Universidad de Buenos Aires

Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo Final

Tema:

Plan de Continuidad del negocio (BCP)

Titulo:

Guía práctica para la elaboración del Plan de Continuidad del Negocio

Autor: Juan José Ortiz Vega

Tutor del Trabajo Final: Lic. Graciela Pataro

Año 2012

Cohorte 2011

DECLARACIÓN JURADA DE ORIGEN DE LOS CONTENIDOS

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y que se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual

Juan José Ortiz Vega

PASAPORTE.18.401.186 de Calarcá – Colombia

DNI. 94740246

RESUMEN

El presente trabajo se basa en la investigación y análisis de los procesos que debe tener un plan de continuidad del negocio en caso de alguna emergencia que afecte las principales actividades y procesos de la organización.

La perturbación de las actividades centrales de la empresa pueden ser originadas por distintas causas tales como: desastres naturales, errores humanos y fallas tecnológicas que impactarán de manera nefasta a los intereses de la organización si no posee un Plan de continuidad.

Para el desarrollo adecuado de este trabajo se pretende enfocar el mismo en el análisis y comparación de estándares internacionales como (**ISO/IEC 27001-2005, ISO/IEC 27002: 2007, NTC 5722, Nist 800-34, NFPA1600:2010 y ASIS SPC.1-2009**) para la implementación de un BCP[1], basándose en el análisis comparativo de las normativas antes mencionadas se pretende desarrollar una guía de implementación de un BCP donde se explicará de manera detallada y clara los principales pasos para el desarrollo de un plan de continuidad.

Como herramienta de trabajo para el desarrollo de este documento se toman como referencia normativas internacionales y el desarrollo de un cuadro comparativo para determinar sus similitudes y diferencias. Con este cuadro se pretende hallar las mejores acciones a tomar para el desarrollo de un BCP.

Finalmente como resultado de esta investigación y análisis se plantearan conclusiones al respecto y se mostrará una guía práctica de todos los pasos a desarrollar para obtener un óptimo desempeño del BCP que asegure la supervivencia del negocio de la organización.

[1] Siglas en inglés de Business Continuity Plan,

PALABRAS CLAVE

Plan de Continuidad del negocio, Continuidad, Estándares de seguridad, Seguridad de la información y Gestión de la seguridad de la información

TABLA DE CONTENIDO

INDICE DE ILUSTRACIONES

INDICE DE TABLAS

AGRADECIMIENTOS

Agradezco en primera instancia a Dios todo poderoso, ya que gracias a él pude llegar a este país y momento de mi vida y que sin su amparo y protección no lo hubiese logrado.

Agradezco a mis dos madres Lucy y Doris que siempre me apoyan en los pasos que doy hacia adelante, les doy las gracias por el amor y las bendiciones que a diario recibo desde la lejanía, las amo y espero que este trabajo les guste.

Agradezco a mi novia Laura, por estar día tras día apoyándome cuando más lo necesitaba, por su paciencia, por el amor y alegría que despierta en mí con su sonrisa.

Agradezco a mi tutora la Licenciada Graciela Pataro por su colaboración y formalidad en todo momento desde su primera clase, gracias.

Juan José Ortiz Vega

1. INTRODUCCION

El compromiso que tienen hoy las empresas con sus clientes de mantener el servicio activo cada día crece más y aun más los riesgos de no cumplir con esta responsabilidad. Mantener la promesa de servicio a los clientes ante eventos inesperados se ha vuelto un gran desafío y para eso las entidades han tomado la decisión de aplicar como contramedida a estos riesgos el desarrollo de Planes de Continuidad para garantizar el servicio continuo de sus actividades.

Aunque los eventos de interrupción y falla no son tan frecuentes en el diario trabajo de las empresas, estos ocurren y pueden generar pérdidas para las organizaciones. Los factores que amenazan la operación de los servicios empresariales provienen de fuentes internas y externas que pueden generar impacto sobre las personas, la tecnología, los procesos o las instalaciones de las mismas.

La gestión y el desarrollo de un plan de continuidad buscan preparar a los integrantes de la organización en la reacción oportuna y en el menor tiempo posible a eventos que impacten en gran medida a las funciones vitales de la organización y la seguridad de la información, todo esto con el fin de mantener con la ayuda de estrategias de seguridad de la información, apoyo continuo de la gerencia, políticas de seguridad, controles activos de los procesos y sensibilización del personal de la empresa, la continuidad y la confianza de los clientes, además de evitar posibles crisis en la Organización

1. OBJETIVOS

1.1. Objetivo General

Desarrollar una guía práctica para la elaboración del plan de continuidad del negocio tomando como referencia los elementos presentes en las normas Nist 800-34, ISO27001/2, NTC 5722, NFPA1600:2010 y ANSI ASIS SPC.1-2009

1.2. Objetivos Específicos

- Analizar los elementos que contemplan un plan con continuidad del negocio.
- Establecer diferencias entre las normativas Nist 800-34, ISO27001/2, NTC 5722, NFPA1600:2010 y ANSI ASIS SPC.1-2009 con el desarrollo de un cuadro comparativo de las mismas.
- Analizar los riesgos que requieran la activación del plan de continuidad del negocio.
- Desarrollar una guía práctica basada en el cuadro comparativo entre las normativas antes nombradas.

2. MARCO TEORICO

2.1. ¿Qué es un Plan de Continuidad del Negocio?

Un plan de continuidad del negocio (Bussines Continuity Plan – BCP) se puede definir como la identificación y protección de los procesos del negocio considerados críticos para sostener un desempeño aceptable. Funciona mediante la identificación de potenciales amenazas, la definición de estrategias para su eliminación, minimización y la preparación de procedimientos para asegurar la subsistencia de los mismos al momento de concretarse dichas amenazas. [1]

Un BCP es una concepción gerencial que se basa en el entendimiento de los procesos de la organización, de los elementos que soportan su operación y el riesgo que representa la paralización parcial o total de los mismos en términos de pérdidas de oportunidades de negocio. [1]

Los planes de continuidad del negocio no solo se desarrollan para enfocarse en la prevención de los riesgos que afecten las actividades de la organización, ya que es imposible asegurarse que todos los puntos de falla fueron identificados y donde hay riesgos que son imposibles de prevenir o no son rentables para la empresa.[1]

2.2. ¿Cuáles son algunas de las conocidas Normativas existentes para establecer un BCP?

- Nist 800-34 (Contingency Planning Guide for Information Technology Systems)
- ISO27001 (Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos).
- ISO27002 (Tecnología de la información - Código de buenas prácticas para la gestión de la seguridad de la información). NTC 5722 (Norma Técnica Colombiana 5722 Gestión De La Continuidad Del Negocio Requisitos).

- NFPA1600:2010 (Standard on Disaster/Emergency Management and Business Continuity Programs).
- ANSI ASIS SPC.1-2009 (Organizational Resilience: Security, Preparedness, And continuity management systems –Requirements with guidance for use)

2.3. ¿Cuál es la metodología usada para el desarrollo del BCP?

2.3.1. CICLO DE DEMING (PDCA)

Para la elaboración de un plan de continuad del negocio se sugiere usualmente tomar como referencia la técnica desarrollada por el Dr. Williams Edwards Deming que se centra en la mejora continua de los procesos de la organización y que se basa en cuatro pasos fundamentales que ayudan a la evolución adecuada de los procesos de implementación de cualquier proyecto. [2]

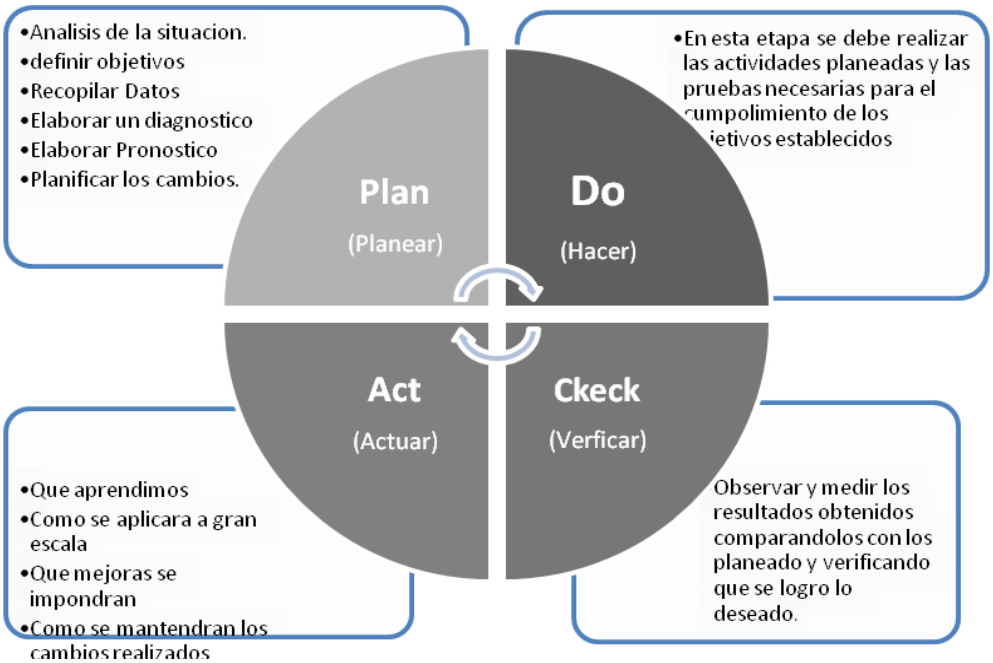

Ilustración 1: Ciclo de Deming

Fuente. Dibujo del autor del presente trabajo

Plantilla de seguimiento de PDCA					Fecha		Hora	
					Área			
					Líder de Área			

Problema / Mejora	Causa	Acción	Responsable	Fecha	Plan	Hacer	Verificar	Actuar

Tabla 1. Plantilla Ciclo De Deming PDCA (Fuente. Autor)

Las siglas de este ciclo (PDCA) corresponden a las palabras en Inglés Plan, Do, Check, Act que para este trabajo se utilizaran las equivalentes al español que serian Planear, Hacer, Verificar; Actuar. [2]

La interpretación y el objetivo de esta metodología seria:

- **Planear**
  - Planear las actividades a realizar, investigar las causas de los problemas.
  - Observar si las personas que actualmente componen la organización ya gestionaron una solución y observar cual fue la solución y tomar registro de ella.

- **Hacer**
  - Formar un grupo de trabajo de personal de varias áreas de la empresa
  - Poner en marcha lo planeado con antelación.
  - Se realizaran las pruebas necesarias para comprobar las causas del problema.
  - Se capacitara al grupo de trabajo para que gestione los problemas de la mejor manera.
  - Se implementara las soluciones determinadas sobre los problemas encontrados en la planificación.

- **Verificar**
  - Posteriormente se verifica que las actividades que se pusieron en marcha si dieron los frutos deseados.
  - Se analizaran las situaciones encontradas y tratadas.
  - Se tomara nota de los resultados, se hará un diagnostico de lo encontrado y se planificaran cambios.
- **Actuar**
  - Se aplican las mejoras respectivas a los errores encontrados durante todo el proceso y de esta forma al volver a empezar el ciclo.
  - Se tomaran las mejoras como ítems iníciales para la mejora en la calidad de las operaciones de las actividades siguientes.

Como parte fundamental para establecer este plan se recomienda el desarrollo de una guía aplicada al concepto de Ciclo De Deming para controlar y documentar lo encontrado y los pasos para su solución y análisis **(Ver Anexo 1)**.

3. ETAPAS DEL PLAN DE CONTINUIDAD DEL NEGOCIO

Tras el análisis de la comparación de las normativas del Anexo 1, se determinó que el Plan de Continuidad del Negocio BCP se desarrolla bajo las premisas de cuatro etapas de desarrollo:

3.1. ETAPA 1. Análisis Del Negocio Y Evaluación De Riesgos: Según el Ciclo de Deming esta será la etapa de planeación (PLAN). En esta etapa se conocerá de manera detallada como es el negocio y los riesgos que lo afectarían.

3.2. ETAPA 2. Estrategias para la continuidad y Creación de Políticas: En esta etapa se desarrollan las estrategias y según el Ciclo de Deming seria la etapa de hacer(DO)

3.3. ETAPA 3. Desarrollo Del Plan de Continuidad: Tras crear políticas y estrategias para el plan se desarrolla el BCP se da pie al desarrollo del mismo y estaría ubicado en la etapa de hacer(DO) del ciclo de Deming

3.4. ETAPA 4. Pruebas y Mantenimiento: Ubicándonos en el ciclo de Deming serían las etapas de Verificar (CHECK) y Actuar (ACT), que consisten en tomar los procesos realizados durante el ciclo de vida de la actividades del BCP y verificar la eficacia de lo realizado. Tras realizar las revisiones necesarias se tomarán los resultados obtenidos y se plantearán las mejoras o cambios a lo que se está haciendo que ayuden a la mejora continua de la organización y del BCP.

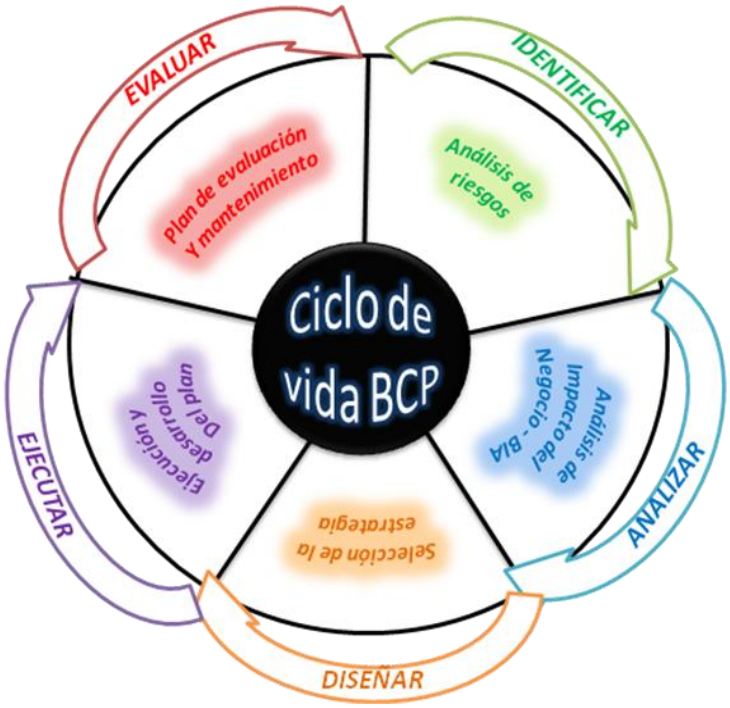

Ilustración 2 Ciclo de Vida del BCP

Fuente: Dibujo del autor del presente trabajo

Estas etapas son fundamentales para el desarrollo del BCP y para lograr un perfecto entendimiento de los implementadores del mismo, a continuación se expondrá de manera detallada cada etapa para ampliar la idea de las mismas.

4. GUÍA PRÁCTICA PARA LA ELABORACIÓN DEL PLAN DE CONTINUIDAD

4.1. ETAPA 1. Análisis Del Negocio Y Evaluación De Riesgos

Antes de empezar con el desarrollo del plan es fundamental definir los objetivos y el alcance de las actividades y procesos de la organización ya que es importante destacar los que se posee en la actualidad (Personal, procesos, recursos, etc.) lo que se desea hacer y hasta dónde se puede llegar con el plan.

4.1.1. Obtener apoyo de la gerencia

Obtener el apoyo de la gerencia es fundamental para el desarrollo de cualquier actividad dentro de la organización. Dar ideas claras y mostrar los beneficios de los resultados esperados ayudarán a que los directivos apoyen de manera continua el desarrollo e implementación del BCP. Los directivos deben estar conscientes de todas de las actividades a realizar para mitigar las amenazas y riesgos que lograrán una recuperación del negocio de forma rápida y efectiva.

4.1.2. Funciones, procesos y áreas de la organización.

Definir cuáles serán las funciones primordiales, los procesos que se realizan en la organización, las áreas encargadas de poner en marcha dichos procesos, ayuda fuertemente a proyectar las fortalezas y las debilidades de la organización.

