situaciones de crisis. Adicionalmente busca soportar el mantenimiento y la actualización requerida de los diferentes componentes y procedimientos asociados al Plan de continuidad del Negocio. Todas las funciones y responsabilidades relacionadas con el Plan de continuidad del negocio deben ser definidas y documentadas y ser sujetas a auditoría.

Los equipos del Plan de Continuidad del Negocio están formados por el personal clave de todas las áreas del negocio necesarias para el diseño, implementación, pruebas, activación y retorno a la situación normal de operación del negocio.

Aunque la composición y número de equipos puede variar según el tipo de estrategia de recuperación, a continuación se muestran algunos ejemplos de los equipos y las funciones que pueden formar parte del Plan. (ISO, 2011)

- Equipo director o comité de crisis

El objetivo de este comité es reducir al máximo el riesgo y la incertidumbre en la dirección de la situación. Este Comité debe tomar las decisiones “clave” durante los incidentes, además de hacer de enlace con la dirección de la entidad, manteniéndoles informados de la situación regularmente.

Las principales responsabilidades de este comité son:

a) Analizar la situación.

b) Tomar la decisión de activar o no el Plan de Continuidad.

c) Iniciar el proceso de notificación a los empleados a través de los diferentes responsables.

d) Realizar el seguimiento del proceso de recuperación, con relación a los tiempos estimados de recuperación. (ISO, 2011)

- Equipo de recuperación

El equipo de recuperación es responsable de establecer la infraestructura necesaria para la recuperación. Esto incluye aspectos tales como todos servidores, PC's, comunicaciones de voz y datos y cualquier otro elemento necesario para la restauración de los servicios.

Las principales responsabilidades de este equipo son:

a) Participar en la preparación y realización de las pruebas relacionadas con el Plan de Continuidad.

b) Identificar cambios y oportunidades de mejoras al plan de continuidad, relacionados con cada proceso crítico.

c) Identificar y Suministrar la información necesaria para actualizar el Plan de Continuidad.

d) Mantener la infraestructura que soporta la operación en contingencia.

e) Documentar los procedimientos de movilización y retorno.

f) Soportar los nuevos procesos críticos que se incluyan dentro del alcance del Plan. (ISO, 2011).

- Equipo logístico

Este equipo es responsable de todo lo relacionado con las necesidades logísticas en el marco de la recuperación, tales como:

a) Transporte de material y personas (si es necesario) al lugar de recuperación.

b) Suministros de oficina.

c) Alimentos.

d) Reservas de hotel, si son necesarias.

e) Contacto con los proveedores.

Este equipo debe trabajar conjuntamente con los demás, para asegurar que todas las necesidades logísticas sean cubiertas. (ISO, 2011)

- Equipo de relaciones públicas y atención a clientes

Este equipo es responsable de canalizar la información que se comunica hacia el exterior de la entidad. Sus funciones principales son:

a) Elaborar de comunicados para la prensa.

b) Establecer comunicación con los clientes.

Uno de los valores más importantes de una entidad son sus clientes, por lo que es importante mantener informados a los mismos, estableciendo canales de comunicación adecuados. (Del Pino, 2007)

4.3 PLANEACIÓN

4.3.1 Objetivos del Plan de Continuidad del Negocio y planes para alcanzarlos

La alta dirección de la entidad vigilada, por la Superintendencia Financiera de Colombia, debe asegurar el establecimiento y documentación de los objetivos del Plan de Continuidad del Negocio. Así mismo, debe velar por la conservación de la documentación referida y debe determinar claramente la forma en que se alcanzarán los objetivos definidos.

Los objetivos para un Plan de Continuidad del Negocio deben:

a) Estar claramente definidos.

b) Ser consecuentes con la política de continuidad.

c) Permitir su medición.

d) Tener plazos para su cumplimiento.

e) Tener en cuenta las necesidades y expectativas de las partes interesadas.

f) Tener en cuenta las regulaciones y requerimientos de ley.

g) Permitir la generación de oportunidades de mejora para el Plan de Continuidad.

h) Permitir su monitoreo y actualización.

Con el fin de garantizar que se alcancen estos objetivos definidos, las entidades vigiladas por la Superintendencia Financiera de Colombia deben determinar:

a) El responsable o los responsables de alcanzar los objetivos del Plan de Continuidad.

b) Las actividades que se realizarán y cuando se llevarán a cabo.

c) La manera en que serán evaluados los resultados de los objetivos establecidos. (ISO, 2011).

4.4 ESTRUCTURA DEL PLAN

4.4.1 Recursos del Plan de Continuidad del Negocio

La entidad vigilada por la Superintendencia Financiera de Colombia debe determinar y proveer los recursos necesarios para el Plan de Continuidad del Negocio.

Le corresponde a la administración de la entidad asegurar la disponibilidad de los recursos necesarios para el adecuado desarrollo del Plan de Continuidad del Negocio y el cumplimiento de los objetivos de continuidad.

A través de la alta dirección la entidad vigilada debe proveer recursos de personal, de infraestructura física, tecnológicos (hardware, software, comunicaciones), de información (impresa o digital) y suministros de oficina que permitan darle cumplimiento a la política y a los objetivos de Continuidad. Así mismo se debe propiciar la comunicación efectiva del Plan de Continuidad de Negocio dentro y fuera de la entidad. (ISO, 2011).

4.4.2 Personal de Respuesta a Incidentes

La entidad vigilada debe designar al personal idóneo con la responsabilidad, autoridad y competencia necesarias para manejar y dar respuesta a los incidentes. Las responsabilidades del personal de respuesta a incidentes deben estar incluidas en procedimientos que permitan:

a) Detectar y escalonar los incidentes.

b) Evaluar los incidentes.

c) Activar una respuesta adecuada a los incidentes.

d) Establecer los niveles de emergencia y primeros auxilios.

e) Determinar los parámetros de seguridad.

f) Establecer un centro de operaciones de emergencia.

g) Establecer el enlace con el equipo de relaciones públicas y atención a clientes de la entidad.

h) Coordinar y comunicar la respuesta a incidentes.

i) Analizar y reportar el incidente

Todo el personal que se encuentra en este grupo debe tener responsabilidades y autoridades claramente definidas que se aplican antes, durante y después del incidente. (ISO, 2011).

4.4.3 Competencias de cada rol

La competencia es entendida como una combinación de educación y entrenamiento apropiada o aplicable, así como habilidades y experiencia, que pueda ser demostrada.

La administración de la entidad vigilada debe determinar las competencias requeridas para todos los roles y responsabilidades de los involucrados en el Plan de Continuidad del Negocio. Todas las personas con funciones asignadas dentro del Plan de Continuidad deben demostrar las competencias requeridas y recibir la capacitación y el apoyo necesario para la adecuada gestión del Plan. En este punto las entidades vigiladas deben:

a) Determinar las competencias necesarias para el personal relacionado con el Plan de Continuidad del Negocio.

b) Suministrar una capacitación que permita que el personal de continuidad alcance las competencias necesarias.

c) Evaluar la eficacia de la capacitación

d) Asegurar que el personal tome conciencia de la importancia de las actividades que desarrollan en el Plan de Continuidad y de cómo contribuyen a los objetivos de dicho plan.

e) Mantener los soporte de todos los puntos anteriores.

El tipo de entrenamiento apropiado para roles específicos puede ser en los siguientes tópicos, dependiendo del punto en que se encuentre el desarrollo del plan:

a) planeación e implementación del Plan de Continuidad del Negocio:

1) Administrar el programa de continuidad del negocio;

2) Realizar análisis de impacto en el negocio (BIA);

3) Documentar el desarrollo e implementación del plan de continuidad del negocio;

4) Ejecutar un programa de pruebas;

5) Evaluar los riesgos;

6) Desarrollar habilidades de comunicación;

b) Respuesta a incidentes y recuperación de negocio:

1) Gestionar la evacuación;

2) Definir un lugar de refugio;

3) Establecer procesos de entrada para dar cuenta de los empleados;

4) Acondicionar sitios de trabajo alterno;

5) Manejar los medios por parte de la entidad vigilada.

Los equipos de respuesta y recuperación deben recibir educación y capacitación acerca de sus responsabilidades y obligaciones de las interacciones que puedan tener con los grupos de socorro y otras partes interesadas. Los equipos deben ser entrenados periódicamente, al menos de manera anual, y los nuevos miembros deben ser entrenados cuando se unen al equipo. Estos equipos también deben recibir capacitación en la prevención de incidentes que pueden derivar en crisis.