Conocer los procesos en detalle conlleva a determinar el punto exacto de las posibles vulnerabilidades. Saber qué personas son las encargadas nos dará idea del perfil que se debe tener para hacer bien las actividades que dan vida a la empresa.

4.1.3. Definir Objetivos del BCP

Definir los objetivos del BCP es determinar de manera detallada las actividades que el BCP va a cubrir en caso de emergencia y garantizar en el momento de su activación la continuidad del negocio.

La finalidad de dejar muy claro estos objetivos es que las personas que intervengan en el mismo sepan hasta qué punto se cubrirán las necesidades de la organización y que actividades vitales estarán aseguradas.

Los objetivos deben estar compuestos por dos componentes primordiales:

- Un valor numérico medible asignable a cualquier persona, área o actividad que nos indique en qué medida se logra dicho objetivo.
- Un tiempo objetivo de recuperación dentro del cual el objetivo se deberá cumplir.

Un objetivo es una o un conjunto de acciones que tengan la posibilidad de ser medidas.

Además los objetivos deben cumplir con las siguientes características:

- La descripción del objetivo debe planteado de manera que sea una visión general de los deseos de la organización.
- Debe describir el tiempo en el que es necesario lograrlo.
- Deben ser específicos y claros para su fácil entendimiento.
- Deben estar coordinados para que no exista posibilidad de fallas en el desarrollo del plan.
- Los objetivos se construyen y se hacen realidad con ayuda de la óptima participación de los integrantes de la empresa. Si los ejecutivos y otros participantes en lograr los objetivos planteados no pueden articularlos trabando en conjunto, los objetivos no se logran y pueden terminar causando daños más severos que los problemas planteados en solucionar en primera instancia.

- Deben tender a ser concretos y con un fin muy claro que ayuden a mantener la motivación de los integrantes de la organización a lograrlos de manera rápida y precisa para dar pie a la continuidad del negocio.
- Deben ser flexibles y que acomodarse a las necesidades de la empresa y el ambiente en la que ésta se mueve, deben ser alcanzables para que la empresa mejore continuamente y se generen nuevos objetivos que complementen la continuidad del negocio.
- Deben ser analizados continuamente y modificados según sea el caso, esta continua vigilancia pretende el mejoramiento oportuno y eficaz de las actividades realizadas en el proceso de la continuidad.

Es fundamental que exista un buen plan de revisión del BCP que permita la actualización de estos objetivos y permita la plena vigencia del BCP.

4.1.4. Definir alcance del BCP

Definir el alcance del Plan de Continuidad ayuda a especificar de manera clara los siguientes puntos:

- Detallar las actividades que se van o no a desarrollar dentro del BCP.
- Definir de forma clara las mejoras o modificaciones que se encuentran sujetas a los resultados obtenidos en el análisis de los parámetros necesarios para el desarrollo del BCP
- Definir de manera detallada las limitaciones ya sean de procesos, áreas y de recursos que tiene la organización.
- Como parte principal de la definición del alcance se encuentra determinar los recursos que se tienen a disposición, ya que en algunas ocasiones es imprescindible obtener más recursos para el desarrollo de actividades que no estaban estimadas en el plan.

Tras definir el alcance del plan de manera clara es obligatorio presentar este mismo a la alta dirección y esperar su aprobación ya que ellos son parte muy importante para la puesta en marcha del BCP.

4.2. Análisis de impacto del Negocio (Bussines Impact Analisys - BIA)

4.2.1. ¿Qué es el BIA?

El BIA es la metodología utilizada para determinar el posible impacto que tendrán los riesgos en las actividades de la organización y ayuda a la creación de estrategias que dan pie a la continuidad del negocio, el BIA ayuda a consolidar el máximo tiempo tolerable (MTD[2]) que se puede tener para la recuperación al efecto de un riesgo, además del tiempo de recuperación (RTO[3]) que se debe lograr para la recuperación satisfactoria ante alguna amenaza [3]

4.2.2. ¿Cuál es el Objetivo del BIA?

Los objetivos de la BIA son:

- Estimar el impacto financiero para cada unidad de negocio, asumiendo el peor escenario.
- Identificar los procesos de la organización de unidades de negocio y el marco de tiempo de recuperación estimado para cada unidad de negocio.

Para el desarrollo de un Análisis de Impacto se debe tener en muy claro que la organización debe:

- Identificar las actividades que dan soporte a sus principales productos y servicios.
- Identificar los impactos resultantes de la interrupción sobre estas actividades, así como su variación en el tiempo.
- Establecer el período máximo tolerable de interrupción (MTD) para cada actividad identificando:

[2] De sus siglas en inglés Maximum Tolerable Downtime
[3] De sus siglas en inglés Recovery Time Objective

a) El máximo periodo de tiempo después del inicio de una interrupción dentro del cual debe reanudarse cada actividad.

b) El nivel mínimo en que debe desempeñarse cada actividad al reanudarse

c) Período de tiempo dentro del cual deben reanudarse los niveles normales de funcionamiento o RTO.

- Categorizar sus actividades según su prioridad para recuperar e identificar sus actividades críticas.
- Identificar todos los procesos pertinentes a las actividades críticas, incluyendo aquellas realizadas por terceros.
- Para los terceros de quienes dependen las actividades críticas, determinar qué componentes del SGCN[4] han sido implementados para los productos y servicios que ellos proporcionan.
- Establecer el tiempo objetivo de recuperación para reanudar las actividades críticas dentro de su período máximo tolerable de interrupción o el RTO.
- Estimar los recursos que cada actividad crítica requerirá para reanudar sus funciones.[4]

Para llevar cada uno de estos puntos se pueden desarrollar varios documentos que ayuden al desarrollo y documentación de estos pasos.

a) Tabla de identificación de procesos y su criticidad:

Nombre del proceso	Subproceso	Descripción	Área responsable	Persona encargada	Nivel de importancia	Consecuencias de falla

Tabla 2. Identificación de procesos y su criticidad – (Fuente. Autor)

b) **Tabla de impactos y gravedad cualitativa:** En esta tabla se podrá registrar de manera detallada la gravedad del impacto que tendría a lo largo del tiempo en las actividades de los procesos de la empresa

[4] Sistema de Gestión de Continuidad del Negocio

tomando como objetivo o vista del mismo todas las áreas en las cuales los procesos se podrían desempañar ([5])

Nombre del proceso				
Gravedad				
Impacto	Día 0	Día 1-2	Día 3-4	Semana 1
Económico				
Imagen empresarial				
Comercial				
Legal				

Tabla 3. Impactos y gravedad cualitativa: – (Fuente. Autor)

NIVEL DE GRAVEDAD
Nulo
Bajo
Medio
Alto

Los impactos más comunes en función del tiempo y que para este caso serán tomados hipotéticamente ya que dependen de las actividades que realice la empresa son los siguientes:

Día 0:

- Contestar llamadas del cliente
- Asuntos relacionados a la salud
- Planes de acción ante fugas de gas, agua y químicos.
- Daños de imagen empresarial.

Día 1 - 2: Tras el primer día de parálisis de las actividades de la organización ésta no ha sentido fuertemente los efectos de las amenazas, pero tras el segundo día se empiezan a sentir los siguientes impactos:

[5] Estas tablas pueden ser modificables según las áreas de donde provengan los procesos a evaluar

- El cliente no puede ser atendido oportunamente y con eficiencia.
- Los procesos de venta no son satisfactorios
- El proceso de pedidos y entregas está retrasado.

Día 3 - 4: Tras el tercer o cuarto día, la empresa no alcanza a soportar lo que implica la interrupción y el impacto en las actividades se incrementa. Para este tiempo la organización reporta los siguientes impactos:

- Clientes insatisfechos y pérdidas económicas
- Perdidas de clientes
- Demandas por incumplimiento

Semana 1: En esta etapa la empresa ya ha gastado demasiados recursos monetarios en la recuperación de las actividades fundamentales o totales de la empresa.

c) **Tabla de Estimación de recursos:** En esta tabla se podrán detallar los procesos y para cada uno de ellos los recursos ya sean técnicos, administrativos, humanos o de terceros que son necesarios para el desarrollo de los mismos.

Proceso	Descripción	Recursos de la actividad	Valor del Recurso	Responsable del Recurso	Tiempo de obtención

Tabla4. Estimación de recursos – (Fuente. Autor)

d) **Tabla de impacto económico o cuantitativo:** En esta tabla se definirá el impacto económico que tiene en la empresa la ocurrencia de las amenazas explotadas por un agente o evento externo.

Nombre del proceso				
Impacto cuantitativo				
Función	4 horas	1 día	2 días	7 días
Función A				
Función B				

Tabla 5. Impacto económico o cuantitativo
Fuente – (Autor)

4.2.3. Parámetros de recuperación:

En el desarrollo del análisis de impacto es necesario establecer los parámetros de recuperación de las actividades de la empresa. Como fase importante del plan de continuidad del negocio las fases de recuperación indican el tiempo máximo de interrupción permitido (MTD), el tiempo de recuperación objetivo (RTO) y el punto de recuperación de las actividades (RPO).

1) El MTD establece el tiempo máximo tolerable en la interrupción de las actividades de la organización.

2) El RTO establece la urgencia con la cual las diferentes unidades de negocio precisan recuperarse 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.[5]

3) El RPO indica el 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.[5]

En la siguiente grafica se establece en la línea del tiempo y desde el momento de alguna catástrofe actúa en las actividades de la empresa como

intervienen el MTD y el RTO y desde cuando las pérdidas para la empresa se consideran realmente graves

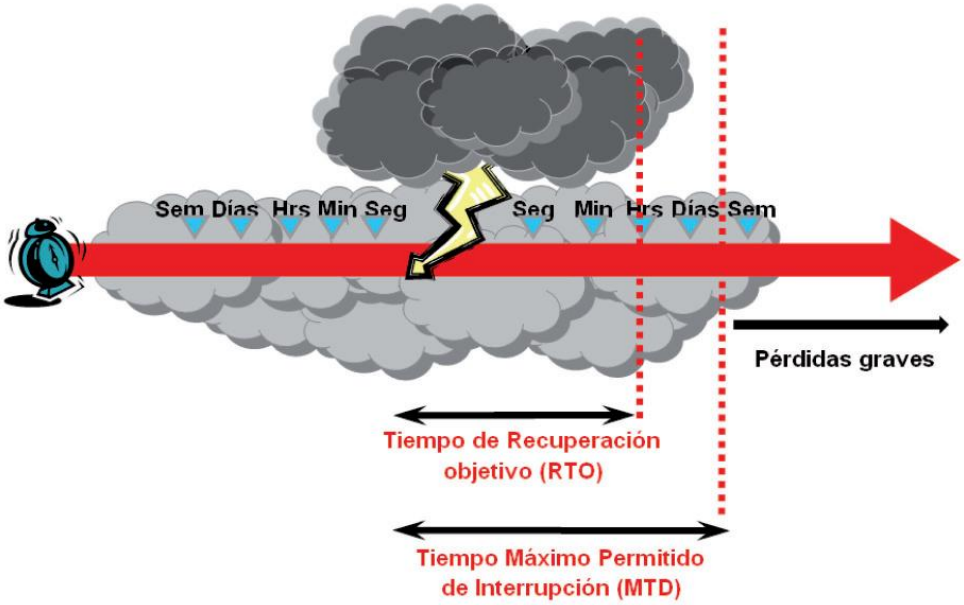

Ilustración 3. Relación de MTD y RTO en la línea del tiempo.

Fuente. Guía práctica para PYMES: como establecer un plan de continuidad del negocio. [5]

4.2.4. Pasos del BIA

En resumen aquí se presentan los pasos de un BIA:

- Seleccione los individuos a entrevistar para la recopilación de datos.
- Crear las técnicas de recolección de datos (encuestas, cuestionarios cualitativos y los enfoques cuantitativos).
- Identifique las funciones críticas de negocio de la compañía.
- Identificar los recursos de los que estas funciones dependen.
- Calcular cuánto tiempo estas funciones pueden sobrevivir sin estos recursos.
- Identificar las vulnerabilidades y amenazas para estas funciones.
- Calcular el riesgo para cada función de negocio diferente.
- Documentar los hallazgos e informar a la gerencia.

4.3. Evaluación de riesgos

4.3.1. ¿Qué es el riesgo?

Existen varias formas de ver el significado del riesgo, como tal el riesgo puede ser tomado de muchas maneras, como seria:

- **Riesgo:** Un riesgo es la probabilidad de que un agente de amenaza tome ventaja de una vulnerabilidad y tenga un impacto en el negocio.[6]
- **Exposición:** Una exposición es una instancia donde la información está expuesta a pérdidas por parte de un agente de amenaza y donde existe una vulnerabilidad que expone a la organización a posibles daños. [6] La exposición, no significa que el evento que produce la pérdida o daño del recurso “este ocurriendo”, solo significa que podría ocurrir dado que existe una amenaza y una vulnerabilidad que ésta podría explotar.
- **Amenaza:** Una amenaza es cualquier peligro potencial a la información o sistemas. La amenaza es que alguien, o algo, identificará una vulnerabilidad específica y la usará en contra de la compañía o un individuo.[6]

Tras tener claro los posibles conceptos de riesgo se puede entender que la organización puede realizar 4 acciones de tratamiento fundamentales sobre estos riesgos:

- **Evitar**: se pueden evitar los riesgos por medio de controles eficaces que ayuden a la eliminación de las causas de dichos riesgos.
- **Reducir:** La única forma de reducir la frecuencia de los riesgos es aplicando los controles necesarios sobre la raíz de los riesgos para reducir la frecuencia de su materialización.
- **Transferir el Riesgo**: esta opción de tratamiento del riesgo se basa en compartir con una entidad externa los riesgos del mismo, esto se hace por medio de (subcontratación, seguros, entre otros). Sin embargo la transferencia del estos riesgos no es completa ya que la empresa sigue

asumiendo parte del riesgo y adquiriendo nuevas riesgos al dejar en manos de personas ajenas la seguridad de sus recursos.

- **Aceptar el Riesgo:** Utilizada cuando se considera que mitigar el riesgo es más costoso que el impacto que este pueda producir en la empresa.

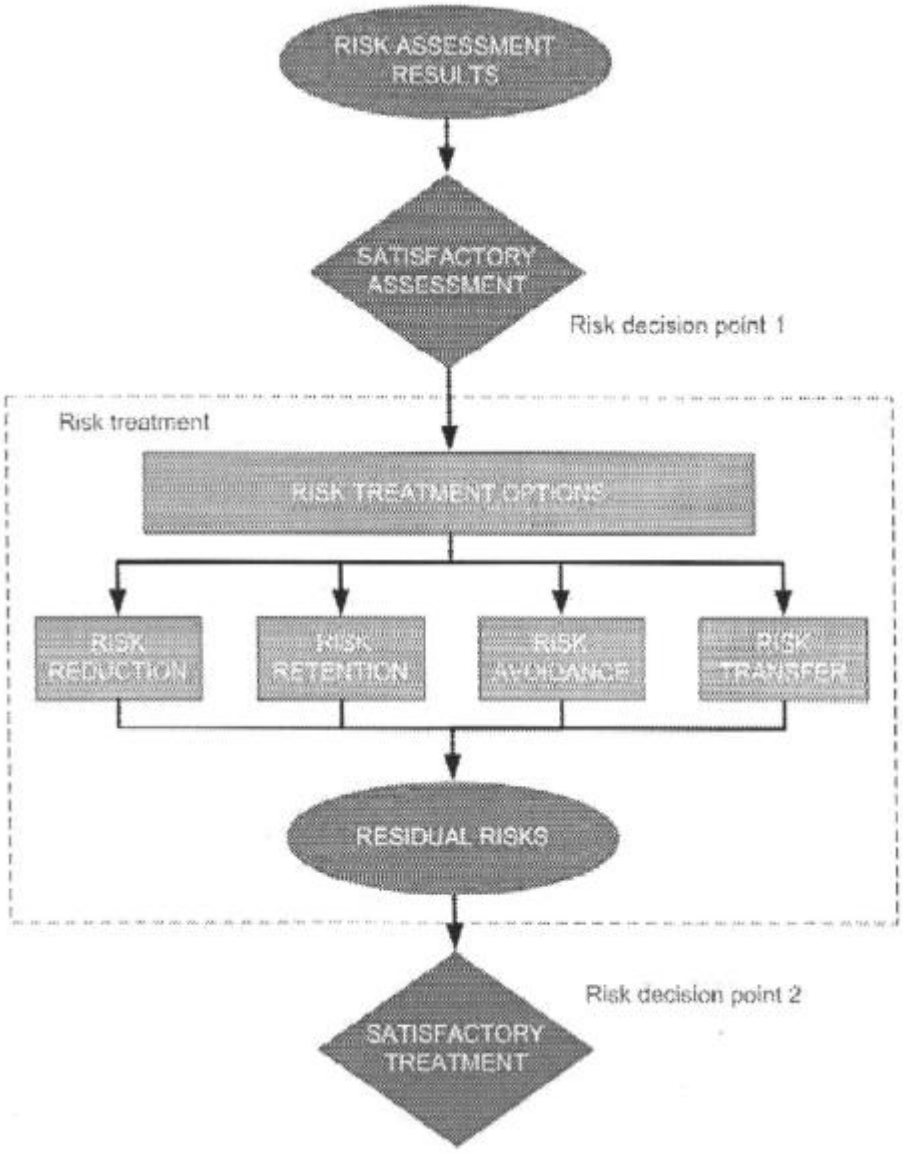

Ilustración 4. Tratamiento de Riesgos
Fuente: ISO 27005[7]

Al conocer con detenimiento de lo que es un riesgo y las formas de su tratamiento hay que ser consciente que existe un costo al analizar y tratar los riesgos a lo largo de la vida del desarrollo del BCP.

En la ilustración 5 se demuestra que el costo de tratamiento del riesgo al inicio del proyecto del BCP es demasiado alto pero que tras la evaluación continua de las causas y el establecimiento de parámetros de control los riesgos van disminuyendo hasta el punto de equilibrio y donde existe mayor impacto de los riesgos. Después de establecer y ejecutar el plan de continuidad los riesgos se verán disminuidos hasta su eliminación total y se evidencia que los costos monetarios disminuyen.

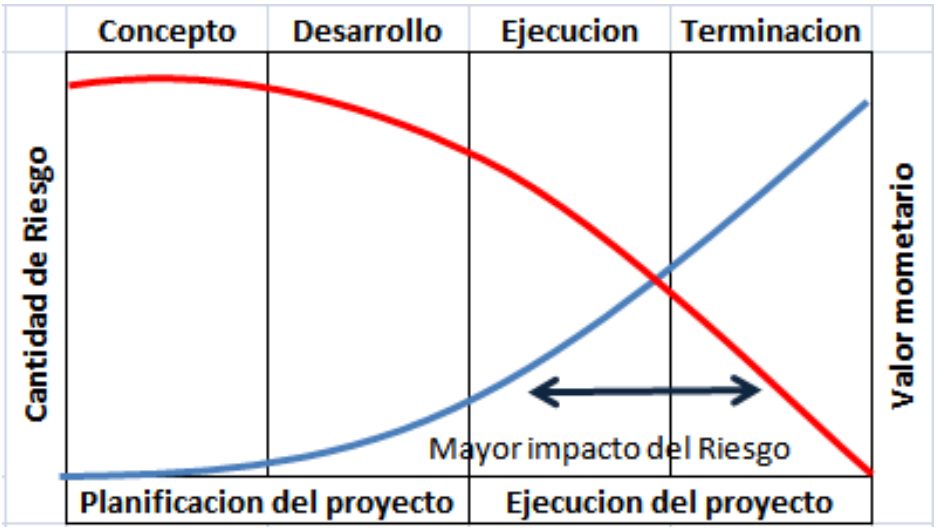

Ilustración 5: Relación Costo – Riesgo. (Fuente. PMBOK [8])

En el concepto de riesgo se debe tener en cuenta que existen tres componentes esenciales:

- Un evento o exposición que da comienzo al riesgo.
- Una probabilidad de ocurrencia.
- Una consecuencia

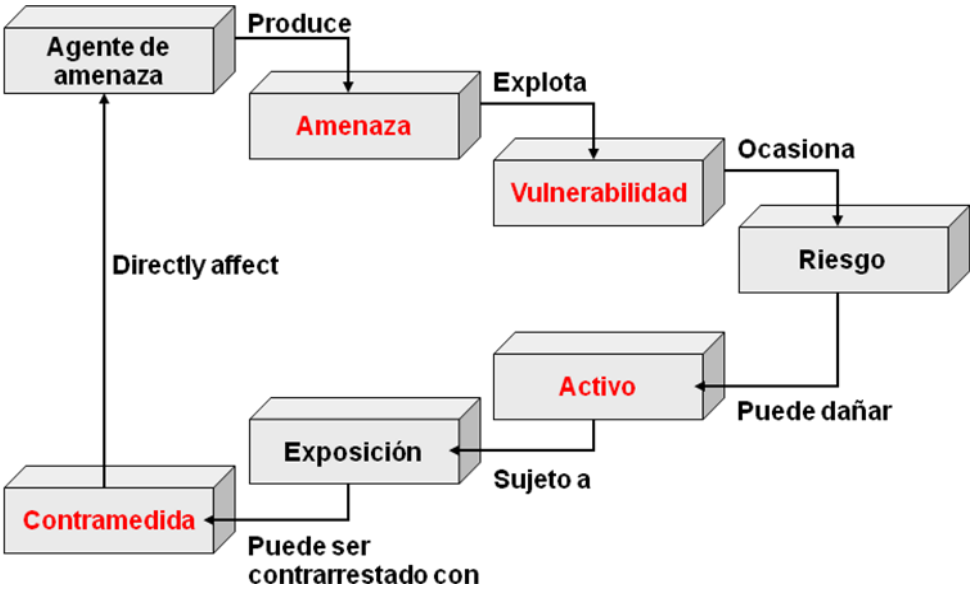

Ilustración 6. Relaciones entre los riesgos, vulnerabilidades, amenazas y contramedidas

Fuente. Information Security and Risk Management Chapter 3. [11]

Como conclusión podemos decir que los riesgos son:

- situacionales porque se presentan y se comportan diferente en determinadas situaciones,
- son interdependientes ya que ocasionalmente están relacionados unos con otros,
- son tolerables, aunque la tolerancia de estos riesgos varía de organización a organización,
- son la evolución de las vulnerabilidades de las organizaciones,
- causan daños en los activos de las empresas,
- pueden ser controlados y medidos a lo largo del tiempo.

También podemos concluir que el tratamiento de los riesgos tiene muchas variantes y que estos dependen de las necesidades y recursos que tenga la organización.

4.4. Clasificación del riesgo

Los riesgos se pueden clasificar según la fuente de la que provengan y se dividen en dos tipos:

- **Fuentes Internas**

Se consideran fuentes internas cuando las causas se relacionan con las personas, actividades o procesos desarrollados al interior de la organización.

- **Fuentes Externas**

Se considera fuente externa cuando la fuente de las amenazas no está en al interior de las actividades de la empresa y son impredecibles en su totalidad ya que son variables incontrolables así se tenga conocimiento de estos riesgos.

Tecnología	Programación	Financiación	Legal
Tecnología nueva o no probada	Disponibilidad de recursos	Fondos y presupuesto	Propiedad intelectual
Disponibilidad de experiencia técnica	Planificación inadecuada	Exactitud de estimación	Políticas de Gobierno
Actuación del subcontratista	Restricción de programación	Cambio en coste de materiales	Derechos de datos
Riesgos de diseño	Información insuficiente		Ambigüedades de contrato
Transición desde diseño a producción	Dependencia de la empresa		Multas
Disponibilidad de materiales	Dependencias del cliente		Derechos de patentes o incumplimientos

Tabla 6. Clasificación de Fuentes Internas
Fuente: Instituto Nacional de Tecnologías de la Comunicación [6]

Impredecibles	Predecibles pero inciertos
Cambios reguladores	Cambios de mercado
Impacto ambiental	Tasación
Desastres naturales	Inflación
Interés publico	Tipo de cambio
Relaciones Industriales(Huelgas)	Subcontratista
Mercados dinámicos	Mercados dinámicos

Tabla 7. Clasificación de Fuentes Externas
Fuente: Instituto Nacional de Tecnologías de la Comunicación [6]

4.5. Identificación del riesgo

La identificación de los riesgos es un proceso que consiste en determinar cuáles son las amenazas que afectan directa e indirectamente a la organización, las actividades de identificación deben estar presentes en:

- El alcance del BCP
- Durante el desarrollo del BCP
- En la estimación de recursos utilizados en el Plan, ya que si no se calculan de manera adecuada podrán hacer faltan en momentos en los cuales sea necesario la adquisición o aprisionamiento de recursos necesarios para la continuidad.

Además de identificar los riesgos se debe determinaran las fuentes de los mismos y para esto hay que tener en mente todas las posibles fuentes ya sean las más obvia o las que tengan poca posibilidad de dar origen a un riesgo esto ayudara a asegurar la eficacia de las soluciones o correcciones a los focos de los mismos.

Se identificarán y se documentarán los factores o síntomas que disparan los riesgos. Hay que tener en cuenta que estos sencillos pasos de identificación pueden estar en toda la vida del proyecto y ayudarán a la gestión del BCP.

Las metodologías que se pueden usar para la identificación de riesgos son:

- **Tormenta de Ideas**
- **Entrevistas:** Las entrevistas deben ser desarrolladas con las personas encargadas de las actividades críticas de la organización y que son las más indicadas para reconocer lo que afecta directamente al buen desempeño de la empresa.
- **Análisis PEST[6]:** El concepto principal de este análisis es conocer el entorno en el cual se va a mover nuestra organización. Está compuesto por factores Políticos, Económicos, Sociales y Tecnológicos y que tras el análisis de estos factores se conocerá lo que tiene la organización y a lo que se tiene que enfrentar y lo que la organización puede realizar para lograr un mejoramiento.

[6] El nombre de PEST proviene de las siglas de los factores analizados por el mismo.

Ya que el enfoque del análisis Pest son los factores externos de la organización es recomendable ser establecido antes de realizar el análisis FODA ya que este analiza los factores internos y el análisis de PEST se basa en el mercado.

- **Factores del análisis PEST:**
  - **Factor Político:** Para el análisis de esta área se debe tener muy en claro las funciones o regulaciones políticas que pueden afectar a nuestro negocio o a los consumidores que acceden a nuestros servicios.

Como ejemplo se podrían tener en cuenta las siguientes preguntas y pueden ser usadas en el desarrollo o modificadas en el análisis PEST.

i. ¿Cuál es la posición del gobierno en el ambiente comercial actual?

ii. ¿Cuáles son los acuerdos comerciales que actualmente el gobierno tiene con otros países y como afectan a nuestra organización?

iii. ¿Tiene el gobierno algún tratado de libre comercio que afecte o beneficie a nuestra empresa?

- **Factor Social:** En este factor se analizará de manera detallada las cosas que se ven actualmente en la sociedad como la religión predominante, la influencia de los productos extranjeros en las personas, la opinión de las personas ante el ambiente y la naturaleza, las preferencias ante el ocio, etc.
- **Factor Económico:** Para el análisis de este factor es necesario tener muy claro los aspectos económicos de la sociedad, como tasa de desempleo, los tipos de interés, la inflación, etc.
- **Factor Tecnológico:** ya que la tecnología ocupa más del 50% de la vida de las personas y ayuda a las empresas a dar trámite a sus actividades, se debe analizar los beneficios para las personas como comprar boletos de viaje por internet, que nuevos productos tecnológicos existen que ayuden al desempeño ágil los negocios, etc.

Las plantillas del análisis PEST se presentan en cuatro casillas donde se plantean las ideas de cada uno de los 4 factores que componen este tipo de análisis.

Análisis PEST	
Políticos	**Sociales**
Lista de posibles factores políticos que afecten a la organización de manera positiva o negativa.	Lista de eventos que afectan al funcionamiento de las funciones de la organización
Económicos	**Tecnológicos**
Lista de todos los factores económicos que afectan a los gastos de la organización	Lista de las mejoras que da la tecnología a los procesos de la organización (Ejemplo. Ayuda que da Internet a los procesos productivos de la organización)

Tabla 8. Análisis PEST
Fuente: Tabla desarrollada por el autor de este trabajo

- **Análisis FODA[7]:** El análisis FODA se desarrolla para formar una idea inicial de lo que se tiene en la organización. Este análisis plantea reconocer las Fortalezas, Oportunidades, Debilidades y Amenazas que tiene la empresa en su interior, este análisis ayuda a los desarrolladores del BCP a tener claro lo que en sí es su empresa, qué recursos y capacidades se tiene, qué debilidades sufre la empresa y qué oportunidades tiene de salir adelante la empresa frente a riesgos y amenazas.

[7] El nombre de FODA proviene de las siglas de los factores internos analizados por el mismo

Matriz de Análisis FODA	Fortalezas	Debilidades
	Listado de Fortalezas	Listado de Debilidades
Oportunidades	Estrategias(FO)	Estrategias(DO)
Listado de Oportunidades	Usar las fortalezas para aprovechar las oportunidades	Minimizar las debilidades aprovechando las oportunidades
Amenazas	Estrategias(FA)	Estrategias(DA)
Listado de Amenazas	Usar las fortalezas para evitar o reducir el impacto de las amenazas	Minimizar las debilidades y evitar las amenazas

Tabla 9. Análisis FODA

Fuente: Tabla diseñada por el autor de este trabajo

4.6. Análisis de riesgos

El análisis de riesgos es una herramienta que ayuda a la toma de decisiones y donde se realiza una especulación de los efectos futuros que puedan ocurrir en la empresa, estas especulaciones se basan en los eventos relevantes que afectaron al ciclo de vida de la organización. El análisis de riesgos trata de responder a varias inquietudes comunes en el desarrollo e implementación de proyectos. [16]

- ¿Qué puede salir mal?
- ¿Qué tan probable es la ocurrencia de que algo salga mal?
- ¿Qué consecuencias existirían si algo en especial sale mal?
- ¿Qué se puede hacer para evitar que los eventos encontrados salgan mal?

Tras realizar un análisis de riesgos detallado se encontraran varios beneficios tales como:

- Desarrollar planes de contingencia con antelación
- Mantener un ambiente controlado y con pocas probabilidades de riesgo
- Permite conocer todos los riesgos que afectan al funcionamiento de la organización.

- Ayudar con la comunicación con la gerencia ya que tras tener claro los riesgos que enfrentará la empresa se podría explicar a la gerencia la importancia de realizar cambios e invertir en el desarrollo de planes de continuidad.

Para el desarrollo de un análisis de riesgos se tienen 2 metodologías que pueden ser usadas de manera individual o conjunta dependiendo de los objetivos planteados por el equipo de desarrollo del BCP.

Para dar una descripción simple se plantea la siguiente tabla comparativa de ambos métodos.

Característica	Cualitativo	Cuantitativo
Cálculos	Simples	Complejos
Aplicable	Siempre	No siempre
Análisis de costo/beneficio	Subjetivo	Concreto
Objetividad	Baja	Alta
Comprensible por la dirección	Menos	Más
Herramientas automatizadas	No aplicable	Aplicable
Utiliza métricas claras	No	Sí

Tabla 10. Cuadro comparativo de análisis cualitativo y cuantitativo - Fuente [11]

4.6.1. Análisis cualitativo:

Esta metodología se basa en la experiencia y pensamiento subjetivo de las personas que la ponen en práctica. Trata de estudiar qué tan factible y con qué ocurrencia pueden manifestarse los riesgos. El análisis cualitativo es rápido pero impreciso ya que conjuga: juicio, experiencia e intuición.