Las entidades vigiladas deben establecer programas de entrenamiento y sensibilización para todos los empleados y terceros que se encuentren involucrados en la gestión del Plan de Continuidad del Negocio. (ISO, 2011)

4.4.4 Sensibilización

De nada sirve invertir cuantiosas sumas en un proyecto de transformación empresarial como un Plan de Continuidad del Negocio, con todas sus implicaciones en contratación de consultorías, conformación de costosos equipos de trabajo, procesos de análisis, elaboración de manuales, capacitación especializada, inversión en tecnología y todo tipo de herramientas, si la actitud, los hábitos y las costumbres en los diferentes niveles permanecen intactas.

Muchas organizaciones invierten considerables recursos en la preparación e implementación de Planes de Continuidad de Negocio con el fin de mitigar de la mejor forma el impacto de cualquier eventualidad, pero lamentablemente gran parte de su esfuerzo no produce los resultados esperados porque no se cuenta con el compromiso de las partes involucradas.

En este punto es muy importante que la entidad vigilada determine si, las juntas directivas, los gerentes y funcionarios están conscientes de sus responsabilidades con respecto al Plan de Continuidad. En este sentido la entidad vigilada debería emprender actividades de sensibilización para el Plan de Continuidad del Negocio, orientadas a apoyar la transformación de la cultura empresarial, divulgando a todas las partes interesadas, el avance, los logros, los beneficios, y las obligaciones de cada uno con respecto al referido plan.

La entidad vigilada debe definir el público objetivo de esta sensibilización, que pueden ser juntas directivas, equipos gerenciales, mandos medios, personal operativo de las diferentes áreas de la entidad entre otros.

Las actividades de sensibilización pueden ser:

a) Reuniones de entendimiento de la entidad entre los líderes de los procesos y los responsables del Plan de Continuidad.

b) Análisis de documentación (políticas, manuales, reglamentos, procedimientos, actas).

c) Diseño y generación de Material (diapositivas, videos, piezas didácticas, folletos, casos prácticos).

d) Charlas con facilitadores especializados. (CAES S.A, 2013)

4.4.5 Comunicación y consulta

Las entidades que se encuentran bajo la vigilancia de la SFC deben establecer procesos continuos y reiterativos para suministrar, compartir u obtener la información.

Es pertinente que la comunicación y consulta con las partes interesadas tenga lugar durante todas las etapas del Plan de Continuidad del Negocio, por tal motivo la entidad vigilada debe desarrollar, de manera temprana, los planes para la comunicación y la consulta, dentro de los cuales debería contemplar los siguientes aspectos:

a) Definir la comunicación con los empleados de la entidad.

b) Definir la comunicación con partes interesadas externas.

c) Recibir, documentar y responder a las comunicaciones de todas las partes interesadas.

d) Alertar a los interesados que pudieran resultar afectados por un evento de interrupción real o potencial.

e) Disponer de los medios de comunicación durante un incidente.

f) Probar los medios de comunicación que serán utilizados durante el incidente.

La comunicación y la consulta deben facilitar los intercambios de información de manera veraz, pertinente, precisa y fácil de entender. (ISO, 2011).

4.4.6 Documentación del Plan

La documentación de la información evidencia el cumplimiento con los requisitos y el funcionamiento efectivo del Plan de Continuidad del Negocio.

El estándar internacional ISO 22301 recomienda que la documentación, relacionada con el Plan de Continuidad, incluya:

a) la política de continuidad del negocio;

b) los objetivos de la entidad relacionados con la continuidad del negocio y los objetivos del Plan de Continuidad del Negocio;

c) el análisis de impacto en el negocio (BIA);

d) la evaluación del riesgo;

e) las opciones de continuidad de negocio (estrategias de recuperación);

f) los programas de sensibilización;

g) los programas de entrenamiento;

h) el procedimiento de continuidad del negocio;

i) la programación de las pruebas del plan y los informes derivados;

j) los acuerdos de niveles de servicio durante un evento de no continuidad declarado.

La entidad vigilada por la Superintendencia Financiera de Colombia debe asegurar la integridad, la disponibilidad y confidencialidad de la información documentada.

Las entidades vigiladas por las SFC deben cumplir plenamente con todas las leyes y reglamentos pertinentes en relación con la retención de la información documentada y establecer, implementar y mantener los procesos necesarios para lograr el cumplimiento.

Por último el Plan de Continuidad de la entidad debe cumplir con los requisitos de información documentada que figuran a continuación.

a) Creación y actualización.

b) Control de versiones.

c) Control de Registros tales como actas de reuniones, informes de auditoría, formatos (de capacitación y entrenamiento), procedimientos (de movilización y retorno) y plantillas (BIA-Procedimientos-guiones de comunicación). (ISO, 2011).

4.5 OPERACIÓN

4.5.1 Planeación y control operacional

Las entidades vigiladas por la Superintendencia Financiera de Colombia deben determinar, planificar, ejecutar y controlar las actividades operativas necesarias para cumplir con su política y los objetivos de continuidad del negocio de manera que puedan satisfacer las necesidades y requisitos legales aplicables. Este aspecto guarda relación con el punto de la planeación establecido anteriormente en esta guía, en el que se definieron los objetivos del Plan de Continuidad del Negocio y los planes para alcanzarlos. En este punto la entidad vigilada deberá definir unos mecanismos de control, los cuales deben incluir:

a) Establecer criterios para los procesos relacionados con el Plan de Continuidad, tales como la cadena de abastecimiento, los servicios a contratar u outsourcing.

b) Implementar controles acordes a los criterios establecidos.

c) Mantener la información necesaria documentada de manera que se pueda demostrar que los controles están siendo efectivos.

Adicionalmente, la entidad vigilada deberá controlar los cambios planeados y revisar las consecuencias de cambios no intencionales, tomando acciones para mitigar cualquier efecto adverso, según sea necesario, además deberá asegurar el control de los procesos que tiene tercerizados en relación con el Plan de Continuidad del Negocio.

4.5.2 BIA y Evaluación de Riesgos

La Entidad vigilada deberá establecer, implementar y mantener un proceso documentado y formal para el análisis de impacto del negocio (BIA) y la evaluación de riesgos, que:

a) Establezca el contexto y los criterios para evaluar el impacto potencial de un evento disruptivo.

b) Tenga en cuenta los requisitos legales que debe cumplir la Entidad.

c) Incluya el análisis sistemático y la priorización del riesgo, y sus costos asociados

d) Defina los resultados requeridos desde el análisis de impacto del negocio y la evaluación de riesgos.

e) Especifique los requisitos para que esta información se mantenga actualizada y cumpla con los requisitos de disponibilidad, integridad y confidencialidad.

La entidad vigilada puede disponer de las diferentes metodologías existentes para el análisis de impacto del negocio y la evaluación de riesgos. (ISO, 2011)

- El análisis de impacto del negocio (BIA)

El objetivo del análisis de impacto sobre el negocio, conocido más comúnmente como BIA (Business Impact Analysis), es determinar el impacto de la interrupción de los procesos que son críticos para la continuidad de las operaciones del negocio.

El análisis de impacto del negocio deberá incluir los siguientes aspectos:

1) Identificación de actividades que soportan la provisión de productos y servicios;

2) Evaluación del impacto en el tiempo por no realizar tales actividades: Un evento que genera un impacto en los diferentes procesos, puede producir consecuencias negativas, que se miden de manera cuantitativa o cualitativa.

Para tal efecto, se debe analizar las interrupciones producidas, las mismas que pueden detallarse conforme a la siguiente manera.

i) Medición cuantitativa: se deberá efectuar las siguientes evaluaciones:

a) Análisis del tiempo de interrupción de los procesos.

b) Análisis del costo de interrupción medido por los recursos paralizados.

ii) Medición cualitativa:

a) Análisis de la pérdida de imagen de la institución por afección en los servicios

b) Análisis del impacto a través del "juicio de experto"

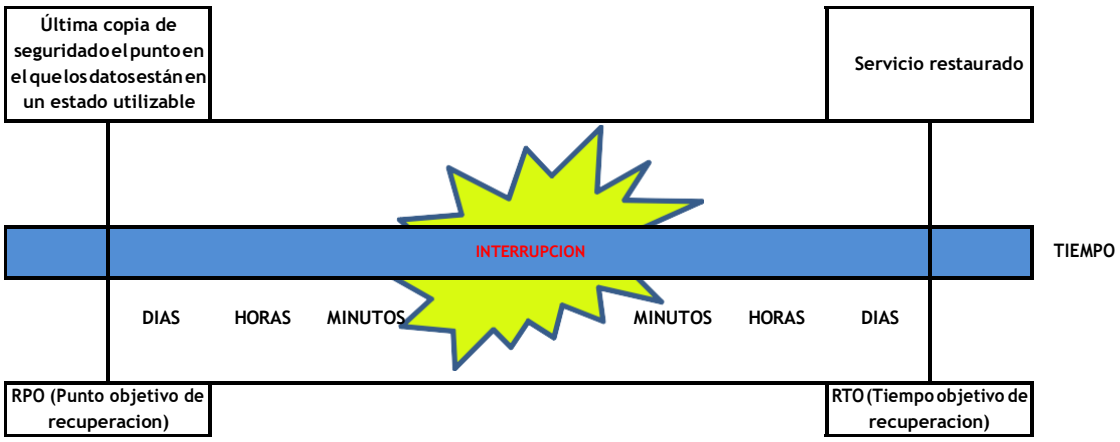
3) Establecer períodos de tiempo priorizados para reasumir tales actividades a un nivel mínimo establecido aceptable, considerando el tiempo en el cual el no reasumirlas se convierte en inaceptable:

a) Definir el tiempo de recuperación objetivo - RTO (Recovery Time Objetive): El RTO es el período de tiempo en el cual se debe restablecer el producto, servicio, actividad o recursos, después de un evento disruptivo.

b) Establecer el punto recuperación objetivo - RPO (Recovery Point Objetive): El RPO es el punto en el que la información, usada por una actividad crítica, debe ser restaurada para permitir que la referida actividad opere una vez que se reanude.

c) Identificar dependencias y los recursos de soporte para esas actividades, incluyendo proveedores, aliados y otras partes interesadas. (ISO, 2011)

Grafica 3: RPO/RTO



Fuente: www.macexperts.com

- Evaluación del riesgo

La entidad vigilada deberá establecer, implementar y mantener un proceso formal y documentado de evaluación del riesgo que de forma sistemática identifique, analice y evalúe el riesgo de incidentes disruptivos en la entidad. Este proceso puede ser elaborado de acuerdo con ISO 31000, la cual establece los principios y directrices para la gestión del riesgo.

Para la evaluación del riesgo la entidad vigilada deberá:

a) Identificar riesgos de interrupción de las actividades que la entidad ha catalogado como importantes, así como en los procesos, sistemas, información, personas, activos, aliados estratégicos y otros recursos que las soportan,

b) Analizar sistemáticamente el riesgo,

c) Evaluar cuáles riesgos de interrupción requieren medidas de tratamiento, de acuerdo con los objetivos de continuidad del negocio y el apetito de riesgo de la entidad.

Existen diferentes metodologías de Análisis de Riesgos tales como MARION, OCTAVE, MAGERIT, entre otras

Para el desarrollo de esta guía no se ha seleccionado ninguna metodología concreta, sino que se realiza una descripción general de los pasos que componen un Análisis de Riesgos.

- Identificación del riesgo

1) Determinar los procesos críticos del área a cargo, resultado que se obtuvo en la etapa de Análisis de Impacto del Negocio (BIA).

2) Establecer los recursos necesarios para la continuidad de los procesos críticos, que también se estimaron en la etapa de Análisis de Impacto del Negocio (BIA).

3) Describir las posibles amenazas que conlleven a una interrupción en la operación las cuales se deben evaluar identificando si tales situaciones pueden darse en el proceso analizado.

4) Determinar las vulnerabilidades que tiene el proceso para cada amenaza identificada.

Para identificarla es necesario responder esta pregunta: ¿Cómo puede ocurrir una amenaza? Al responderla se definen las distintas situaciones por las que puede materializar la amenaza.

5) Describir el riesgo contemplando las variables de amenaza y vulnerabilidad.

6) Enmarcar las vulnerabilidades en los siguientes factores de riesgo:

a) Recurso Humano

b) Infraestructura física

c) Tecnología.

d) Procesos.

e) Acontecimientos externos. (Del pino, 2007)

- Cálculo del riesgo inherente

Los riesgos se evalúan desde dos variables, la frecuencia y el impacto. Por la primera se entiende la posibilidad de ocurrencia del riesgo; esta puede ser medida en términos de probabilidad de ocurrencia, si se ha materializado (Por ejemplo: No. de veces / año), o de factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado. Por impacto se entiende como las consecuencias (económicas, operacionales, legales o reputacionales) que puede ocasionar a la entidad la materialización del riesgo.

Para el cálculo del nivel riesgo inherente se utilizarán las siguientes tablas con cinco niveles cada una, las cuales pueden verse a continuación.

Cada nivel de la tabla tiene asignado una escala, el número de eventos, la descripción del significado del nombre y un valor. Los valores asignados a los niveles de la frecuencia

(Probabilidad) se incrementan en forma lineal, igualmente, se utiliza esta premisa para los valores asignados a los niveles de las escalas de Impacto. (Mejía, 2006).

Tabla 4 Valoración de la frecuencia

ESCALA	NUMERO DE EVENTOS	DESCRIPCIÓN	VALORACIÓN
Improbable	Una vez en más de un año	El evento puede ocurrir solo bajo circunstancias excepcionales	1
Remota	Entre una y 5 veces al año	Su ocurrencia es poco probable	2
Ocasional	Entre 6 y 11 veces al año	Podría ocurrir en determinados momentos o circunstancias y con frecuencia baja	3
Frecuente	Entre 11 y 15 veces al año	Podría ocurrir en determinados momentos o circunstancias y con frecuencia alta	4
Constante	Más de 15 veces al año	Podría ocurrir en cualquier momento y en cualquier circunstancia y con frecuencia alta	5

Fuente: Elaboración propia

Tabla 5 Valoración del impacto

ESCALA	LEGAL	REPUTACIONAL	ECONÓMICO	OPERACIONAL	VALORACIÓN
Insignificante	Multas, gastos jurídicos e indemnizaciones menores al 1% del patrimonio.	Situaciones que no trascienden a los medios informativos	Pérdidas hasta de 5.000.000	Interrupción de la operación por menos de 4 horas	1
Moderado	Multas, gastos jurídicos e indemnizaciones entre el 1% y el 2% del patrimonio.	Aviso sorpresivo de prensa u otro medio masivo.	Pérdidas entre 5.100.000 y 10.000.000	Interrupción de la operación entre 5 horas y un día	2

ESCALA	LEGAL	REPUTACIONAL	ECONÓMICO	OPERACIONAL	VALORACIÓN
Grave	Multas, gastos jurídicos e indemnizaciones entre el 3% y el 4% del patrimonio.	Crítica de organismos de control o clientes en medios masivos de comunicación	Pérdidas entre 10.100.000 y 50.000.000	Interrupción de la operación entre un día y 5 días	3
Critico	Multas, gastos jurídicos e indemnizaciones entre el 5% y el 10% del patrimonio actual de la Entidad.	Divulgación de eventos y/o investigación por organismo regulador dado a conocer al público	Pérdidas entre 50.100.000 y 100.000.000	Interrupción de la operación entre 6 días y 10 días	4
Catastrófico	Multas, gastos jurídicos e indemnizaciones mayores 10% del patrimonio actual de la Entidad.	Pérdida de confianza por parte del público, intervención de entidades competentes.	Pérdidas por más de 100.000.000	Interrupción de la operación por más de 10 días	5

Fuente: Elaboración propia

Habiendo valorado tanto la frecuencia y el impacto del riesgo, los dos puntajes son multiplicados para dar el puntaje de riesgo Inherente. Dado que tanto la frecuencia como el impacto son calificados de 1 a 5, el puntaje de riesgo inherente máximo es 25 y el mínimo es 1. (Mejía, 2006).