Nivel	Calificación	Descripción
A	Casi segura	Se espera que ocurra en la mayoría de las circunstancias
B	Probable	Ocurrirá en la mayoría de las circunstancias
C	Posible	Puede ocurrir en cualquier momento
D	Improbable	Podría ocurrir en cualquier momento
E	Rara	Ocurriría solo en circunstancias excepcionales

Tabla 11. Tabla de Probabilidad de riesgo [12]

Nivel	Calificación	Descripción
1	Insignificante	No hay heridos, no hay pérdidas financieras
2	Menor	Primeros auxilios, perdida financiera mediana
3	Moderada	Tratamiento médico, alta pérdida financiera.
4	Importante	Heridas graves, importantes pérdidas financieras.
5	Catastrófica	Muertes, excesivas pérdidas financieras.

Tabla 12. Descripción cualitativa de Consecuencias [12]

Probabilidad	Consecuencias				
	(Insignificantes)	(Menor)	(Moderadas)	(Mayores)	(Catastróficas)
Casi segura	Alto	Alto	Extremo	Extremo	Extremo
Probable	Moderado	Alto	Alto	Extremo	Extremo
Posible	Bajo	Moderado	Alto	Extremo	Extremo
Improbable	Bajo	Bajo	Moderado	Alto	Extremo
Rara	Bajo	Bajo	Moderado	Alto	Alto

Tabla 13. Matriz de Análisis Cualitativo de Riesgos [12]

Las metodologías más usadas para este tipo de análisis son:

- Técnicas Delphi
- Matriz de probabilidad – impacto
- Brainstorming
- Cuestionarios
- Checklist
- Entrevistas

4.6.2. Análisis cuantitativo

El análisis cuantitativo se basa en cuantificar la probabilidad de que ocurran ciertos eventos dañinos para la empresa. Esta metodología de análisis se basa en la asignación de algún valor numérico para determinar el nivel de importancia del riesgo.

Tras realizar este análisis se puede determinar la importancia de los riesgos, cuál de estos debe ser atendido de forma inmediata, determinar los

riesgos que aunque no están en una fase alarmante pero que pueden volverse en serios.

Aunque el análisis cuantitativo da datos más reales que el cualitativo aún sigue siendo impreciso, pero su fácil implementación da pie a una rápida clasificación de riesgos.

Las metodologías más usadas para este análisis son:

- Método de Montecarlo (Simulación de impacto potencial)
- CBA o Análisis Costo – Beneficio
- Análisis de valor ganado
- Árbol de decisión
- Análisis de sensibilidad

Como tal existen varias metodologías que ayudan a la gestión de riesgos pero para el caso práctico de esta guía las mencionaremos brevemente.

MAGERIT: Es una metodología de carácter público, perteneciente al Ministerio de Administraciones Públicas (MAP) de España. Su utilización no requiere autorización previa del MAP. Magerit interesa a todos aquellos que trabajan con información y los sistemas informáticos que la tratan. Si dicha información o los servicios que se prestan gracias a ella son valiosos, esta metodología les permitirá saber cuánto de este valor está en juego y les ayudará a protegerlo. [9]

Magerit persigue los siguientes objetivos:

- Concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de atajarlos a tiempo [9]
- Ofrecer un método sistemático para analizar tales riesgos[9]
- Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control [9]
- Apoyar la preparación a la organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso [9]

- Asimismo, se ha cuidado la uniformidad de los informes que recogen los hallazgos y las conclusiones de un proyecto de análisis y gestión de riesgos: modelo de valor, mapa de riesgos, evaluación de salvaguardas, estado de riesgo, informe de insuficiencias, y plan de seguridad [9]

MAGERIT describe la metodología desde tres ángulos:

- Los pasos para realizar un análisis del estado de riesgo y para gestionar su mitigación. Es una presentación netamente conceptual. [9]
- Las tareas básicas para realizar un proyecto de análisis y gestión de riesgos, entendiendo que no basta con tener los conceptos claros, sino que es conveniente pautar roles, actividades, hitos y documentación para que la realización del proyecto de análisis y gestión de riesgos esté bajo control en todo momento. [9]
- Uno de sus capítulos aplica la metodología al caso del desarrollo de sistemas de información, en el entendimiento que los proyectos de desarrollo de sistemas deben tener en cuenta los riesgos desde el primer momento, tanto los riesgos a los que están expuestos, como los riesgos que las propias aplicaciones introducen en el sistema. [9]
- Como complemento desgrana una serie de aspectos prácticos, derivados de la experiencia acumulada en el tiempo para la realización de un análisis y una gestión realmente efectivos. [9]

OCTAVE: Evalúa amenazas y vulnerabilidades de los recursos tecnológicos y operacionales importantes de una organización. El método OCTAVE (Operationally Critical Thereat, Asset and Vulnerability Evaluation) permite la comprensión del manejo de los recursos, identificación y evaluación de los riesgos que afectan la seguridad dentro de una organización. Exige llevar la evaluación de la organización y del personal de la tecnología de información (IT) por parte del equipo de análisis mediante el apoyo de un patrocinador interesado en la seguridad.[10].

Las funciones del equipo de análisis:

- Identificar los recursos importantes mediante encuestas y entrevistas.
- Realizar actividades de análisis de riesgo.
- Relacionar amenazas y vulnerabilidades.
- Crear estrategias de protección, planes de mitigación y diseñar políticas de seguridad.

5. ETAPA 2. ESTRATEGIAS PARA LA CONTINUIDAD

Tras analizar de manera detallada los resultados del BIA y el análisis de riesgos, se debe tener la capacidad de crear e implementar estrategias y controles preventivos acordes a las necesidades de la empresa que ayuden a:

- La mitigación de riesgo.
- Disminución de tiempos y costos en el tratamiento
- Llevar el control de los riesgos y amenazas a la empresa
- Detectar responsables de áreas y de funciones de la continuidad.
- Establecer acuerdos de continuidad con terceros
- Establecer lugares alternos donde poder dar comienzo a la estabilización de las operaciones de la organización.
- Establecer cuáles son las personas adecuadas para la implementación de la continuidad.

Ilustración 5. Recursos de la organización en el BCP
Fuente: Guía práctica para PYMES: Como implementar un plan de continuidad del negocio

Para comenzar con las estrategias de continuidad del negocio se debe:

- Conocer cuáles son las personas que intervienen en las actividades más importantes de la organización con el objetivo de ubicar de manera adecuada a este personal en los lugares apropiados dentro de la empresa para que garantice que con sus conocimientos se podrán mantener en funcionamiento y con continuidad las actividades de la organización. Para garantizar mantener este conocimiento se debe documentar, la formación académica, los conocimientos multidisciplinarios y la asignación que tienen dentro de la organización.
- Establecer estrategias que no afecten la actividad en los lugares de trabajo, para esto la mejor alternativa es elegir sedes alternas y tener acuerdos con terceros y con distribuidores de tecnología que ayuden a la continuidad de las operaciones con ayuda de los recursos tecnológicos apropiados para establecer un nuevo centro de operaciones en el menor tiempo que ayuden a la vuelta a la vida de las actividades de la organización.
- Tener el conocimiento de la tecnología usada en las operaciones de la empresa y se debe conocer la capacidad de la

organización en implementar estos recursos tecnológicos en lugares alternos en caso de cualquier desastre.

- Llevar una documentación apropiada de las actividades de recuperación, de los casos en los que el plan sea activado y sobre todo de las copias de seguridad que son parte vital de las estrategias para la continuidad de la organización.

Tabla de registro y Procedimiento de Backup				
Departamento:	**Nombre del Departamento**			
Nombre de la aplicación	**Fecha y hora del backup de la aplicación**	**Período de retención**	**Periodo almacenado**	**Responsable del backup**
Aplicación 1	MM/DD/AAAA HH:MM:SS	XXX tiempo	MM/DD/AAAA – MM/DD/AAAA	Líder del Área

Tabla 14. Tabla de registro y procedimiento de Backup
Fuente: Diseñada por el Autor del proyecto

- La más importante de las estrategias que debe considerar un negocio es **salvaguardar la vida de sus empleados**, todo esto se logra teniendo un conocimiento constante sobre las vías de emergencia, los números de línea de emergencia, los lugares seguros ubicados cerca de la sede empresarial. Todo esto debe ser documentado y distribuido de manera oportuna a los empleados. [5]
- Tener la capacidad de establecer las actividades de la organización en sedes alternas, estas sedes deben garantizar que con su infraestructura se pueda establecer la continuidad de los procesos de la empresa. La organización debe considerar los costos de tener una nueva sede y estudiar en detalle la capacidad económica que poseen en la actualidad para adquirir o arrendar sedes donde se pueda llevar a cabo la continuidad con el negocio.

Site	Cost	Hardware Equipment	Telecom-munications	Setup Time	Location
Cold Site	Low	None	None	Long	Fixed
Warm Site	Medium	Partial	Partial/Full	Medium	Fixed
Hot Site	Medium/ High	Full	Full	Short	Fixed
Mobile Site	High	Dependent	Dependent	Dependent	Not Fixed
Mirrored Site	High	Full	Full	None	Fixed

Tabla 15. Criterios de Selección de Sitio Alterno

Fuente: NIST Special Publication 800-34.

- Tener en mente que el traslado de personal de áreas no tan vitales de la empresa a sectores de la misma que sean de mayor importancia y que necesiten de una recuperación de sus funciones.
- Tener muy claro como transportar al personal a las sedes alternas para dar inicio a las operaciones de la organización.
- No olvidar considerar las familias de los empleados, ya que en situaciones de desastres mayores las mismas pueden verse afectadas y por ende los mismos empleados se encuentran en situaciones complejas de manejar.
- Tener un software de respaldo con el cual se pueda iniciar los procesos fundamentales de las actividades de la empresa.

7. ETAPA 3. DESARROLLO DEL PLAN DE CONTINUIDAD

Tras llegar a este punto ya se debe tener claro las estrategias de acuerdo a las necesidades de la organización, los procesos y procedimientos que realiza la empresa en sus actividades de más importancia.

De aquí en adelante es imprescindible determinar cuáles serán las personas y los grupos de trabajo que intervendrán directamente en el desarrollo e implementación del BCP, se determinarán sus responsabilidades, se desarrollarán los procedimientos a seguir antes y después de alguna contingencia y se determinará el plan que se tendrá para la vuelta a la normalidad.

7.1. Definir Personal, Grupos de Trabajo y Responsabilidades

Una parte fundamental de las estrategias de continuidad del negocio es definir qué personas son las encargadas de la creación, desarrollo, implementación, coordinación, comunicación, capacitación y activación del BCP.

Para empezar es necesario tener un líder total del BCP, establecer como coordinador a una persona que active el BCP, que coordine las actividades al momento de una contingencia, esta persona debe ser una persona que se encargue de distribuir copias del plan de continuidad a todas las áreas de las principales actividades de la organización.

Nombre de Líder	Fecha de entrega	Numero de la Copia del BCP	Persona a cargo de la copia	Firma

Tabla 16. Tabla de registro de copias del BCP
Fuente: Diseñada por el Autor del proyecto

Este coordinador tiene la responsabilidad de realizar simulacros del BCP y tras la culminación de las actividades del simulacro realizar análisis de los resultados obtenidos con la colaboración de grupos de trabajo de las áreas afectadas, este trabajo en equipo sirve para aclarar dudas, arreglar las falencias encontradas e ir perfeccionando el plan.

Numero de Simulacro	Objetivo del Simulacro	Fecha / Hora	Resultado Esperado	Resultado Obtenido	Tiempo estimado de respuesta	Tiempo total del simulacro	Áreas participantes

Tabla 17. Tabla de registro Simulacros
Fuente: Diseñada por el Autor del proyecto

El coordinador debe tener también un backup en otra persona del equipo de trabajo del BCP.

Después de seleccionar un coordinador del BCP es necesario integrar equipos de trabajo de todas las áreas de la organización, estos equipos de trabajo dependen de los recursos (Humanos, técnicos y monetarios) que posea la empresa.

- **Líder de Grupo:** Los lideres de grupo deben ser personas con aptitud de líder, deben poseer capacidades y conocimientos profundos del área en la cual trabajan, estas personas no se debe limitar de tomar una decisión en momentos reales de emergencia, las funciones del líder de grupo son:
    - Velar porque en cada simulacro o caso real el aporte de su grupo contribuya a las necesidades de la organización.
    - Colaborar con la identificación de las falencias del BCP y aportar mejoras al mismo sin afectar las demás áreas de la empresa.
    - Tener la capacidad de planear soluciones en conjunto con los líderes de otras áreas o grupos.
- **Suplente del Líder:** Este suplente debe tener las mismas capacidades del líder encargado del área, el líder suplente debe cumplir con las funciones antes mencionadas. Además debe rendir cuentas de manera detallada de las actividades realizadas en la activación del BCP al líder del grupo tras su reintegración a las actividades de la organización.
- **Miembros del Equipo:** Los equipos de trabajo para las actividades de recuperación y continuidad del negocio son: Equipo de tecnología, Equipo de comunicación, Equipo de Aplicaciones y Equipo de Operaciones.

- **Composición de Equipos:**
- **Tecnología**: Las funciones de este equipo de trabajo es determinar los riesgos que afectan directamente al área de TI de la empresa, este grupo de trabajo se encarga de servir como apoyo a las áreas de la empresa afectadas técnicamente en los sistemas de información. Las actividades más importantes que realiza este grupo es establecer y aprovisionar la sede alterna donde dará comienzo la continuidad de las principales actividades de la empresa.

- **Comunicación:** Las función de este equipo debe ser la documentación del estado de la red de comunicaciones antes, durante y después de algún acontecimiento de interrupción. Además de la documentación este grupo es el encargado de restablecer el funcionamiento y aprovisionamiento de las comunicaciones de los sistemas de información, de la instalación de hardware y software necesarios para la recuperación de las comunicaciones entre las oficinas, sedes y centrales de comunicación.
- **Aplicación:** Las funciones de este grupo son asegurar que las aplicaciones tengan backup, que puedan ser iniciadas en otros servidores alternos al principal, que la movilidad de las mismas sea posible en cualquier momento para así asegurar la continuidad de las operaciones de la organización.
- **Operaciones:** Las funciones de este grupo son asegurarse que existen recursos suficientes para la recuperación de las funciones afectadas, es responsable de la creación de un cronograma donde se refleje en detalle las actividades de la recuperación de actividades.

7.2. Capacitaciones y Comunicación

La capacitación y comunicación adecuada, clara y continua a los integrantes de la organización sobre todos los campos de acción del BCP ayuda a fortalecer la vida sana de la organización y a crear cultura en los empleados y personas responsables de los procesos fundamentales de la empresa.

7.2.1. Métodos de Comunicación

La comunicación cuando es aplicada en las empresas se llama comunicación organizacional, la comunicación es un punto vital de la misma ya que es imposible sobrevivir sin ella. Según Gary Kreps[8] "la comunicación organizacional es el proceso por medio del cual los miembros recolectan información pertinente acerca de su organización y los cambios que ocurren

[8] **Gary L. Kreps es un estudioso de la comunicación. Actualmente es Profesor Distinguido, Presidente del Departamento de Comunicación y director del Centro para la Comunicación de Salud y Riesgos en la Universidad George Mason en Fairfax, Virginia, Estados Unidos.**

dentro de ella. La comunicación ayuda a los miembros a lograr las metas individuales y de organización, al permitirles interpretar el cambio de la organización y finalmente coordinar el cumplimiento de sus necesidades personales con el logro de sus responsabilidades evolutivas en la organización". [13].

La comunicación son un conjunto de reglas que ayudan al fácil, claro y fluido entendimiento de la información que debe manejar la organización.

La comunicación rige cada una de las actividades de la organización y es vital para los directivos ya que con una comunicación eficaz se puede lograr una excelente planificación, organización y control de las actividades de la empresa.

La comunicación en la organización se divide en:

Comunicación interna: Esta metodología es usada para mantener la buena armonía entre los integrantes de la organización y contribuye a la distribución oportuna de las normativas y actividades presentes en la misma.

Comunicación externa: metodología usada para mantener una armonía entre los diferentes integrantes externos, informar de manera clara las decisiones de las directivas o promover productos y servicios de una manera amigable y llamativa.