El riesgo inherente se ubica en los siguientes niveles de riesgo

Tabla 6 Niveles de riesgo/Puntaje

NIVEL DE RIESGO	DESCRIPCIÓN	PUNTAJE
Bajo	Si el riesgo se ubica en el rango Bajo significa la Entidad asumirlo, es decir, el riesgo se encuentra en un nivel que puede aceptarlo sin necesidad de tomar otros controles diferentes a los que se poseen	1 - 2
Medio	Si el riesgo se ubica en el intervalo Medio implica que se deben acometer acciones de reducción de daños y especificar las responsabilidades de su implantación y supervisión cuando así se requiera	3 - 6
Alto	Si el riesgo se ubica en el intervalo Alto significa que el riesgo puede generar pérdidas que afecten las utilidades de la entidad, pero se mantiene la continuidad del proceso productivo por tanto se deben adoptar medidas para llevar los Riesgos a la Zona Bajo o Moderado, en lo posible.	8 - 12
Extremo	Si el riesgo se ubica en el rango Extremo se debe eliminar la causa que genera el riesgo en la medida que sea posible, de lo contrario se deben implementar controles de prevención para evitar la Frecuencia del riesgo, de Protección para disminuir el Impacto o compartir o transferir el riesgo si es posible a través de pólizas de seguros u otras opciones que se encuentren disponibles.	15 - 25

Fuente: Elaboración propia

- Evaluación de los controles

Este proceso permite evaluar todos los controles asociados a las vulnerabilidades identificadas, garantizando a la Entidad que se apliquen los tipos y niveles adecuados de control para poder dar un adecuado tratamiento al riesgo.

Los criterios de evaluación del control son: Documentado, Aplicación y Efectividad, a los cuales se les ha asignado un peso de 20, 30 y 50 puntos respectivamente sobre 100.

El criterio “Documentado” es calificado teniendo en cuenta cuatro aspectos:

a) Control no documentado, Puntaje 0.

b) Control documentado, Puntaje 8.

c) Control aprobado, Puntaje 8.

d) Control divulgado, Puntaje 4.

El criterio “Aplicación” es calificado teniendo en cuenta los siguientes aspectos:

a) El control nunca se aplica, Puntaje 0.

b) Se aplica a discreción, Puntaje 10.

c) Se aplica siempre, Puntaje 30.

El criterio “Efectividad” es calificado teniendo en cuenta los siguientes aspectos:

a) Baja, Puntaje 0.

b) Media, Puntaje 10.

c) Alta, Puntaje 30.

d) Muy alta. Puntaje 50.

Dependiendo si el control afecta frecuencia o impacto desplaza en la matriz de calificación, evaluación y respuesta a los riesgos.

Tabla 7 Calificación del control

RANGO DE CALIFICACIÓN DE LOS CONTROLES	DISMINUCIÓN FRECUENCIA/IMPACTO
0 - 50	0
51 - 75	1
76 - 100	2

Fuente: Elaboración propia

Cuando una vulnerabilidad tiene varios controles que mitigan el factor de frecuencia, éstos se agrupan y se toma el valor más alto de las calificaciones obtenidas de los controles. De igual manera se procede cuando una vulnerabilidad tiene varios controles que mitigan el impacto. (ICITEX, 2013)

- Cálculo del riesgo residual

Luego de la valoración de los controles se identifica el efecto de mitigación en frecuencia e impacto del riesgo, y se multiplican los nuevos valores de la frecuencia y el impacto para obtener el puntaje de riesgo residual, posteriormente se ubica el nuevo puntaje en los siguientes niveles de riesgo, teniendo en cuenta que por cada nivel de riesgo se debe adoptar una medida de tratamiento:

Tabla 8 Niveles de riesgo/Medidas de tratamiento

NIVEL DE RIESGO	DESCRIPCIÓN	PUNTAJE	MEDIDAS DE TRATAMIENTO
Bajo	Si el riesgo se ubica en el rango Bajo significa la Entidad asumirlo, es decir, el riesgo se encuentra en un nivel que puede aceptarlo sin necesidad de tomar otros controles diferentes a los que se poseen	1 - 2	aceptar

Medio	Si el riesgo se ubica en el intervalo Moderado implica que se deben acometer acciones de reducción de daños y especificar las responsabilidades de su implantación y supervisión cuando así se requiera	3 - 6	prevenir, proteger, retener, transferir
Alto	Si el riesgo se ubica en el intervalo Alto significa que el riesgo puede generar pérdidas que afecten las utilidades de la entidad, pero se mantiene la continuidad del proceso productivo por tanto se deben adoptar medidas para llevar los Riesgos a la Zona Bajo o Moderado, en lo posible.	8 - 12	prevenir, proteger, transferir
Extremo	Si el riesgo se ubica en el rango Extremo se debe eliminar la causa que genera el riesgo en la medida que sea posible, de lo contrario se deben implementar controles de prevención para evitar la Frecuencia del riesgo, de Protección para disminuir el Impacto o compartir o transferir el riesgo si es posible a través de pólizas de seguros u otras opciones que se encuentren disponibles.	15 - 25	evitar, prevenir, proteger, transferir

Fuente: Elaboración propia

- Tratamiento del riesgo residual

Una vez identificados y cuantificados los riesgos, así como el impacto que tienen para la entidad, se analizan y se establecen las medidas para el tratamiento de los riesgos

El tratamiento de riesgos consiste en seleccionar y aplicar las medidas más adecuadas, con el fin de poder modificar el riesgo, para evitar daños para la Entidad.

El tratamiento del riesgo debe garantizar como mínimo:

a) Un funcionamiento efectivo y eficiente de la entidad.

b) Controles internos efectivos.

c) Conformidad con la normatividad y reglamentos vigentes.

El tratamiento de los riesgos conlleva elegir alguna de las siguientes alternativas:

Evitar: Eliminar su frecuencia o disminuir totalmente su impacto. Para ello se debe eliminar la actividad que genera el riesgo o reubicar los recursos amenazados donde se elimina su nivel de exposición y se precisan medidas de protección extremos.

Prevenir: La prevención trabaja con la anticipación, es necesario vislumbrar los eventos que pueden suceder y establecer políticas, normas, controles y procedimientos conducentes a que el evento no ocurra o disminuya su frecuencia. La prevención actúa sobre las causas de los riesgos.

Proteger: Es la acción en el momento del peligro o la presencia del riesgo. Esta se logra a través del diseño y aplicación de políticas, normas y procedimientos, conducentes a disminuir la intensidad o el impacto negativo sobre los recursos amenazados, que generan los riesgos en caso de ocurrencia. La protección actúa sobre los efectos de los riesgos.

Aceptar: Tomar esta medida significa que no es necesario desarrollar medidas adicionales de prevención o protección del riesgo analizado, porque su evaluación, desde el punto de vista de frecuencia y de impacto, da como resultado un riesgo poco representativo, esto es, su ocurrencia no tendría un efecto significativo o la posibilidad de que se presente es muy remota. Estos riesgos aceptados deben ser revisados periódicamente dadas las circunstancias cambiantes del entorno y de la misma Entidad.

Transferir: Aquí participa otra parte que asume o comparte alguna parte del riesgo. Entre los mecanismos se encuentran el uso de contratos, acuerdos de seguros y estructuras organizacionales, tales como la sociedad o las alianzas estratégicas.

Retener: Con la retención se decide afrontar las consecuencias de los riesgos en forma planeada a través de la creación de un fondo, previo el diseño de alternativas que faciliten responder ante ellos.

Basadas en las opciones de tratamiento anteriormente enunciadas, se seleccionan los controles

apropiados que permitan disminuir su frecuencia y/o impacto en caso de que se materialice. (Mejía, 2006)

- Monitoreo de los riesgos de continuidad

Se realiza seguimiento a los riesgos y la efectividad de los controles y planes de acción para determinar el nivel de exposición frente al aspecto de disponibilidad de los elementos que se requieren para la continuidad del negocio. (ISO, 2009)

4.5.3 Definición de la estrategia del Plan de Continuidad del Negocio

Las estrategias de continuidad del negocio son las acciones que se deben tomar con el objetivo de restablecer las operaciones del negocio, en el plazo determinado, una vez que ocurra alguna interrupción o falla en los procesos o funciones críticas (ICITEX, 2013)

- Determinación y selección de la estrategia

La determinación y selección de la estrategia deberá estar basada en los resultados del análisis de impacto de negocios y de la evaluación del riesgo.

Es necesario identificar las diferentes estrategias de continuidad y seleccionar las más adecuada para que le permita a la entidad:

a) Proteger, estabilizar y recuperar las actividades críticas, así como sus dependencias y recursos de apoyo

b) Mitigar, responder y administrar los impactos del evento de interrupción.

Las diferentes situaciones para las cuales se deben definir estrategias de recuperación pueden ser:

1) Ausencia de personal: Se presenta cuando el ejecutor del proceso no puede asistir a trabajar para desarrollar las actividades propias de su cargo.

2) Sitio alterno: La alternativa de traslado del personal se presenta en el evento que los empleados no puedan acceder a las instalaciones de la entidad.

3) Fallas tecnológicas: se presenta cuando el hardware y/o software presenta fallas, o por interrupción prolongada de telecomunicaciones. (ICITEX, 2013)

- Establecimiento de los requisitos de recursos

Es muy importante que la entidad establezca los requisitos de recursos mínimos para implementar las estrategias seleccionadas.

Los recursos deberían establecerse bajo las siguientes premisas:

a) Que todos los recursos solicitados son los mínimos necesarios, ya que se trata de operación en un escenario de continuidad y no de una duplicación de las operaciones de la entidad.

b) Que los recursos en operación normal tienen un porcentaje de utilización menor al 100% de la capacidad instalada, por lo tanto los recursos de oficina pueden ser compartidos por varios funcionarios sin importar el proceso al que pertenecen.

Los tipos de recursos considerados deberán incluir como mínimo:

a) Personas.

b) Información y datos.

c) Infraestructura física y servicios asociados.

d) Instalaciones, equipos e insumos.

e) Sistemas de información y las comunicaciones.

f) Transporte.

g) Recursos económicos.

h) Proveedores.

4.5.4 Establecer e Implementar los procedimientos del Plan de Continuidad del Negocio.

La entidad deberá establecer, implementar, documentar y mantener procedimientos de continuidad del negocio para gestionar los eventos de interrupción y continuar sus actividades.

Los procedimientos deberán:

a) Establecer un protocolo apropiado de comunicaciones internas y externas específicas, efectivas, flexibles y con foco definido.

b) Establecer los pasos que serán ejecutados antes, durante y después de un evento de interrupción de las actividades críticas,

c) Adaptarse a las amenazas no previstas y las condiciones cambiantes internas y externas

- Estructura de respuesta a incidentes

La entidad deberá establecer, documentar e implementar procedimientos y una estructura organizacional para responder a un evento de interrupción usando personal con la necesaria responsabilidad, autoridad y competencia para manejar un incidente.

La estructura de respuesta deberá:

a) Identificar tolerancias en el impacto que justifican iniciar una respuesta formal,

b) Evaluar la naturaleza, extensión y el impacto del evento de interrupción.

c) Activar una respuesta apropiada de continuidad del negocio,

d) Tener procesos y procedimientos para la activación, operación, coordinación y comunicación de la respuesta al incidente

e) Tener recursos disponibles para soportar los procesos y procedimientos para administrar un evento de interrupción de tal manera que minimice su impacto.

f) Comunicar a las partes interesadas, autoridades, y a los medios de comunicación los diferentes aspectos relacionados con incidente. (ISO, 2011).

- Procedimiento de advertencia y comunicación

Es este punto es necesario que la entidad establezca, implemente, documente y mantenga procedimientos para detectar y monitorear, periódicamente, los eventos de interrupción. Así mismo estos procedimientos deben permitir la comunicación al interior de la entidad y la recepción, documentación y respuesta a las comunicaciones de las partes interesadas; los referidos procedimientos deben asegurar que los diferentes medios de comunicación se encuentren disponibles durante el evento de interrupción, y facilitar la comunicación estructurada con los servicios de emergencia (Bomberos, defensa civil, policía, entre otros). Por último los procedimientos deben permitir el registro de la información esencial del evento, las acciones y decisiones tomadas con respecto al mismo.

Es necesario que los procedimientos de advertencia y comunicación sean probados periódicamente. (ISO, 2011).

- Procedimiento para el Plan de Continuidad del Negocio

Es pertinente que la entidad vigilada implemente procedimientos documentados para responder a un evento de interrupción y como continuará o recuperará sus actividades críticas dentro de un de un tiempo determinado.

El procedimiento del plan de continuidad del negocio debe contener

a) Los roles y responsabilidades de las personas y equipos que intervienen el plan de continuidad del negocio.

b) Las actividades para ejecutar la respuesta al evento de interrupción.

c) Los detalles para gestionar las consecuencias inmediatas del evento teniendo en cuenta el bienestar de las personas, las opciones estratégicas, tácticas y operativas para responder al evento, y la prevención de mayores pérdidas o no disponibilidad de actividades críticas.

d) Los detalles de la manera en que se comunicará los aspectos del evento a los empleados y sus familiares, a las partes interesadas y a los servicios de emergencia;

e) Las actividades para detener la ejecución del Plan de Continuidad del Negocio una vez que finalice el evento de interrupción. (ISO, 2011).

- Procedimiento recuperación

La entidad vigilada debe contar con un procedimiento documentado para retornar al estado habitual de las actividades de negocio luego de un evento de interrupción.

El procedimiento de recuperación debe contener las actividades a nivel técnico y operativo para retornar a la normalidad, así mismo debe incluir al equipo responsable de ejecutar tales actividades. (ISO, 2011).

4.5.5 Pruebas

La entidad que se encuentre bajo la vigilancia de la Superintendencia Financiera de Colombia deberá ejercitar y probar sus procedimientos de continuidad del negocio para asegurar que son consistentes con los objetivos de continuidad establecidos.

Las pruebas que lleve a cabo la entidad deberán estar acordes con el alcance y objetivos del Plan de continuidad del negocio y partir de escenarios adecuados y planeados con objetivos claramente definidos.

Las entidades vigiladas deberán contar con un cronograma de pruebas, se recomienda que este cronograma incluya la frecuencia de las pruebas parciales y totales que se realizaran en el año. Estas pruebas y sus resultados deben ser documentados y comunicados, las fallas encontradas deben generar las respectivas actualizaciones y planes de mejora a los diferentes equipos de trabajo que conforman el Plan de Continuidad del Negocio.

Las pruebas deben cumplir con los siguientes objetivos específicos:

a) Verificar la totalidad y precisión del Plan.

b) Evaluar el desempeño del personal involucrado.

c) Evaluar la coordinación entre el personal involucrado, proveedores y terceros.

d) Identificar la capacidad de recuperar registros e información vital.

e) Medir el desempeño de los sistemas operativos.

Es importante que la entidad diseñe un plan de prueba el cual, tiene el objetivo de definir la prueba a efectuar dentro de la verificación y actualización permanente del Procedimiento de Continuidad de Negocio. Para esto se considera los escenarios de falla y frente a cada uno de estos define las diferentes pruebas requeridas para verificar la capacidad de recuperación de los procesos críticos y el cumplimiento de los tiempos objetivos de recuperación definidos en el Análisis de Impacto en el Negocio.

Una vez identificados los escenarios se establecen los aspectos mínimos del Plan de Pruebas que deben contemplar las siguientes tareas:

a) Seleccionar una fecha y hora para la prueba.

b) Definir los objetivos de la prueba, procesos o infraestructura a recuperar.

c) Identificar los empleados que participarán en la prueba.

d) Identificar el empleado que verificará la prueba.

e) Identificar proveedores que participaran en la prueba.

f) Asegurar el espacio físico para la prueba de acuerdo con los requerimientos mínimos.

g) Organizar los equipos de cómputo y otros de acuerdo con los requerimientos mínimos.

h) Familiarizar a los integrantes de equipos de recuperación con el Plan de Continuidad.

i) Definir el programa o agenda de la prueba.

j) Definir los procedimientos de recuperación de acuerdo con el Plan.

k) Distribuir los documentos (Manuales, guías, formatos, entre otros) de la prueba. (ISO, 2011).

4.6 EVALUACIÓN DEL PLAN

4.6.1 Monitoreo

El propósito del monitoreo es asegurar la efectividad del Plan de Continuidad del Negocio, para lograr la recuperación de actividades críticas dentro de los tiempos establecidos, asegurando la continuidad de los servicios y productos de la entidad vigilada

La entidad vigilada debe establecer los aspectos del Plan de Continuidad que serán monitoreados y medidos, los métodos de monitoreo y la periodicidad con la que se realizara el monitoreo.

El monitoreo al Plan de Continuidad del Negocio le permitirá a la entidad vigilada obtener:

a) Pruebas definidas y documentadas del monitoreo realizado al Plan de Continuidad del Negocio.

b) Detalle de los cambios realizados al Plan de Continuidad.

c) La verificación y validación del cumplimiento de las políticas y estrategias establecidas para el Plan de Continuidad del Negocio.

d) La identificación y seguimiento de los cambios en los sistemas y procesos críticos de la entidad.

e) La identificación de cambios en la legislación aplicable.

f) La revisión periódica del análisis de impacto (BIA) y de la evaluación de riesgos.

g) Retroalimentación acerca del entendimiento que tiene el personal, involucrado en la gestión del Plan de Continuidad del Negocio, con respecto a sus funciones y responsabilidades.

h) Seguimiento a las acciones preventivas y correctivas.