7.2.2. Métodos de Capacitación

La capacitación se basa en informar de manera didáctica las buenas prácticas que son necesarias para la implantación del BCP de la organización.

Algunos de los diferentes métodos de capacitación más utilizados son:

- Revistas informativas
- Talleres

- Actividades lúdicas
- Reuniones con los directivos.
- Mensajes Virtuales
- Simulacros
- Carteles en carteleras o en Intranets propias

7.2.3. Desarrollo de Procedimientos y Alertas

Una vez establecido los equipo de trabajo, su capacitación y funciones en el desarrollo del BCP es necesario desarrollar la menara de actuar en los momentos previos, durante y después de la activación del plan.

Para crear los procesos se debe dejar muy claro lo que va a hacer cada proceso, quien será el responsable de activar dicho proceso en el momento que sea necesario, que características debe cumplir la amenaza para poder activar el plan, como será el método para activar el plan.

Todo esto es desarrollado con el fin de llevar a la empresa a la normalidad los procesos después de alguna catástrofe.

En la siguiente grafica se muestran las etapas que deben pasar para llegar al objetivo de todo lo que se ha hablado en el desarrollo de este trabajo, la recuperación y la vuelta a la normalidad de las actividades de la organización:

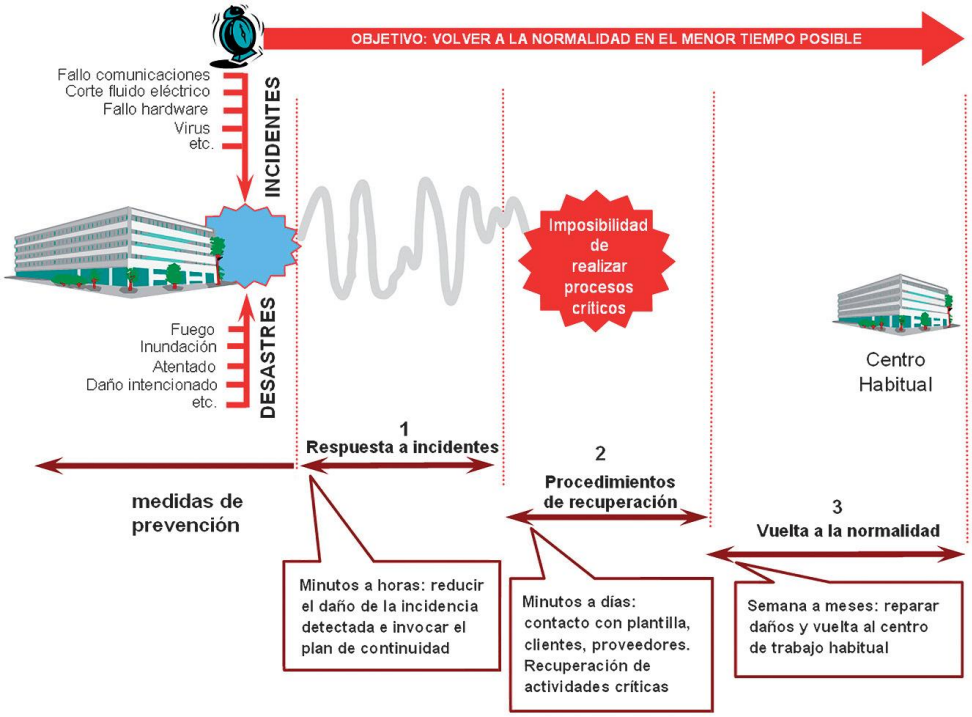

Ilustración 6. Etapas para la vuelta a la Normalidad

Fuente. Guía práctica para PYMES: Como implementar un plan de continuidad del negocio [5]

Las principales fases de para la recuperación y vuelta a la normalidad serian las siguientes:

Fase de respuesta a incidentes: Etapa en la que se identifican las fallas, se lanza el plan de continuidad a su funcionamiento y donde los equipos de desarrollo del plan toman sus posiciones frente a las actividades descritas en el BCP.

Procedimientos de Recuperación: Los procedimientos de recuperación son los principales pasos para lograr la estabilización de las actividades de la empresa y se detalla a continuación:

1. Análisis de incidentes
2. Análisis de impacto (Personal o infraestructura)
3. Análisis de tiempo de interrupción
4. Análisis de gravedad
5. Comunicación al personal encargado
6. Análisis de situación actual y reunión del comité organizacional

7. Activación del plan
8. Selección de áreas de urgencia máxima y procedimientos a poner en marcha

8. ETAPA 4. PRUEBAS Y MANTENIMIENTO

8.1. Pruebas del BCP:

La mejor forma de conocer si los procesos del plan de continuidad están bien establecidos y están cumpliendo con lo esperado, se debe desarrollar una forma de examinar los procesos del mismo. Los desarrolladores y participantes del BCP deben realizar pruebas continuas, midiendo los tiempos de ejecución y de tratamiento de las fallas encontradas, la idea es hacer pruebas que simulen la realidad pero que no afecten a la empresa al punto de dejarla vulnerable a cualquier daño.

8.2. Revisión y Mantenimiento:

Tras realizar las pruebas necesarias al BCP, se realiza el mantenimiento y revisión continua del BCP basándose en el plan de la mejora continua (Ver numeral 3.3.1.), este plan sirve como guía para el desarrollo de una revisión y mejora de las actividades del BCP, que tras cada actualización o mejora debe ser evaluada.

8.3. Auditoría Interna

Como parte fundamental del buen desarrollo del BCP en la empresa, es necesario realizar periódicamente y de manera programada auditorías internas de los procesos del plan. Esta auditoría debe ser transparente ya que ayuda al autocontrol de los recursos y actividades del BCP.

Esta auditoría tiene como objetivo:

- Evaluar los procesos del BCP y sus integrantes.
- Promover la adopción de mecanismos de autocontrol

- Efectuar recomendaciones sobre procesos y adecuaciones necesarias para hacer las cosas de la manera correcta.

Para realizar este tipo de auditorías es necesario crear un grupo auditor conformado por personas de todas las áreas y que den puntos de vista diferentes de las áreas y procesos auditados, de esta forma se lograra un proceso de control exitoso y con proyección positiva para el BCP y los objetivos de la empresa.

8.4. Revisión de la Dirección:

Tras la actualización o mantenimiento de alguna parte del BCP, ésta debe ser revisada y autorizada por la dirección y tras su aprobación se notificará del cambio a los integrantes de la organización para su conocimiento.

9. CONCLUSIONES Y RECOMENDACIONES

Tras realizar este trabajo se llego a las siguientes conclusiones:

El desarrollo e Implementación de un BCP, ayuda a afianzar los lazos al interior de la empresa y contribuye a que los integrantes de la organización desde sus directivos hasta las personas de más bajo nivel en la estructura organizacional de la empresa conozcan cómo funcionan sus procesos y comprendan cómo actuar en un momento de falla de las mismas.

Implementar un Plan de continuidad del negocio ayuda a conocer las actividades de la organización, a mitigar riesgos y conocer debilidades.

Tras la implementación y desarrollo del BCP se logra determinar la importancia de las actividades de la empresa y como resultado se sabrá cuál de estas actividades debe ser atendida en primera instancia y cuál sería el tiempo exacto para su recuperación.

Tras realizar este trabajo se determina que no es necesario el desarrollo de cada uno de los pasos aquí descritos ya que todo depende de las necesidades de la empresa. Como por ejemplo:

Si la falencia de la organización es causada por daños eléctricos en la edificación, no es necesario de la activación de la totalidad del plan, esta amenaza puede ser gestionada con gran sencillez y sin causar la activación de procesos de emergencia que solo hacen gastar recursos y tiempo de personal responsable de otras áreas de la empresa. En el caso contrario si la empresa afectada fuese una central eléctrica que vive y da beneficios a más personas y como tal sería necesario la activación total del BCP para lograr en el menor tiempo posible la recuperación de sus actividades y las de las personas afectadas a las cual la central presta sus servicios.

Si para la empresa no es primordial la tecnología se podrá enfocar en lo más importante para ella como tal podría ser la información, la materia prima o las personas como en el caso de los hospitales, y desarrollar sobre estos intereses estrategias para su protección.

Hay que recordar que las amenazas siempre estarán presentes en la empresa y que deben ser evaluadas y tratadas de manera constante, como por ejemplo:

El ingreso de personal a áreas de la organización: llevar el control continuo del ingreso de personal es fundamental para resguardar la seguridad de los recursos de la organización e implementar controles de acceso ayudará a la gestión de los posibles riesgos que sufriría la empresa al dar acceso a personas malintencionadas.

Documentar es parte vital de la empresa y del desarrollo del BCP, ya que con la ayuda de documentos actualizados se podrá evaluar las actividades realizadas a través del tiempo y se podrá mejorar los procesos y políticas de la empresa.

Recomendaciones:

Se recomienda realizar mantenimiento continuo del BCP, con base en los eventos transcurridos en el proceso de activación del plan, los eventos que vayan surgiendo luego de las continuas pruebas del plan y con los eventos externos ya sean políticos, tecnológicos o económicos que afecten directa o indirectamente a la empresa.

Establecer canales de comunicación adecuados para que tras un siniestro las personas puedan saber cómo y cuándo activar el plan.

Usar todos los medios posibles para que los integrantes de la empresa tengan pleno conocimientos de los procesos del BCP.

Realizar una documentación de todo lo sucedido antes, durante y después de la activación del BCP ya que esta información ayudará a la mejora continua del mismo.

Tener claro la cantidad y calidad de recursos que se deben tener para el desarrollo e implementación de un plan de continuidad del negocio

Se debe saber cómo transportar a los empleados y las herramientas necesarias hacia la sede alterna para dar comienzo a las actividades de la continuidad según lo establecido en el BCP.

Es fundamental dejarle claro a la Dirección la importancia del BCP y gestionar el compromiso de la organización al desarrollo e implementación de los planes de continuidad.

BIBLIOGRAFÍA

[1] https://www.pwc.com/ve/es/asesoria-gerencial/boletin/assets/boletin-advisory-edicion-09-2008.pdf (Consultada 8/Julio/2012).

[2] http://www.pdca.es/pruebas/pdca.html# (Consultada 8/Julio/2012).

[3]http://www.sisteseg.com/files/Microsoft_Word_-_BIA_BUSINESS_IMPACT_ANALYSIS.pdf (Consultada 12/Agosto/2012)

[4] Norma Técnica NTC Colombiana 5722 2009-11-18, Gestión de la Continuidad del Negocio. Requisitos, e: bussiness continuity management. Specification Correspondencia, Editada por el Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC), pag.12

[5] Guía práctica para PYMES: Como implementar un plan de continuidad del negocio, Pág. 33, http://www.inteco.es/file/t2sHW92KsAV506ZWcHTKRg (Consultada 29/9/2012)

[6] Information Security and Risk Management – CHAPTER 3 Pag.54

[7] ISO 27005 – Tecnologías de información, Técnicas de Seguridad – Administración de manejo de la información, (Consultada 8/Julio/2012)

[8] http://www.pmi.org/PMBOK-Guide-and-Standards.aspx (Consultada 8/Julio/2012)

[9] Instituto Nacional de Tecnologías de la Comunicación GUÍA AVANZADA DE GESTIÓN DE RIESGOS - Diciembre 2008, Pag.55

[10] Instituto Nacional de Tecnologías de la Comunicación GUÍA AVANZADA DE GESTIÓN DE RIESGOS - Diciembre 2008, Pag.56

[11] All in one – CISSP Exam Guide – Shon Harris, McGraw-Hill Osborne Media; 5 edición (2010)

[12] Una introducción al análisis de riesgo; Asociación Colombiana de Ingenieros de Sistemas - http://www.acis.org.co/fileadmin/Conferencias/ACIS-Riesgos.pdf (consultada 31/8/2012)

[13] http://www.ull.es/publicaciones/latina/16egidos.htm (consultada 04/10/2012)

ANEXO 1. Tabla Comparativa de Normativas

Normas de Continuidad del Negocio	**ESTANDAR INTERNACIONAL ISO/IEC 27001-2005 Tecnología de la Información- Técnicas de Seguridad- Sistemas de gestión de Seguridad de la Información - Requerimientos SGSI**	**PROYECTO NORMA MERCOSUR ISO/IEC 27002: 2007 Tecnologías de la información - Código de Buenas Prácticas para la gestión de la seguridad de la información.**	**NORMA TECNCA COLOMBIANA NTC 5722 Gestión de la Continuidad del Negocio. REQUISITOS (Adopción Idéntica por Traducción de la BSI 25999-2007).**	**NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY NIST 800-34 Contingency Planning Guide for Information Technology Systems, Rev 1**	**STANDARD ON DISASTER/EMERGENCY MANAGEMENT AND BUSINESS CONTINUITY PROGRAMS NFPA1600:2010**	**ORGANIZATIONAL RESILIENCE ASIS SPC.1-2009: Security, Preparedness, and Continuity Management Systems – Requirements with Guidance for Use**
Fecha de publicación	Primera edición 2005-10-15		18/11/2009	Mayo/2010	05/12/2009	12/03/2009
Desarrollador	Comité Técnico Conjunto ISO/IEC JTC 1, Tecnología de la información, Subcomité SC 27, Técnicas de seguridad TI.	Comité Técnico Conjunto ISO/IEC JTC 1, Tecnología de la información, Subcomité SC 27, Técnicas de seguridad TI.	El Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC)	NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY	NFPA - National Fire Protection Association, FEMA - Federal Emergency Management Agency, Nema Electrical Manufacturers Association, IAEM - International association of emergency managers.	American National Standard for Industrial Security
Normas base	La base de esta normativa es la norma BS 7799-2:2002, desarrollada por la entidad de normalización británica, la British Standard Institution (BSI)	La base de esta normativa es la norma ISO/IEC 17799 la cual le fue asignada el número 27002 en el año 2007	La base de esta normativa es la BSI 25999-2:2007 y la Guía Técnica Colombiana (GTC 176).	FIPS 199, NIST 800-53	Esta normativa no especifica si está relacionada con otra normativa.	ISO 73:2002-Risk Management-Vocabulary-Guidelines for use in standards, ISO 9001:2000-Quality management systems, ISO14001:2004-Enviromental management systems
Descripción	Norma creada para fomentar en las organizaciones y sus integrantes, el desarrollo de un ambiente adecuado para establecer la seguridad de la información y donde no se fomenta el despliegue de tecnología o de infraestructura.		Normativa creada para hacer énfasis en la importancia de comprender las necesidades de la continuidad del negocio estableciendo políticas que ayuden a la seguridad de la información y la vida de la organización.	Guía de Planes de Contingencia para la Tecnología de la Información, proporciona instrucciones, recomendaciones y consideraciones para la planificación de contingencia del gobierno de TI.	Normativa creada para ayudar a las instituciones a identificar, analizar y crea soluciones a riesgos presentes en su interior y en el ambiente en que se desempeñan	Esta norma está diseñada para que pueda ser integrada con calidad, seguridad, medio ambiente, seguridad de la información y riesgos.

Función	Educar y enseñar a las organizaciones a **establecer, implementar, operar, monitorear, revisar, mantener y mejorar** los sistemas de gestión de la seguridad de la información SGSI , fomentar estas prácticas como base para el desarrollo de un Plan de Continuidad del Negocio (BCP).	Esta Norma establece recomendaciones y principios generales para **iniciar, implantar, mantener y mejorar la gestión de la seguridad de la información** en una organización. Los objetivos señalados en esta Norma proporcionan recomendaciones generales sobre las metas comúnmente aceptadas para la gestión de la seguridad de la información.	Esta norma técnica colombiana especifica los requerimientos para **planificar, implementar, supervisar, mantener y mejorar** los sistemas de gestión de la continuidad del negocio.	Definir los siete pasos del proceso de los planes de contingencia de la organización y como se integran a los escenarios del ciclo de vida de desarrollo de sistemas. 1. desarrollo de políticas que ayuden a orientar el desarrollo de un plan de contingencia efectivo 1. crear políticas 2. análisis de impacto del negocio (BIA) 3. identificar controles preventivos 4. crear estrategias de contingencia 5. desarrollar el plan de contingencia 6. test del plan de contingencia 7. Realizar mantenimiento del plan de contingencia	Esta normativa abre la mente de las personas integrantes del grupo que desarrollará el programa y ayuda a dejar en claro la identificación, análisis y desarrollo de soluciones de riesgos que ayuden a la continuidad del negocio frente a los riesgos encontrados en el medio o al interior de la empresa.	Esta normativa está enfocada en los sistemas de gestión integral de la seguridad, preparación, respuesta, mitigación, de incidentes perturbadores que resultan en una emergencia, crisis o desastre. Esta normativa se desarrolla enfocada a los procesos para lograr el éxito, esta metodología propende a la mejora continua ya que proporciona la manera de establecer, mantener y mejorar la organización.

Para que se implementa	Se implementa para dar orden a la gestión de la seguridad de la información en la organizaciones.	Se implementa como principios básicos de las practicas de la seguridad	Se implementa para evaluar la capacidad de la organización para cumplir con las necesidades de la continuidad del negocio.	Se implementa esta normativa para el desarrollo efectivo de los planes de contingencia.	Se implementa para establecer de manera clara los pasos para mantener, implementar y desarrollar el programa de prevención	La aplicación de un sistema de procesos dentro de una organización, junto con la identificación e interacciones de estos procesos y su gestión, puede ser referido como un "enfoque de proceso". Que ayuda a: a) Comprender el riesgo de una organización, seguridad, preparación, respuesta, continuidad, y los requisitos de recuperación; b) El establecimiento de una política y objetivos para la gestión de riesgos; c) Implementar y usar los controles para gestionar los riesgos de la organización dentro de la contexto de la misión de la organización; d) Supervisar y revisar el desempeño y la eficacia de la gestión del RO(organizational resilience) sistema; y e) La mejora continua basada en mediciones objetivas.
En que se enfoca la norma?	Esta norma se enfoca en hacer entender a los integrantes de la organización la importancia del desarrollo y mejoramiento de los procesos que gestionan la seguridad de la información	Establecer normativas que ayuden a la organización a controlar los riesgos que afectan a la organización.	Se enfoca en dar a entender cómo crear un sistema de gestión de la continuidad del negocio que sea apropiado para la organización y sus integrantes.	Se enfoca en dar la guía necesaria para el desarrollo de planes de contingencia.	Se enfoca en dar a la persona encargada de la continuidad del negocio los criterios para evaluar los riesgos y poder crear soluciones a los riesgos encontrados.	Esta normativa se enfoca en desarrollo de procesos que permitan la continuidad del negocio y la comprensión y mitigación de riesgos

Objetivos de la norma	Entender las necesidades de la organización. Comprender el objetivo de las políticas de seguridad de la información. Implementar controles que ayuden a la seguridad de la información. Monitorear la efectividad de los cambios y procesos establecidos para la seguridad de la gestión de la información. Mejoramiento continuo de los procesos que garanticen que a futuro no se presentaran problemas de seguridad.	El objetivo de esta norma es establecer controles para iniciar, implementar, mantener y mejorar la gestión de la información y alcanzar los requerimientos de la evaluación de riesgos	Su objetivo es definir los límites a los cuales deben llegar los sistemas de gestión de la continuidad del negocio, dejando claro los procesos que se deben realizar para implementar, mantener y mejorar la gestión de la continuidad.	El objetivo de esta guía es identificar los principios fundamentales de planificación para desarrollar y mantener los planes de contingencia. Este documento sirve de guía para ayudar al personal a evaluar los sistemas de información y las operaciones para determinar los requisitos de contingencia y prioridades.	Propósito. Esta norma establece los criterios fundamentales para desarrollar, implementar, evaluar y mantener el programa para la prevención, mitigación, preparación, respuesta, continuidad y recuperación.	Esta norma permite a una organización:a) Desarrollar un programa de prevención, preparación, respuesta, continuidad y política de recuperación; b) Establecer los objetivos, procedimientos y procesos para alcanzar los compromisos de la política; c) Asegurar la competencia, el conocimiento y la capacitación; d) Establecer indicadores para medir el desempeño y demostrar el éxito; e) Adoptar las acciones necesarias para mejorar el rendimiento; f) Demostrar la conformidad del sistema con los requisitos de esta norma, y g) Establecer y aplicar un proceso para la mejora continua.
Qué modelo adapta para su desarrollo PDCA o SDLC	**PDCA**	**PDCA**	**PDCA**	**SDLC** o ciclo de vida de desarrollo de sistemas que tiene como fases primordiales: Fase inicial, Desarrollo / fase de adquisición, fase de implementación, fase de operación / mantenimiento, fase de eliminación	**PDCA**	**PDCA**
Que es la seguridad informática?	No tiene un concepto fijo de lo que es la seguridad.	La seguridad de la información es la protección de la información contra una amplia gama de amenazas para asegurar la continuidad del negocio, minimizar los daños al negocio y maximizar el retorno de las inversiones y las oportunidades de negocio.	No tiene un concepto de lo que significa la seguridad de la información.	No tiene un concepto de lo que significa la seguridad de la información.	En esta normativa no se especifica el significado de seguridad informática	En esta normativa no se especifica el significado de seguridad informática

Actividades expuestas en la norma que se involucran en el PDCA, SDLC o la metodología usada para el desarrollo del BCP	**Planear**	Desarrollar un plan donde se establezcan las características de la organización, los métodos de evaluación del riesgo, los alcances y como se evaluarán los resultados, además de establecer la prevención de errores, detección y respuestas a las fallas, mantenimiento periódico del plan, revisión y auditoría del mismo y sus funciones primarias.	Determinar los valores, objetivos y principios que la organización ha fijado para dar un apoyo firme a sus procesos, Valoración de los riesgos de la organización, con ésta se identifican las amenazas, se evalúa la vulnerabilidad y la probabilidad de su ocurrencia y se estima como será el impacto para la organización. Toma como fuente el conjunto de requisitos legales, que ayudan al buen desempeño de las funciones de la organizaciones.	Identificar las principales actividades y productos que deben estar dentro de la gestión de continuidad que se desea establecer, determinar las políticas de continuidad del negocio, las metas, objetivos, controles, procesos y procedimientos que se deben realizar para la gestión del riesgo y la mejora de la continuidad del negocio para entregar resultados acordes con las políticas y objetivos generales de la organización.	**Fase inicial**	Se realiza el estudio de cómo será desarrollado el sistema. Se determinará si el sistema será creado para trabajar bajo un entorno controlado o bajo condiciones inusuales, se determinan los requerimientos necesarios para el desarrollo efectivo del sistema, además se debe establecerá el nivel de recuperación que debe tener todo el sistema para garantizar el funcionamiento óptimo de los sistemas a desarrollar.	**planear**	Esta etapa se basa en determinar, el propósito y la aplicación del plan de continuidad a desarrollar. Aquí se definen la metodología a usar, las políticas que regirán a todo el BCP en su desarrollo, implementación y mantenimiento, se determina cual será el coordinador del programa y el comité con el cual se trabajara todo el programa de BCP, además se determinara el tiempo de evaluación del programa.	En esta normativa se destaca la importancia de definir el alcance de las actividades que se desarrollarán en la organización, la misión y visión del BCP, definir los activos a usar, hacer un análisis de riesgos internos y externos que afectan a la organización, además de un análisis de impacto (BIA) que ayudará a definir la gestión de emergencia, desastres y la continuidad del negocio. La organización debe desarrollar políticas donde se haga énfasis en el compromiso, donde se incluya el compromiso de no infringir la ley, donde se establezca la revisión continua de los procesos de la organización en beneficio de la continuidad, todo esto debe ser documentado ya que puede servir para evaluar todas las actividades de la organización, además de determinar los tiempos de recuperación, los costos y los beneficios y llevar un histórico de los riesgos e impactos encontrados.

Actividades expuestas en la norma que se involucran en el PDCA, SDLC o la metodología usada para el desarrollo del BCP	**Hacer**	Formulación del plan de tratamiento de riesgos y actividades de mejoramiento de la seguridad, capacitar a los empleados para su optima reacción. Establecer políticas, objetivos, roles y responsabilidades a los integrantes de la organización que ayuden a la activación del plan de seguridad. Establecer el compromiso que la gerencia tiene en el desarrollo de la gestión de la seguridad describiendo las políticas para el mismo y su responsabilidad, se debe determinar los recursos a usar en el desempeño y mantenimiento de la gestión. Se manejará como base para la integración de la gestión de la seguridad la prevención, la detección, la respuesta inmediata, el mantenimiento, la revisión y auditoría en todas las actividades realizadas.	Desarrollar en el interior de la organización controles que se consideren esenciales para el buen desarrollo de las actividades de la empresa tales como: protección de datos personales, protección de registros de la organización, derechos de propiedad intelectual, documentación de las políticas, asignación de responsabilidades, concientización y capacitación de la información, gestión de la continuidad del negocio, se debe determinar los controles dependiendo de los riesgos que la empresa desea enfrentar y sobre todo los logros que la organización se ha propuesto.	Implementar y ejecutar la política, los controles, procesos y procedimientos de la continuidad del negocio	**Desarrollo / fase de adquisición**	Se deben especificar los requerimientos del sistema, detallar como van a ser sus funciones de manera que se puedan evitar fallas a futuro y donde la corrección de los errores se reduzcan y donde se pueda garantizar la fiabilidad y disponibilidad durante la fase de operaciones.	**Hacer**	Esta fase del PDCA se basa en tener claro la administración de recursos, la comunicación y las alertas anticipadas, la asistencia de terceros con los que se tenga acuerdos, la implementación de los procesos desarrollados para la mitigación de las amenazas, implantar en los empleados la cultura del BCP, en esta etapa se pone en funcionamiento el BCP se gestiona la administración de incidentes y se ponen en práctica las operaciones de emergencia.	En esta etapa las directivas de la organización deben asignar responsabilidades y los recursos necesarios para llevar a cabo las actividades del sistema de gestión, Además se debe realizar entrenamiento continuo sobre el funcionamiento del sistema, se debe comunicar continuamente los cambios sobre el sistema o la organización. La organización debe documentar todo lo sucedido con los procesos actuales o nuevos. Se debe velar por la seguridad de la documentación que servirá como histórico para evaluaciones posteriores, en esta etapa se debe llevar un control de los procesos que van ser activados y de los riesgos encontrados en la etapa de planeación. En esta etapa se desarrolla y se pone en práctica los procedimientos de respuesta desarrollados tras los resultados del BIA.

Actividades expuestas en la norma que se involucran en el PDCA, SDLC o la metodología usada para el desarrollo del BCP	**Chequear**	Se deben realizar procedimientos de revisión continua de las actividades de la gestión de seguridad y si su desempeño está cumpliendo con los objetivos planteados, desarrollar auditorias para verificar si lo dicho anteriormente es verdadero y si cumplen con los requerimientos legales, tras estas revisiones se deben tomar decisiones de modificación, actualización o desarrollo de nuevas políticas o procedimientos que ayuden a la efectividad de la gestión, además de la revisión debe tener en cuenta la prevención, detección, respuesta inmediata y mantenimiento de todo este proceso.	Revisión continua de las políticas de seguridad que ayuden a su mejoramiento, registrar los resultados de la implementación de políticas de versiones anteriores, mejorar continuamente el objetivo de los controles, mejorar la asignación de recursos que ayuden al desarrollo de los procesos de la seguridad de la información, evaluar periódicamente los riesgos actuales y los futuros para determinar su alcance y posibilidad de ocurrencia.	Supervisar y revisar el desempeño frente a los objetivos y la política de continuidad del negocio, reportar los resultados para su revisión y determinar y autorizar las accione destinadas a remediar y mejorar.	**fase operación / mantenimiento**	Se debe establecer la importancia de los sistemas de la empresa para de esta forma diseñar como será el método de recuperación, el plan de recuperación debe actualizarse de manera periódica con las lecciones aprendidas y las mejoras realizadas.	**Chequear**	La entidad debe evaluar los planes, procedimientos y capacidades a través de pruebas periódicas y ejercicios. Las pruebas realizadas deben ser realizadas de manera periódica dependiendo de las necesidades de la empresa. Las pruebas deben ser desarrolladas enfocadas a identificar bondades del BCP o deficiencias del mismo, aclarar funciones y responsabilidades, mejoramiento entre los equipos que intervienen en el BCP, Identificar recursos adicionales y evaluar las políticas y controles implementados en el BCP.	En esta normativa se describe la necesidad de verificar periódicamente con pruebas e informes posteriores a incidentes los la funcionalidad de los procesos, con estas evaluaciones se debe reflejar el cambio inmediato en los procedimientos. La organización debe establecer métricas de rendimiento de los procedimientos que ayuden a medir de forma regular su comportamiento. La organización debe realizar un programa de auditoría planificada, tomando en consideración el estado y la importancia de los procesos y las áreas a auditar, así como los resultados de auditorías previas.

Actividades expuestas en la norma que se involucran en el PDCA, SDLC o la metodología usada para el desarrollo del BCP	**Actuar**	Se deberá mantener y mejorar el sistema de gestión implementado en la empresa al tomar acciones correctivas o preventivas que ayudarán a la eficiencia del Sistema de gestión, se tomará registro de las decisiones tomadas para llevar un control que servirá para estudios posteriores		Mantener y mejorar el sistema de gestión de continuidad del negocio llevando a cabo actividades preventivas y correctivas de los procesos o procedimientos de la organización con base en los resultados de las revisiones hechas sobre todas las actividades y controles implementados en la organización.	**fase de implementación**	En esta fase aunque se sabe que el sistema implementado esta bajo pruebas constantes se debe asegurar que las estrategias a usar sean acordes a las necesidades y si cumplen con lo planeado, para tal caso es debido realizar un plan de pruebas donde se probaran detalladamente las estrategias de la contingencia.	**Actuar**	La entidad debe mejorar la eficacia de los objetivos, políticas y procesos que se establecen en el BCP. En esta etapa del PDCA se evalúa nuevamente cualquiera de las situaciones documentadas desde la activación del BCP hasta el momento donde se llega a la normalidad de las actividades, aquí se corrige el BCP basándose en las lecciones aprendidas.	La dirección revisará el sistema de gestión de la organización y se asegurara de la adecuación y eficacia, con esta revisión debe incluir la mejora y la necesidad de cambios en el sistema. La dirección debe basar la revisión en los resultados de las auditorias anteriores y en el resultado de los procesos implementados, tras la revisión de toda esta información se deben realizar cambios en las políticas y los objetivos que afecten positivamente a la organización.
					fase de eliminación	En esta fase se especifica que los equipos que saldrían de la empresa también deben salir del BCP pero antes debe existir un reemplazo en total funcionamiento de las funciones con las cuales venía trabajando el equipo a reemplazar			

Puntos para dar comienzo al plan	1. Obtener apoyo de la gerencia.	1. La dirección debería apoyar activamente la seguridad dentro de la organización atreves de una orientación clara y la asignación explicita de responsabilidades.	1. Establecer que la dirección tenga un compromiso con las políticas y planes de la gestión de la continuidad del negocio.	1. Se debe tener muy encuentra la opinión de los gerentes y coordinadores para tener éxito en las actividades del plan de contingencia.	1. En primera instancia es importante que la gerencia de vía libre a el coordinador y al comité de programa de desarrollar actividades dentro de la empresa, que contribuyan a la continuidad.	1. Se desarrolla un documento por escrito donde se determine el compromiso de la dirección, donde se establezca que la gerencia está comprometida con el desarrollo del sistema de gestión, donde la gerencia se encargue de comunicar la importancia del sistema de gestión y donde la gerencia proporcione los recursos necesarios para implementar y mantener el sistema de gestión
Puntos para dar comienzo al plan	2. Definir roles y responsabilidades.	2. La asignación de responsabilidades de seguridad de la información debe hacerse de acuerdo a las políticas de seguridad y complementada con guías de implementación y desarrollo	2. Se debe definir y documentar de manera detallada y con claridad los roles, funciones, responsabilidades, competencias y los responsables de activar el plan.	2. Según esta normativa es paso fundamental definir detalladamente los roles y las responsabilidades de las personas que intervienen en el desarrollo del plan de contingencia.	2. Según esta norma en un plan de emergencia se debe asignar responsabilidades a la organización y a los ínvidos para ejecutar acciones especificar en tiempos y lugares predeterminados en caso de emergencia.	2. La alta dirección deberá designar representantes en cada una de las áreas que conforman la empresa, con responsabilidades definidas con las cuales podrá implementar sistemas de gestión.
Puntos para dar comienzo al plan	3. Definir el alcance.	3. Definir hasta donde podrá llegar el plan y en qué casos son los que no cumple con lo requerido.	3. La organización debe determinar el alcance de la gestión de la continuidad del negocio y establecer sus objetivos primordiales.	3. Esta normativa no expone la importancia de definir el alcance del plan a desarrollar.	3. Esta normativa explica la importancia de establecer las metas, objetivos y el alcance del Programa a desarrollar.	3. La organización debe definir los límites del programa, requisitos teniendo en cuenta la misión de la empresa, los escenarios de riesgo.
Puntos para dar comienzo al plan	4. Desarrollo de políticas para el SGSI.	4. Desarrollar un documento con las políticas que se implementaran y los resultados de las mismas después de la puesta en marcha dentro de los procesos de la organización.	4. Establecer un documento detallado donde se haga referencia a los objetivos, alcances y limitaciones de la políticas a implementar, estas deben estar aprobadas por las directivas y debe ser comunicada adecuadamente a todos los integrantes	4. Esta normativa específica que se debe Identificar los requisitos legales o reglamentarios para los planes de contingencia • Declaración de política • Obtener la aprobación de la política • Publicar Desarrollar políticas de Contingencia	4. La entidad debe desarrollar políticas que definen la autoridad competente, la misión y visión, las metas, el manejo de las políticas y procedimientos, las leyes y normas que regirán el programa desarrollado.	4. La organización deberá desarrollar políticas donde se tome la importancia del compromiso de los empleados, el compromiso de la mejora continua, se desarrollarán políticas para garantizar el compromiso con la mejora continua.