Los resultados del monitoreo deben registrarse y reportarse a las partes interesadas internas o externas que la entidad vigilada considere pertinentes. (ISO, 2011).

4.6.2 Auditoría del plan

El propósito de la auditoría es detectar desviaciones en el Plan de Continuidad del Negocio con el fin de brindar recomendaciones de acuerdo a estándares y mejores prácticas definidas.

La entidad que se encuentra bajo la vigilancia de la Superintendencia Financiera de Colombia deberá definir una periodicidad para realizar las auditorías al Plan de Continuidad del Negocio, y debe asegurar que estas evalúan la efectividad del Plan, conforme a lo establecido en los requisitos de la entidad, los requerimientos legales y los estándares internacionales.

La auditoría realizada al Plan de Continuidad, deberá estar basada en los resultados de la evaluación del riesgo de las actividades críticas del negocio o BIA y los resultados de auditorías anteriores.

La auditoría para el Plan de Continuidad debe seguir métodos y/o técnicas que optimicen este proceso. Algunas de estas técnicas y/o métodos pueden ser: La auto evaluación y las auditorías.

Los responsables del Plan de Continuidad del Negocio deberán asegurar que las acciones correctivas derivadas de la auditoría se adelanten de manera oportuna. Igualmente, deben realizar un seguimiento a las acciones correctivas con el ánimo de detectar sus modificaciones o actualizaciones, y deberán reportar los resultados de este seguimiento a las instancias pertinentes.

Cabe anotar que el Plan de Continuidad del Negocio puede ser auditado por diferentes entes tanto internos como externos tales como, la auditoría interna, la Superintendencia Financiera de Colombia o la Revisoría fiscal. (ISO, 2011).

4.7 MEJORAMIENTO DEL PLAN

4.7.1 Acciones preventivas y correctivas

Las acciones correctivas y preventivas son unas herramientas básicas para la mejora continua del Plan de Continuidad. El objetivo de estas acciones es eliminar causas reales y potenciales de problemas o incumplimientos, evitando que estos vuelvan a repetirse. Una acción correctiva se inicia cuando se presenta un incumplimiento de un requisito específico del Plan de Continuidad, mientras que la acción preventiva se entenderá como un incumplimiento potencial que aún no ha ocurrido pero, se tienen fuertes indicios de que podría suceder.

Es recomendable que la Entidad vigilada establezca y documente un procedimiento para la implementación de acciones correctivas y preventivas, este procedimiento deberá describir como mínimo las siguientes actividades:

a) Identificación de incumplimientos, reales o potenciales, del Plan de Continuidad del Negocio.

b) Definición de causas del incumplimiento real o potencial.

c) Evaluación la necesidad de las acciones correctivas o preventivas.

d) Definición e implementación de las acciones correctivas o preventivas.

e) Registrar e informar los resultados de las acciones emprendidas.

- Acción correctiva y acción preventiva: enfoque por procesos (PHVA)

El procedimiento para la implementación de las acciones correctivas puede seguir el ciclo PHVA también conocido como ciclo Deming, el cual considera las siguientes fases

Actuar: Identificar e implementar las acciones necesarias para alcanzar los resultados planificados y la mejora continua de los procesos de acciones correctivas y preventivas.

Planear: Decidir el cómo se va hacer, es decir metodologías, registros, puntos de verificación y control. En esta etapa también es necesario establecer procedimientos documentados para acciones correctivas y preventivas.

Hacer: Implementar "el cómo se va hacer", cuando se identifique incumplimiento real o potencial.

Verificar: Realizar el seguimiento, la medición y el análisis de los procesos de Acciones correctivas y preventivas. (ISO, 2000)

4.7.2 Mejoramiento continuo

En este punto la entidad vigilada por la Superintendencia Financiera de Colombia debe mejorar de manera continua la idoneidad, suficiencia y efectividad del Plan de Continuidad del Negocio.

Es necesario que la entidad vigilada defina un proceso continuo mediante el cual se establezcan objetivos y oportunidades de mejora a través del uso de los hallazgos y recomendaciones de la auditoría, los resultados de las acciones correctivas y preventivas u otros medios.

El proceso para administrar la mejora continua del Plan de Continuidad debe considerar como mínimo los elementos siguientes:

a) Administración del cambio en la entidad: Considerar todos los cambios que modifiquen la estructura del Plan de Continuidad del Negocio tales como cambios en el personal, cambios en los procesos de negocio, cambios de la plataforma de TI, entre otros.

b) Pruebas del Plan de Continuidad: A partir de las pruebas se deberá documentar los resultados de los mismos y desarrollar procedimientos para la actualización inmediata de todos los procesos y toda la documentación que se vean afectados.

c) Revisión constante. Los responsables del Plan de Continuidad del Negocio mantendrán una vigilancia constante sobre el negocio para identificar eventuales cambios que desencadenen un proceso de actualización del Plan de Continuidad del Negocio.

En este punto también es posible utilizar el ciclo PHVA ajustándolo a las particularidades del proceso de mejora continua. De manera resumida, el ciclo PHVA se puede describir así:

Planear: Establecer los objetivos y procesos necesarios para obtener los resultados, de conformidad con los requisitos de las parte interesadas y las políticas de continuidad de la entidad.

Hacer: Implementar procesos para alcanzar los objetivos de continuidad.

Verificar: Realizar seguimiento y medir los procedimientos en relación con las políticas, los objetivos y los requisitos de continuidad, reportando los resultados alcanzados.

Actuar: Realizar acciones para promover la mejora del desempeño del (los) procedimiento(s) de continuidad. (ISO, 2000).

4.8 BENEFICIOS DE CONTAR CON UN PLAN DE CONTINUIDAD DEL NEGOCIO

La implementación de un Plan de Continuidad del Negocio trae múltiples beneficios para la entidad dentro de los cuales se listan:

a) La alineación de los objetivos de continuidad con los objetivos de entidad.

b) La obtención de una ventaja competitiva frente a la competencia.

c) El aumento de la confianza por parte de los clientes.

d) El establecimiento del costo aproximado de las pérdidas, al no poder ejecutar un proceso crítico.

e) La clasificación de los activos para priorizar su protección en caso de una eventual interrupción.

f) El análisis de riesgo e impacto de los componentes que soportan al proceso.

g) La creación de una cultura de continuidad de negocio.

h) El cumplimiento de los requisitos legales o reglamentarios

i) La definición de una estructura organizacional para el Plan de Continuidad

j) La definición de estrategias de continuidad de negocio.

k) El diseño de medidas para reducción de riesgos identificados.

l) La elaboración y actualización de la documentación que contiene los aspectos del Plan de Continuidad.

m) El establecimiento de un plan de acción a corto, mediano y largo plazo, para darle continuidad a los procesos críticos de la entidad.

n) La identificación de los diversos eventos que podrían impactar las operaciones, las finanzas, los recursos humanos y tecnológicos y la reputación de la Entidad.

o) La identificación de los puntos más críticos y vulnerables de los procesos relevantes de la Entidad.

p) El conocimiento de los tiempos críticos de recuperación para volver a la situación anterior a la interrupción sin comprometer a la entidad.

q) El conocimiento de la situación actual de la entidad ante un evento de interrupción, mediante las pruebas del plan de continuidad.

r) El equilibrio entre las variables: costo, beneficio y riesgo.

s) El establecimiento de convenios con proveedores para la entrega de suministros, en tiempos acordados.

t) La prevención o mitigación de las pérdidas para la entidad en caso de un evento de interrupción.

u) La selección de los recursos mínimos a para cumplir con la estrategia de continuidad. (Leiva, 2008)

4.9 DIFICULTADES PARA IMPLANTAR UN PLAN DE CONTINUIDAD DEL NEGOCIO

La entidad puede afrontar algunos inconvenientes para implementar un Plan de Continuidad entre ellos podemos enumerar.

a) Las demoras en la toma de decisiones por parte de la entidad.

b) La falta de compromiso de la Dirección.

c) La falta de involucramiento del personal de la Entidad.

d) La falta de personal disponible y capacitado para asumir la responsabilidad de implementar el plan de continuidad.

e) Las limitaciones de presupuesto.

f) La pérdida de personal clave.

g) Planteamiento de los objetivos del plan de continuidad poco realistas o inalcanzables.

h) Falta de estabilidad de los procesos críticos de la entidad.

i) Reestructuración de la entidad.

j) Cambios en las prioridades de la entidad.

k) La resistencia al cambio. (Leiva, 2008).