Puntos para dar comienzo al plan	5. Definir la metodología para el análisis de riesgos	5. Identificar, cuantificar y priorizar los riesgos contra los criterios de aceptación de riesgo, además de estimar su magnitud y su importancia para esto se debe en primera instancia determinará los activos involucrados y los procesos básicos de la organización.	5. Permitir que la organización determine las actividades criticas y los recursos necesarios que sirven para sus principales servicios. Entender las amenazas a las que están expuestos sus actividades, establecer cuál va a será el método para determinar el impacto de los riesgos encontrados, el tiempo de reacción para reiniciar las actividades, dar niveles de importancia para reinicio de actividades y determinar los activos que son necesarios para iniciar las procesos de recuperación. Todo esto debe estar documentado de tal manera que sea claro para la organización determinar lo que pasaría si una amenaza identificada se vuelva realidad.	5. Esta normativa no especifica qué metodologías deben utilizase para el análisis de los riesgos pero explica la importancia de identificar los procesos, recursos y determinar la prioridad que se debe tener con los recursos críticos de la empresa.	5. Esta normativa explica que la entidad debe identificar riesgos, la probabilidad de ocurrencia y la vulnerabilidad ante los riesgos naturales, tecnológicos y humanos, tras el análisis de estos riesgos se debe analizar el impacto que estos tendrán en la vida continua de la organización.	5. En esta normativa se da mucha importancia a la evaluación y análisis de impacto. Esto se logra con la identificación de los activos y actividades críticas para el funcionamiento de la empresa, además de la identificación y cálculo del impacto de los riesgos es necesario analizar la prioridad de los controles y tratamientos de los riesgos encontrados.

Puntos para dar comienzo al plan	6. Dar solución al riesgo aplicando controles y documentar lo realizado (Histórico).	6. Esta normativa explica que las organizaciones después de evaluar la importancia de los riesgos que las afectan se debe determinar el tratamiento de las mismas, para este caso la organización tendrá la opción de aceptar determinado riesgo dependiendo de los alcances que tenga este riesgo en la organización, otra opción es evitar los riesgos minimizando por completo su ocurrencia y creando estrategias para su control total o parcial.	6. La organización debe conocer en detalle sus actividades criticas y la solución a los riesgos que estas puedan sufrir, los encargados de implementar el SGCN deben poner en práctica soluciones que reduzcan la probabilidad de interrupción y el tiempo de dichas interrupciones, la organización debe implementar soluciones adecuadas al nivel de aceptación del riesgo que se determino en el análisis de riesgos y se debe documentar de tal forma que para futuras interrupciones se pueda responder con eficacia y de forma oportuna a alguna amenaza.	6. Tras determinar los riesgos y lo que estas amenazas afectarían a la empresa, se determina que se debe identificar los controles preventivos y se deben desarrollar estrategias de recuperación como: Backup, lugares alternativos, Reemplazo de equipos, Establecer roles y responsabilidades, esta información debe ser documentada de manera detallada para que sirva como guía a las personas que hacen parte de la implementación del BCP	6. La entidad debe implementar estrategias para eliminar el riesgo o mitigar los efectos del peligro, debe realizar identificación y análisis de riesgos de las amenazas presentes en la naturaleza, en los recursos humanos y la tecnología.	6. La organización tras el estudio de los riesgos está preparada para el tratamiento y la implementación de controles para la mitigación de los riesgos encontrados, para la empresa y las directivas es muy importante la documentación
Puntos para dar comienzo al plan	7. Declarar la aplicabilidad de los controles y explicar en detalle el o los objetivos de estos.	7. Describir los alcances y los objetivos de la estrategia para así ser implementada.	7. La organización debe detallar la forma como se gestionaran los incidentes en el momento y después de que se manifieste.		7. Esta normativa debe definir los objetivos del programa y el modo en la que se relaciona con las políticas de la organización.	7. Los controles establecidos deben ser detallados para no causar confusión a las personas que contribuyen a la implementación y desarrollo del programa.

Puntos para dar comienzo al plan	8. Plan de tratamiento de Riesgos, detalla cómo se va a implementar el control, en qué momento, porque personas, etc.	8. Determinar en detalle que actividades se desarrollaran para mantener la organización en funcionamiento.	8. La organización debe contar con planes documentados que detallen como la organización va a gestionar el incidente, como se recuperara y como se mantendrá en funcionamiento en el momento de una emergencia.	8. Esta normativa trata de identificar los procesos críticos, el tiempo fuera de servicio y las prioridades de recuperación, tras esto se identifican las estrategias de recuperación y se explica en detalle su funcionamiento.	8. Esta normativa habla de manera muy sencilla sobre tratamiento de riesgos y sobre los puntos de vista que se deben tener en cuenta para la identificación, análisis y mitigación de los riesgos y vulnerabilidades e las personas, los bienes, el medio ambiente.	8. la organización debe tener un detallado documento de todas las actividades de la organización y de los tratamientos desarrollados y el resultado obtenido tras aplicar el tratamiento al riesgo encontrado.
Puntos para dar comienzo al plan	9. Definir cómo se va a medir el cumplimiento de los controles propuestos.	9. Desarrollar auditorias de las actividades y resultados de los controles y estrategias implementadas.	9. La dirección debe revisar el SGCN de manera periódica para evaluar las oportunidades de mejora y las necesidades de cambio.	9. Esta normativa no especifica cómo medir el cumplimiento del BCP.	9. Esta normativa no especifica cómo medir el cumplimiento del BCP.	9. La organización debe documentar todo lo realizado y debe tomar datos medibles para probar la eficiencia de los procesos activos y si han cumplido con lo establecido en el programa.
Puntos para dar comienzo al plan	10. Implementar controles y procedimientos que serian obligatorios.	10. Determinar los pasos a seguir de los controles implementados con las actividades de los usuarios de la organización y las partes externas que intervienen en la seguridad.		10. Determina los pasos a seguir en el desarrollo del BIA que sirve para determinar lo métodos de control y el impacto que tienen las fallas en las actividades de la empresa.	10. Aunque no son muy detallados, esta normativa da ideas de cómo se debe controlar y que procedimientos se deben tener en cuenta para el desarrollo de cualquier programa que ayude al mejoramiento y control de los procesos de la empresa.	

Puntos para dar comienzo al plan	11. Capacitar y sensibilizar a los integrantes de la organización con los temas de reforma con la esperanza que todos hagan de forma correcta las actividades de seguridad.	11. Concientizar, educar y formar en seguridad de la información a los empleados de la organización donde se haga hincapié en las responsabilidades, el buen uso de los recursos de la empresa, en la actualización de las políticas y en la importancia de seguir las normativas para que la organización siga en pie ante cualquier emergencia.	11. Asegurarse que se vuelva cultura en la empresa todos los procesos que se establecen en el sistema de gestión de la continuidad, la organización debe ofrecer la concientización, compromiso, formación y entrenamiento a los integrantes de la organización y determinar las competencias necesarias para las personas que estarán bajo el sistemas de la gestión de la organización que se desea implementar, la gerencia debe asegurarse de que los conocimientos del personal sean aptos para su buen desempeño y para el éxito de el SGCN.	11. Esta normativa nos indica que la mejor forma de capacitar a los integrantes de la organización es desarrollando de manera periódica planes de prueba donde se simule la peor situación o la situación con más probabilidad de ocurrencia. Los métodos de capacitación serian en salones de clase simulando casos reales, simulando emergencias en las instalaciones.	11. Esta normativa explica la importancia de realizar capacitaciones a los empleados realizando actividades de prueba en la organización y el objetivo de este plan de capacitación es fomentar conciencia y mejorar el conocimiento y destrezas de las personas de la empresa, se deben llevar registros de capacitación y de los temas tratados como: los impactos potenciales, la preparación a tener en cuenta y la información necesario para desarrollar entre todos un programa de mitigación.	11. La capacitación y el entrenamiento contante de los integrantes de la organización es fundamental para garantizar el desarrollo efectivo los tratamiento realizados ante los riesgos encontrados tras un análisis de los riesgos.
Puntos para dar comienzo al plan	12. Llevar a nivel operativo el SGSI y comenzar con el registro de las actividades.	12. Las actividades realizadas deben ser documentadas con minucioso detalle, dando a conocer los procesos, metodologías utilizadas y manejo de errores, esta información debe estar al alcance de cualquier persona que lo necesite, esta documentación debe ser tratada como un documento formal y debe ser autorizado y realizado			12. en esta normativa no se especifica la menara como se debe activar el programa desarrollado, pero deja claro que es necesario la documentación de las actividades que serán revisadas posteriormente por la gerencia o directivos de la empresa.	12. Esta normativa deja en claro la importancia de llevar registros en la totalidad del desarrollo del programa de gestión.

		por la dirección.				
Puntos para dar comienzo al plan	13. Supervisar las actividades del proyecto SGSI y determinar con los resultados si se cumplen con los objetivos planteados.	13. Revisión independiente a intervalos planificados los procesos, políticas y procedimientos que se enfocan en la seguridad de la información, deben ser registrados y evaluados para determinar si cumplen con la orientación declarada en el documentos de políticas de la seguridad.	13. Al realizar revisiones continuas y de manera programada se determina si se está cumpliendo con lo planificado en el SGCN.	13. Para esta normativa es fundamental la supervisión de los procesos y practicas realizadas sobre el BCP, ya que esta vigilancia continua ayudara a controlar si los procesos y actividades diseñadas logran lo esperado, además tomar lo observado para crear nuevas prácticas o modificaciones del BCP	13. En esta normativa se sugiere la revisión periódica de las actividades del programa implementado, y la necesidad de la documentación del mismo para futuros análisis y mejoras.	13. La gerencia y los integrantes del las áreas encargadas del programa están en la obligación de realizar una revisión permanente de todos los procesos realizados en la activación y después de realizar los tratamientos necesarios sobre las amenazas encontradas.

Puntos para dar comienzo al plan	14. La organización debe desarrollar una auditoría interna periódica donde se vigile detalladamente si los procesos y actividades establecidos en la SGSI cumplen con los objetivos del proyecto y donde muestren las falencias y de proyecten las soluciones.	14 - 15. Revisar el enfoque de la organización hacia la gestión de la seguridad de la información de forma periódica y determinar si las estrategias están bien enfocadas o si es necesario la reevaluación de los controles. Al terminar la revisión se debe documentar los hallazgos y las correcciones realizadas para su buen desempeño	14 - 15. Revisión de las políticas en intervalos planificados y cuando ocurra cambios significativos de las mismas. Además de asegurarse que la organización realice auditoría interna y de autoevaluación del SGCN para revisar la efectividad, la idoneidad de la políticas y objetivos que se plantearon con anterioridad. Las revisiones realizadas en la organización deben ser documentadas para futuras auditorias que permitan determinar si se cumplió o no la mejora de los procesos afectados por las amenazas		14 - 15. Esta normativa revisa periódicamente la disponibilidad de recursos, la infraestructura, los cambios de la organización y todo esto para verificar si se llega a lo esperado o no, y esta auditoría debe ser documentada con las opiniones, y evaluaciones realizadas.	14-15 La gerencia debe formar un equipo de auditores que revisen de manera periódica las actividades y lograr analizar la eficiencia de lo establecido desde el principio del programa de gestión, es de recordar que todo proceso por los auditores debe ser documentado en detalle tras cada actividad realizado y tras cada nuevo hallazgo.

Puntos para dar comienzo al plan	15. Revisión del SGSI para determinar periódicamente su eficacia, y dando oportunidad de cambio o mejoramiento de las falencias encontradas, además de la documentación de lo encontrado y de las necesidades que servirán para mejorar los procesos.			15 - 16. En esta normativa se explica que el plan de continuidad del negocio debe estar bajo una revisión continua ya que la tecnología y la vida de la empresa y todo lo que la rodea puede cambiar de manera constante, como regla general para todo BCP este debe revisado constantemente y dicha revisión debe centrarse en los siguientes elementos: requisitos operacionales, requisitos de seguridad, procedimientos		

Puntos para dar comienzo al plan	16. Acciones preventivas y correctivas de los errores encontrados, estas acciones deben ser aplicadas en los tiempos y en las actividades correctas y que son vitales para el buen funcionamiento de la organización.		16. La organización debe mejorar la eficiencia del SGCN a través de acciones preventivas que protejan de manera anticipada a la organización de problemas potenciales y acciones correctivas que eliminen las amenazas y que aseguren la no ocurrencia de las mismas, estas acciones deben estar acordes a la magnitudes de la amenaza y deben estar acorde a los objetivos de la organización.	técnicos hardware, software y otros equipos (tipos, especificaciones y cantidad), nombres e información de contacto de proveedores, incluyendo alternativo y fuera de las instalaciones del proveedor, alternativas y requisitos de las instalaciones fuera del sitio estos puntos son utilizados normalmente para conocer el funcionamiento y verificar que los procesos están en correcto estado y si están cumpliendo con los esperado	16. Esta normativa deja en claro que es necesario establecer procesos de acción correctiva para subsanar las deficiencias encontradas, esta normativa no es clara en la manera de desarrollar procedimientos.	16. Tras el análisis de las actividades de la organización, los auditores dan los resultados encontrados y se determina las modificaciones que tendrá el BCP dando como resultado la mejora continua de las actividades realizadas.