CONCLUSIONES

De acuerdo con la normatividad vigente, las entidades vigiladas por la Superintendencia Financiera de Colombia deben tomar las medidas para controlar los riesgos inherentes a los que se ven expuestas, con el fin de disminuir la probabilidad de ocurrencia y/o el impacto en caso de que se materialicen tales riesgos. Una de estas medidas es el Plan de Continuidad del Negocio, el cual establece los procedimientos, los sistemas y los recursos necesarios para retornar y continuar la operación, en caso de un incidente de interrupción.

El Plan de Continuidad del Negocio permite mantener la opinión o el reconocimiento que tienen los distintos grupos de interés sobre el comportamiento de la Entidad.

El proceso de la Continuidad del Negocio debe contar con el apoyo de una estructura conformada por equipos de trabajo que busquen mitigar los riesgos y niveles de exposición en un evento interrupción de la operación. Ante una activación del Plan de continuidad de Negocio, estos equipos son los responsables de restablecer los procesos identificados como críticos en plazos no superiores a los que se definan en los tiempos objetivos de recuperación.

Es muy importante entender que un Plan de Continuidad del Negocio no sólo debe atender la recuperación de las instalaciones frente a un desastre. El Plan de Continuidad del Negocio, también debe contemplar las acciones preventivas de lugar. Para dicho efecto en todo Plan se debe, de manera regular, efectuar un análisis del riesgo que contemple la identificación de amenazas significativas que afecten las operaciones de la entidad, las vulnerabilidades y el grado de exposición al riesgo.

Las directivas de la Entidad son responsables de mantener un plan de continuidad de negocio que cubra los procesos críticos, en donde se definan controles para identificar y reducir riesgos, minimizar las consecuencias de los diferentes incidentes y para asegurar la

recuperación oportuna de las operaciones principales. Los sistemas de información que soportan los procesos críticos deben poseer planes de contingencia y recursos necesarios que aseguren la continuidad. Así mismo, todos los proveedores externos que participan del desarrollo de los procesos críticos de la Entidad deben contar con sus respectivos planes de continuidad debidamente documentados y probados de manera que se encuentren alineados con los objetivos de recuperación que se propone la Entidad.

RECOMENDACIONES

1. Se recomienda que la documentación relacionada con el Plan de Continuidad del Negocio sea revisada y actualizada por lo menos una vez al año o cada vez que se presenten cambios relacionados con las estrategias de recuperación, el personal, la tercerización de actividades críticas, el rediseño de procesos o aplicaciones, el lanzamiento de nuevos productos, las fusiones o adquisiciones, los cambios regulatorios significativos, los resultados de pruebas efectuadas y en general cualquier tipo de cambio que se considere pueda llegar a afectar la continuidad del negocio.

2. Es recomendable que las entidades vigiladas establezcan un plan de sensibilización y capacitación para transmitir los conceptos y procedimientos asociados al Plan de Continuidad del Negocio para que pase a ser parte de los valores y de las competencias de la Entidad. Esto permitirá que los empleados adopten y apliquen las prácticas de continuidad en su día a día. El plan de sensibilización y capacitación debería incluir la definición de unos objetivos, la identificación y análisis de la audiencia a involucrar, la definición de medios y contenidos, el diseño y desarrollo de material de apoyo y la ejecución de las sesiones de sensibilización y capacitación.

3. La alta dirección de la entidad debe adquirir un compromiso con el Plan de Continuidad del Negocio pues, de lo contrario la implementación de dicho plan puede tornarse en un proyecto más que se olvida con el tiempo.

REFERENCIAS

Agencia EFE. (2012). Cronología de atentados terroristas en Bogotá. El colombiano. Recuperado de http://www.elcolombiano.com.

Arboleda, A. (2013). Terremoto del Eje Cafetero: 14 años después. W Radio. Recuperado de http://www.wradio.com.co.

ASOBANCARIA. (2006). Guía para la elaboración de planes de contingencia. Recuperado de http://www.asobancaria.com/portal/pls/portal/docs/1/734047.PDF

Buitrago, C. (2009). Continuidad de negocio: estrategia para perdurar. Revistas Universidad Externado de Colombia, Recuperado de http://revistas.uexternado.edu.co/index.php/sotavento/article/view/1634/1473

CAJA COSTARRICENSE DE SEGURO SOCIAL. (2007). Manual para Elaborar un Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones. Recuperado de http://portal.ccss.sa.cr/portal/page/portal/GIT/Tab4/Tab2/TIC-GCN-0001-Guia_para%20Elaboracion_de_Planes_de_Continui.pdf

Del Pino Jiménez, L. (2007). Guía de Desarrollo de un Plan de Continuidad de Negocio. ¿Qué tan seguro está en su trabajo? Recuperado de http://www.criptored.upm.es/guiateoria/gt_m001r.htm

Finanzas personales. (2012) ¿Qué tan seguro está en su trabajo? Recuperado de http://m.finanzaspersonales.com.co

ICETEX. (2013). manual de administración del plan continuidad del negocio. Recuperado de https://www.icetex.gov.co/dnnpro5/LinkClick.aspx

ICONTEC (Ed.). (2011). Norma técnica colombiana – ISO 31000: Gestión del riesgo. Principios y Directrices. Bogotá.

INTECO. (2010). Guía práctica para PYMES: cómo implantar un Plan de Continuidad de Negocio. Recuperado de http://www.inteco.es/file/t2sHW92KsAV506ZWcHTKRg.

ISO (Ed.). (2011). Societal security — Business continuity management systems — Guidance. Ginebra

Martinez, J. (2006). El plan de continuidad de negocio: Guía práctica para su elaboración. Madrid, España: Ediciones Díaz de Santos S.A.

Leiva, A. (2008). Desarrollo del plan de continuidad del negocio para el departamento de TI de una empresa farmacéutica. Recuperado de http://bibdigital.epn.edu.ec/handle/15000/952

Mejía, R. C. (2010). Administración de riesgos un enfoque empresarial. Medellín, Colombia: Fondo editorial Universidad EAFIT.

Ochoa, M. (2001). Metodología para el desarrollo del plan de continuidad de riesgo operativo del banco ecuatoriano de la vivienda. Recuperado de http://repositorio.uasb.edu.ec/bitstream/10644/2786/1/T0990-MFGR-Ochoa-Metodolog%C3%ADa%20para.pdf

Rodríguez, E & Correa, D. (2009). PLAN DE CONTINUIDAD BS 25999 Recuperado de http://www.sisteseg.com/files/Microsoft_Word_-_Articulo_BS_25999_DEF1.pdf.

Servat, A. (2012) nuevo estándar internacional en continuidad del negocio ISO 22301:2012.

SGS América Latina. (2013). ISO 22301: Sistemas de Gestión de Continuidad del Negocio. Recuperado de http://www.sgs-latam.com/es-ES/Local/LATAM/News-and-Press-Releases/2013/03/ISO-22301-Sistemas-de-Gestion-de-Continuidad-del-Negocio.aspx.

SUPERINTENDENCIA FINANCIERA DE COLOMBIA. (2007). Capitulo XXIII Reglas relativas a la administración del riesgo operativo. Recuperado de http://www.superfinanciera.gov.co/Normativa/NormasyReglamentaciones/cir100/cap23_riesgo-opera.doc

SUPERINTENDENCIA FINANCIERA DE COLOMBIA. (2013). Historia de la Superintendencia Financiera de Colombia. Recuperado de http://www.superfinanciera.gov.co/NuestraSuperintendencia/historia.doc

ANEXOS

ANEXO I

Amenazas y vulnerabilidades

El riesgo puede ser definido como “la probabilidad de que una amenaza pueda explotar una vulnerabilidad y causar daño a una entidad. Por otro lado una amenaza puede definirse como el intento de hacer daño, las amenazas pueden clasificarse en humanas, tecnológicas o de infraestructura. Las vulnerabilidades son condiciones de la entidad que pueden hacer que una amenaza se manifieste. En importante entender que una amenaza por sí sola no causa daño, es una simple intención de producir daño. El riesgo se presenta cuando la amenaza y la vulnerabilidad se combinan. La gestión del riesgo en el contexto del Plan de Continuidad Negocio trata los conceptos presentados, para determinar luego, la exposición al riesgo que tiene la empresa e identificar los escenarios de amenazas y vulnerabilidades a los que la entidad está sujeta. A continuación se presentan un listado de las posibles amenazas y vulnerabilidades que deberían tenerse en cuenta en el análisis de riesgos de la continuidad del negocio, cabe anotar que este listado es meramente ilustrativo pues, la entidad puede considerar las amenazas y vulnerabilidades que considere:

Tabla 9 Amenazas y vulnerabilidades

Tipo de amenaza	Amenaza	Vulnerabilidad
Tecnológica	Ataque terrorista / vandalismo	Ubicación no apropiada sitios deficientes en seguridad
		Ausencia/ Falla de Planes de Contingencia
	Falla del sistema de respaldo de suministro eléctrico	Falta de mantenimiento planificado
		Administración inadecuada
	Falla del aire acondicionado	Falta de mantenimiento planificado
		Administración inadecuada
	Ataque informático	Falta/Falla de gestión de herramientas para detección y prevención de código malicioso

		Falta de gestión de control de cambios
		Administración inadecuada de equipos
		Falta / pruebas insuficientes de copias de respaldo
		Falta / Falla de gestión de acceso de usuarios
	Condiciones ambientales adversas (condiciones extremas de polvo, temperatura, humedad, inundación, incendio)	Ubicación en sitios deficientes en seguridad
		Falta de mantenimiento -físico
	Error operacional del personal que administra el recurso	Falta/Desactualización de documentación
		Falta/Falla de capacitación de usuarios
	Falla del hardware	Falta/ Gestión inadecuada de herramientas y logs de auditoria
		Condiciones de instalación y operación inadecuada (eléctrico, instalación de componentes)
		Falta de mantenimiento - lógico o físico
		Ausencia/ Falla de Planes de Contingencia
		Obsolescencia del Hardware
		Falta/ falla de los equipos de soporte
		Falta / Falla de gestión de capacidad
	Robo o pérdida del hardware (Aplica para TI y áreas de negocio)	Ubicación en sitios deficientes en seguridad
		Falta/Falla de procedimiento para el retiro de equipos
		Falta de seguridad en el manejo de equipos fuera de la organización
		Falta/Falla de concientización de usuarios
	Funcionamiento inadecuado del recurso (Aplica áreas de TI y áreas de usuario final)	Falta de verificación de criterios de aceptación de compra de componentes.
	Sobrecarga de voltaje	Falta/ falla de los equipos de soporte
		Condiciones de instalación y operación inadecuada (eléctrico, instalación de componentes)
	Ataque terrorista/vandalismo	Ausencia/ Falla de planes de contingencia
	Código malicioso	Administración de red inadecuada
	Daños accidentales	Ubicación en sitios deficientes en seguridad física (Sitios sin control de acceso adecuados).
	Daños accidentales	Falta/falla de políticas para el trabajo en áreas seguras
	Error operacional del personal	Falta/Desactualización de documentación
		Falta/Falla de capacitación de usuarios

		Falta/ falla de gestión de control de cambios
	Falla del medio de comunicación	Condiciones de instalación, mantenimiento y operación inadecuada
		Uso inadecuado de estándares de infraestructura del medio
		Falta / Falla de gestión de capacidad
	Plagas (roedores y cucarachas)	Falta de mecanismos para el control de plagas
		Falta de mantenimiento del entorno
	Pérdida de disponibilidad y/o disminución de la calidad del servicio	Falta / falla de un proceso de monitoreo del canal
		Falta / falla de gestión de capacidad
		Ausencia de un mecanismo de contingencia
		Falta / falla de gestión de cambios
	Uso inadecuado / no autorizado del recurso	Falta / falla de un proceso de monitoreo del canal
		Falta / Falla de gestión de acceso de usuarios
		Falta/falla de gestión sobre la infraestructura de red
	Errores Operacionales en la administración de la aplicación	Falta de capacitación del personal (aque administra la aplicación)
		Documentación de configuración inexistente o desactualizada
	Errores de Usuario Final	Falta de capacitación del personal
		Documentación inexistente o desactualizada
		Gestión de usuarios y privilegios inadecuada
	Ataques informáticos (virus, inyección de código, DOS, Troyanos, Puertas traseras, bombas lógicas, ataques a protocolos conocidos)	Ausencia de requerimientos de seguridad en el ciclo de desarrollo o adquisición de SW
		Fallas en el proceso de gestión de vulnerabilidades
		Falta de gestión de control de cambios
	Falla de la Aplicación	Especificaciones inadecuadas en el diseño e implementación de la aplicación
		Falta de gestión de control de cambios
		Falta de criterios/pruebas de aceptación
		Falta / pruebas insuficientes de copias de respaldo
		Deficiencias/ ausencia de buenas prácticas de desarrollo
		Esquemas / Contratos de mantenimiento y soporte inexistentes o inadecuados

		Ausencia de planes de mantenimiento de la aplicación.
		Fallas en el proceso de control de versiones
		Falta/falla de gestión de vulnerabilidades técnicas
		Ausencia/ Falla de Planes de Contingencia
		Falta o falla en la gestión de la capacidad de la aplicación
		Falta/Falla en la gestión de herramientas y logs de auditoría
	Manipulación no autorizada/inadecuada de la configuración de la aplicación	Segregación inadecuada de ambientes de producción, pruebas y desarrollo
		Falta / Falla de gestión de acceso de usuarios
		Falta/Falla en la gestión de herramientas y logs de auditoria
		Controles de acceso de usuario no adecuados.
		Falta / Inadecuada definición de Roles y Perfiles
	Violación de derechos de autor	Ausencia o inadecuados esquemas de licenciamiento
Humana	Ausencia repentina	Personal Insatisfecho / desmotivado
		Falta de un esquema de respaldo de funciones / conocimiento
	Coacción/extorsión al personal	Selección inadecuada de personal
		Falta/falla en segregación de funciones
	Ingeniería social	Falta de concientización en Seguridad de la Información
	Coacción al personal	Trabajo de terceros sin supervisión
		Falta de concientización de terceros
	Control inadecuado de servicios suministrados	Brechas en las obligaciones definidas en los contratos
		Contratación no adecuada de terceros
		Falta de requerimientos de seguridad en acuerdos contractuales
		Falta de auditorías del servicio prestado
		Ausencia de indicadores de gestión y seguimiento de planes de acción
	Error operativo en el proceso de selección y contratación de personal	Contratación no adecuada de terceros
	Acceso no autorizado (físico y lógico)	Falta de mecanismos de control de acceso físico
		Falta de definición de requerimientos de seguridad para el tercero
		Trabajo de terceros sin supervisión
	Uso no autorizado de la información y los recursos	Falta / falla de gestión de acceso a usuarios (del tercero)

		Falta de requerimientos de seguridad en acuerdos contractuales. (Horas de trabajo no compatibles, SLAs, propiedad intelectual, uso adecuado de los activos.)
		Falta / deficiencia en el procedimiento de identificación y clasificación de la Información.
		Ausencia de supervisión del trabajo de terceros
		Falta de concientización de terceros en seguridad de la información
	Robo de información sensible o crítica	Falta de requerimientos de seguridad en acuerdos contractuales
		Ausencia de supervisión del trabajo de terceros
	Incumplimiento de los acuerdos contractuales	Contratación no adecuada de terceros
		Falta de requerimientos de seguridad en acuerdos contractuales
		Falta de auditorías del servicio prestado
		Ausencia de indicadores de gestión y seguimiento de planes de acción
	Interrupción repentina en la prestación del servicio	Falta de un plan de continuidad del negocio del tercero
		Falta de un plan de continuidad al interior de la organización
Infraestructura	Fallas de infraestructura de servicios (eléctrico, agua, gas)	Falta de mantenimiento de la infraestructura de servicios
	Acceso no autorizado	Control de acceso inadecuado o inexistente
		Falla o falta de políticas de accesos a áreas seguras
	Incendio	Sistema de detección y extinción de incendios inadecuado
		Falta de mantenimiento de la infraestructura de servicios
	Inundación	Falta de mantenimiento de la infraestructura de servicios
		Ubicación inadecuada de tuberías de agua
		Falla / inexistencia de detectores de aniego
	Desastre natural (Terremotos, Huracanes, Tornados, deslizamientos, maremotos, erupciones volcánicas)	Protección Física Inadecuada
		Falta de un plan de continuidad
	Alteraciones de orden público	Protección Física Inadecuada
		Esquemas de vigilancia Inadecuados (Servicios de vigilancia , Plan de atención de incidentes)
	Acciones Terroristas (Vandalismo , Sabotajes , Bombas, atentados)	Protección Física Inadecuada
		Ubicación en zonas de alto riesgo

Fuente: ETEK