Controles de esta norma?	**Políticas de Seguridad de la información**: Esta norma desea controlar que la gerencia desarrolle una documentación completa de la políticas y que periódicamente sean revisadas para proponer cambios o mejoras al mismo.	**Políticas de seguridad, documentación y revisión: E**l objetivo es proporcionar orientación por parte de la dirección, manteniendo en toda la organización normas y leyes que contribuyan a la estabilidad de la misma. La dirección debe demostrar su apoyo y compromiso comunicando en la organización los cambios y nuevas políticas. las políticas deben ser revisadas a intervalos determinados para verificar su eficiencia y suficiencia en los procesos de la organización.	Esta normativa da como objetivo primordial el establecimiento de políticas y actividades de control que ayuden al mejoramiento de las actividades de la organización y que deben ser creadas y administradas por la gerencia como compromiso al buen desempeño de los procesos de la empresa.	Esta normativa sugiere el desarrollo de políticas que abarquen los objetivos generales de empresa, las responsabilidades, el desarrollo de las estrategias y la identificación de los controles preventivos para la planificación de las contingencias.	Esta normativa no expone controles, da la posibilidad al usuario de tener claro lo que se debe hacer y que tener en cuenta pero no expone controles directos para realizar las políticas de seguridad de la información.	La gerencia es la responsable de realiza políticas que abarquen el desarrollo e implementación de BCP y que no intervenga con las metas de la empresa.
Controles de esta norma?	**Organización interna**: lo que se desea controlar es el apoyo continuo de la gerencia en el desarrollo de los planes de seguridad, asignar responsabilidades, reiterar continuamente la confidencialidad a la que están sujetos los integrantes de este plan y hacer en tiempos programados controles de los procesos y actividades especificados en el SGSI.	**Organización de la seguridad:** el objetivo de este control es gestionar la seguridad de la información y crear un marco de referencia para dar comienzo a la seguridad, la dirección como en todos los procesos de la organización debe estar fuertemente ligada y comprometida a apoyar activamente los procesos internos. los procesos deben ser controlados por personal asignado a ellos con roles y responsabilidades aparte	La organización debe realizar controles continuos de sus actividades, debe regir en la al interior de la misma normativas que contribuyan al desarrollo exitoso del SGCN, se debe establecer de forma detallada la participación de las directivas ya que estos son los encargados de hacer cumplir lo impuesto en el plan de la continuidad.	Esta sugiere la participación continua del CIO (Chief Information Officer) y la gerencia de la organización en el desarrollo total del BCP y las políticas que lo rigen.,		En esta normativa surge como punto importante la cooperación de la directiva ya que es responsable de aprovisionar a la organización de los recursos necesarios para el desarrollo del programa, además la gerencia es responsable de asignar responsabilidades y garantizar que comunicar a los empleados la importancia del BCP

Controles de esta norma?	**Organización Externa**: lo que se desea controlar es la identificación de los riesgos que trae dar acceso a la información a agentes externos.	**Partes Externas:** el objetivo es mantener la seguridad de las partes de la organización que son procesadas o en la que intervienen partes ajenas a esta, se desea controlar accesos, procesos y comunicación que debe manejar los agentes externos, también es fundamental mantener la seguridad de todos los recursos de la organización que brindan sus servicios a clientes que usan frecuentemente los recursos de la entidad y dejar de manera escrita y de manera entendible las normativas y los procedimientos para mantener y establecer la seguridad en los tratados con terceros.	Esta normativa no especifica el control que se debe tener sobre los agentes externos o terceros que tienen control y acceso a información vital de la organización.	Esta normativa no especifica el control que se debe tener sobre los agentes externos o terceros que tienen control y acceso a información vital de la organización.	Esta normativa no especifica el control que se debe tener sobre los agentes externos o terceros que tienen control y acceso a información vital de la organización.	Esta normativa no especifica el control que se debe tener sobre los agentes externos o terceros que tienen control y acceso a información vital de la organización.
Controles de esta norma?	**Gestión de Activos**: el objetivo de este control documentar los activos de gran importancia y controlar el buen uso de los mismos.	**Gestión de Activos**: implementar y mantener una adecuada protección a los activos de la organización asignando responsables al cuidado de los mismos, además se debe llevar una documentación adecuada de los activos informáticos, de servicio y físicos.	Esta normativa no especifica cómo realizar la adecuada gestión de activos para el desarrollo efectivo de la seguridad del SGCN.	Esta normativa no especifica cómo realizar la adecuada gestión de activos para el desarrollo efectivo de la seguridad del SGCN.	**Gestión de Recursos:** esta normativa sugiere la creación de un sistema de identificación de activos y recursos como personas, equipos, instalaciones y tecnología que ayude al acceso oportuno de los recursos que contribuyan a la preparación de la continuidad frente a cualquier incidente. La gestión de activos debe incluir las	Aunque no se habla directamente de cómo se deben gestionar los recursos queda muy claro que la importancia del registro de estos es fundamental para la continuidad del negocio.

					siguientes tareas: Inventario de los recursos, clasificación de recursos, recursos de más importancia que ayuden a la continuidad, responsables de los recursos.	
Controles de esta norma?	**Seguridad física y ambiental**: se desea controlar las áreas seguras, estabilidad en las conexiones, control de ingreso de personal y asegurarse que los equipos de cómputo no sean extraídos de la entidad. Establecer áreas donde se los activos no se vean afectados por amenazas ambientales.	**Seguridad física y ambiental:** se desea creas áreas seguras donde se establezcan perímetros de seguridad, controles de acceso físico, seguridad en las oficinas de la organización, donde la protección de los activos frente a amenazas ambientales este establecida y controlar las áreas donde las personas no autorizadas tienen acceso.	Esta normativa no especifica cómo gestionar la seguridad de la infraestructura en la implementación del SGCN.	En esta normativa no se especifica que metodología es la apropiada para gestionar las infraestructura física de la empresa pero toma muy en cuenta la importancia de tener otra sede que cumpla con estándares de seguridad que ayuden a tomar de nueva la continuidad de las actividades de la empresa	Esta normativa no toma muy en cuenta la seguridad de la infraestructura física de la organización.	Esta normativa no toma muy en cuenta la seguridad de la infraestructura física de la organización.

Controles de esta norma?	**Gestión de las comunicaciones y operaciones:** trata de controlar el buen uso de los medios informáticos, controla las forma de dar servicios a terceros, controla que las operaciones dentro de la empresa estén correctamente configuradas para evitar fallas, controlar la seguridad del software, controla el desarrollo de un back-up periódico de los activos de información, control del intercambio de medios y de información con agentes externos, controlar la seguridad de los registros desarrollados en las auditorias.	**Gestión de comunicación y operaciones:** el objetivo es documentar detalladamente todos los procedimientos que se realizan en las operaciones cotidianas de la organización, se debe documentar de manera explícita los cambios realizados en las actividades, los impactos potenciales que tendrían los cambios y controlar que las áreas de trabajo estén separadas para evitar fraudes y cambios inesperados. Además de lo antedicho se desea establecer la capacidad del sistema implementado, los controles sobre código malicioso, los backups de los sistemas actuales, proteger la interconexión entre sistemas en la trasmisión de datos.	Esta normativa pretende que los resultados de la respuesta de la organización ante las emergencias sean comunicadas de manera clara por las personas adecuadas a los integrantes de la organización.	Esta normativa específica la importancia de la buena comunicación de la información entre los integrantes de la empresa, además de la documentación y distribución de la misma entre las personas responsables del BCP	Comunicaciones y Advertencias: la entidad deberá determinar las necesidad de comunicación y alerta, la comunicación debe ser redundante y confiable, la entidad debe tener una central de comunicaciones que ayude con la transmisión de la comunicación en toda las zonas de la entidad.	La organización debe mantener de manera estable la comunicación de todos los interesados en el bienestar de la empresa tanto internos como agentes externos que pueden ser de gran ayuda en el momento de una interrupción. La organización puede determinar si la comunicación llegue al extremo de dar a conocer sus debilidades y riesgos aunque podría ser una ayuda puede ser un riesgo adicional aprovechado por entidades externas y afectaría aun más la seguridad de la organización y sus actividades.

Controles de esta norma?	**Control de acceso:** establecer políticas de seguridad que especifiquen los métodos de acceso a la información y las personas autorizadas para el acceso a la información, revisión periódica de los permisos de acceso.	**Control de Acceso**: el objetivo en establecer políticas que sean viables para el acceso y que fomenten la seguridad del negocio, se debe registrar de manera adecuada los permisos acceso y los usuarios a los cuales afecta, es de gran importancia la gestión de los privilegios asignados y las contraseñas de acceso que son usadas por los usuarios, la directiva deben reevaluar los privilegios asignados y determinar si aun son necesarios, además de la gestión se debe controlar el acceso a la red y su administración, se desea controlar la autenticación correcta de los usuarios del exterior de la empresa, y el comportamiento de los dispositivos de acceso a la misma.	Esta normativa no especifica los métodos adecuados para controlar los accesos al personal de la organización y agentes externos que intervengan en los procesos vitales de la empresa.	Esta normativa no especifica los métodos adecuados para controlar los accesos al personal de la organización y agentes externos que intervengan en los procesos vitales de la empresa.	Esta normativa no especifica los métodos adecuados para controlar los accesos al personal de la organización y agentes externos que intervengan en los procesos vitales de la empresa.	Esta normativa no especifica los métodos adecuados para controlar los accesos al personal de la organización y agentes externos que intervengan en los procesos vitales de la empresa.

Controles de esta norma?	**Adquisición, desarrollo y mantenimiento:** Lo que se desea es saber que la seguridad implementada sea parte de todos los sistemas vitales de la organización, además evitar los errores, pérdidas o modificaciones sin permiso de archivos o código fuente (Uso de Criptografía) de las aplicaciones vitales de la organización. Como punto vital para este control esta registrar los cambios realizados en el software y sistemas operativos, desarrollar pruebas a los cambios realizados para verificar si no impactan en gran medida a los aplicativos fundamentales de la organización.	**Adquisición, desarrollo y mantenimiento de los sistemas de información:** El objetivo es asegurar que la seguridad sea parte fundamental de los sistemas de información, se debe analizar los requerimientos de seguridad, detallar las necesidades y establecer la seguridad necesaria desde el comienzo del plan, tomando como punto de partida establecer el correcto funcionamiento de las aplicaciones, validando los datos de entrada como claves, respuesta adecuada a los errores y la no divulgación de información. Además se desea que los procesos internos de las aplicaciones reduzcan al mínimo la corrupción de información. al realizar pruebas se desea el no uso de bases de datos que contengan información real, realizar controles del código fuente de las aplicaciones que permitan la ubicación de funciones no permitidas.	Esta normativa deja claro que el desarrollo, mantenimiento y mejora de los procesos deben cumplir con los requerimientos plasmados en el inicio del estudio del desarrollo del SGCN, todos los procesos de desarrollo y mantenimiento de los sistemas deben ser documentados de manera clara ya que esta información servirá para futuros procesos de corrección y prevención de fallas.	Esta normativa específica que la mejora continua es la clave para el desarrollo adecuado de las actividades del BCP y que deben ser analizadas contantemente para lograr un equilibrio entre la vida de la empresa y las actividades que se deben hacer frente una amenaza.		

Controles de esta norma?	**Gestión de incidentes en la seguridad de la información:** reportar las debilidades de la seguridad implementada de manera clara que ayude a su corrección inmediata, además asignar responsabilidades a los empleados para asegurar la respuesta inmediata en caso de riesgo.	**Gestión de incidentes de la seguridad de la información:** Se pretende establecer una metodología que ayude al reporte oportuno de incidentes y debilidades de la seguridad, se desea que los empleados o terceros tengan el conocimiento de las responsabilidades de reportar alguna brecha de seguridad, la información de estos reportes deben ser documentados de manera histórica para futuros estudios y establecimiento de debilidades recurrentes que afecten el servicio de la empresa.		Esta normativa no especifica cómo se debe avisar oportunamente los incidentes o riesgos conocidos, solo explica la importancia del desarrollo del BIA y la identificación oportuna de los riesgos que afectan a la empresa, además de los recursos críticos .	La entidad debe desarrolla un sistema de gestión de incidencias que ayude a dirigir, controlar las operaciones de respuesta. Este sistema deberá describir las funciones específicas de la organización, además se deben desarrollar políticas que contribuyan a la mitigación y gestión de incidentes además de mantener una comunicación constante con los interesados en el desarrollo continuo de las actividades de la empresa.	
Controles de esta norma?	**Gestión de la continuidad comercial:** el objetivo de este control es el de evitar que las actividades de la organización se frenen por motivos externos, esto se logra realizando un estudio de los requerimientos de seguridad de todas las actividades vitales de la organización, se debe identificar las principales causas con las cuales se afectaría el funcionamiento de las actividades de la empresa, para lograr que estos hallazgos tengan	Esta norma no establece ninguna metodología o pasos claros para establecer un BCP	Esta normativa determina las actividades necesarias para controlar y gestionar los incidentes y así garantizar la recuperación y tratamiento oportuno de los mismos.	Esta normativa da los pasos necesarios para establecer el proceso de continuidad	Esta normativa muestra los campos a cubrir en el desarrollo de un Programa que colabore con la continuidad del negocio	
			a. Tener un propósito y un alcance	Conocer las políticas y requerimientos necesarios para la implementación del BCP y obtener la aprobación de su implementación	Dejar claro el propósito las metas, las políticas que se utilizaran para el desarrollo del programa.	

	solución se debe desarrollar un Plan donde se mantenga y se asegure que la información estará disponible para asegurar la continuidad del negocio.		b. Tener propietarios que sean responsables de la revisión del SGCN.	Identificar los recursos y actividades críticos y establecer su importancia	Identificar los recursos necesarios y sus propietarios, los recursos deben ser tanto humanos, como tecnológicos, estos recursos deben ayudar a la continuidad del negocio.	Establecer responsabilidades de las personas a interactuar con el sistema y proveer de recursos que sean necesarios para la puesta en marcha del sistema de gestión.
			c. Establecer líneas de comunicación.	Establecer métodos de tratamiento de riesgos y permitiendo a los empleados conocer estos métodos de una manera clara, fomentando la buena comunicación.	La empresa determinara el método de comunicación y redundancia de la misma, además de establecer una comunicación constante entre los integrantes del programa	La organización es responsable por documentar y comunicar los cambios en los planes, sistemas de gestión , los resultados de la evaluaciones y funciones de la organización, debe fomentar la comunicación interna y externa, debe comunicar sobre los riesgos aceptado, el tramite de los riesgos y las inminentes amenazas que afectarían la organización.
			d. Información de tareas principales para la empresa.			Se documentara toda la información de la empresa y sus principales funciones.
			e. Definir grupos o individuos con sus roles y responsabilidades.	Se establece personas adecuado para la implementación y se define que roles tendrá en el BCP	Definir los roles y responsabilidades de las personas a activar y desarrollar el programa.	Se definirán roles y responsabilidades a las personas que integren el grupo que ayudara a la gestión.
			f. Determinar el método y las circunstancias en las cuales se activa el plan.	Determinar estrategias donde se dé solución a los riesgos encontrados.	Determinar cómo se trataran los riesgos, si existe la posibilidad de ayuda externa para lograr la normalidad de las actividades cotidianas	Esta normativa no establece ni la forma ni el momento para activar el plan de gestión.
			g. Proceso de retorno a la normalidad.			

			h. Los detalles para gestionar los incidentes de forma inmediata.	Establecer estrategias que deben ser desarrolladas por la empresa	Esta normativa no establece como deben ser tratados ni tampoco con que tiempo de respuesta pero explica la importancia del BIA y el análisis de riesgos para lograr el control y la continuidad	La organización establecerá la metodología necesario para el análisis y tratamiento por medio de estrategias la gestión de riesgos
			i. Los detalles sobre cómo se le comunican a los empleados lo sucedido con los incidentes.	Se establece una comunicación constante con los personas integrantes de la organización que intervengan en el desarrollo e implementación del BCP	Capacitaciones constantes de los empleados, dando a conocer lo aprendido después de una catástrofe, tomando como recuso más importante la bitácora de los sucedido.	Se deberá comunicar a los empleados de los sucesos encontrados y los eventos por desarrollar en el desarrollo del programa.
			j. Describir el método para registrar la información	Documentar la información de manera clara donde cualquier integrante de la empresa lo pueda usar.	El registro constante de la información ayuda a aprender y conocer de alguna fuente directa lo sucedido tras una catástrofe y conocer que salió bien y que no fue efectivo para el tratamiento de riesgos-.	Esta normativa explica la importancia de la documentación de los eventos, procesos y actividades del programa pero no especifica la metodología a implementar.