2018

Versión 1.0

Implementación del Plan de Continuidad del Negocio según: ISO 27031:2011 e ISO 22301:2012

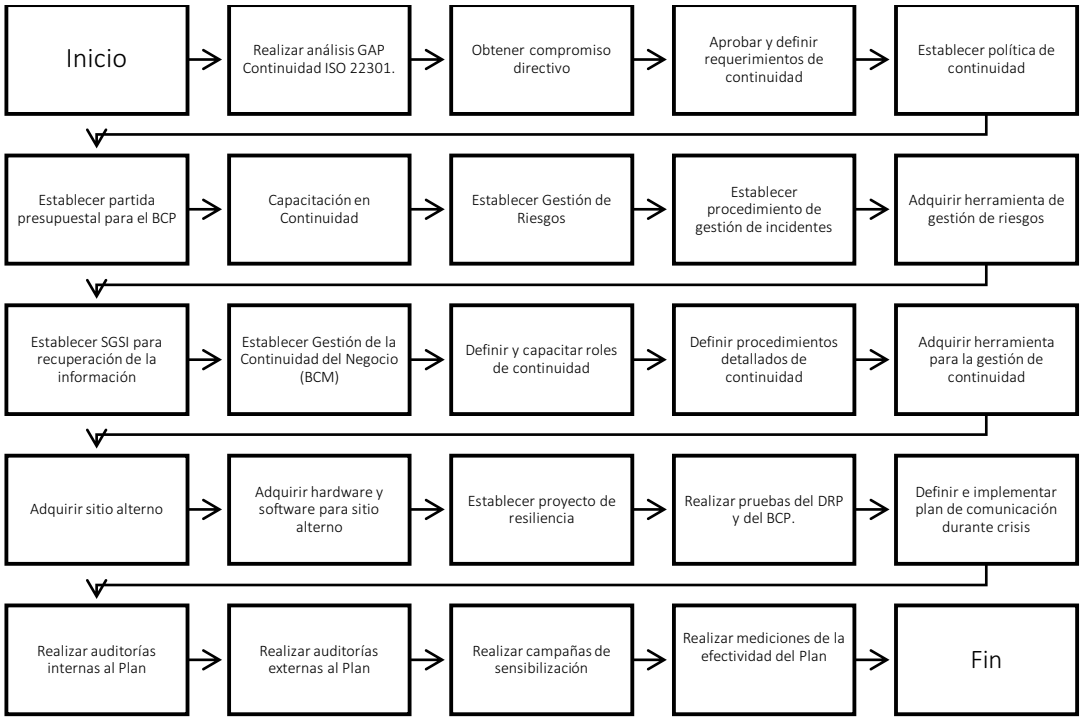
Tabla de contenido

1. IMPLEMENTACION DE UN PLAN DE CONTINUIDAD ISO 22301

1.1. Plan de continuidad

A continuación, la metodología recomendada para todo el proceso de implementación de un plan de continuidad del negocio o un plan de recuperación ante desastres. Cada paso es descrito más adelante en todo su detalle:

Figura No. 1. Implementación del Plan de Continuidad.



1.2. Realizar análisis de brecha de Continuidad:

La realización del análisis brecha, permite conocer el estado actual con respecto a las mejores prácticas en continuidad del negocio. Se recomienda que este proceso se realice una vez al año y que los niveles de madurez se establezcan entre 0 y 100 por ciento.

Los dominios que deben ser medidos son:

1. Análisis de impacto al negocio (BIA) incluyendo:	2. Evaluación de riesgos	3. Definición de estrategias de continuidad
4. Planes de continuidad	5. Plan de comunicación de crisis	6. Entrenamiento y sensibilización
7. Existencia de política general de continuidad		

1.3. Aprobación por la dirección

Se confirma la aprobación de la política por parte de la alta gerencia para la realización del proyecto y, por otro lado, se revisa la existencia de los recursos financieros, humanos y logísticos requeridos tanto para la etapa de diseño e implementación del BCP y DRP.

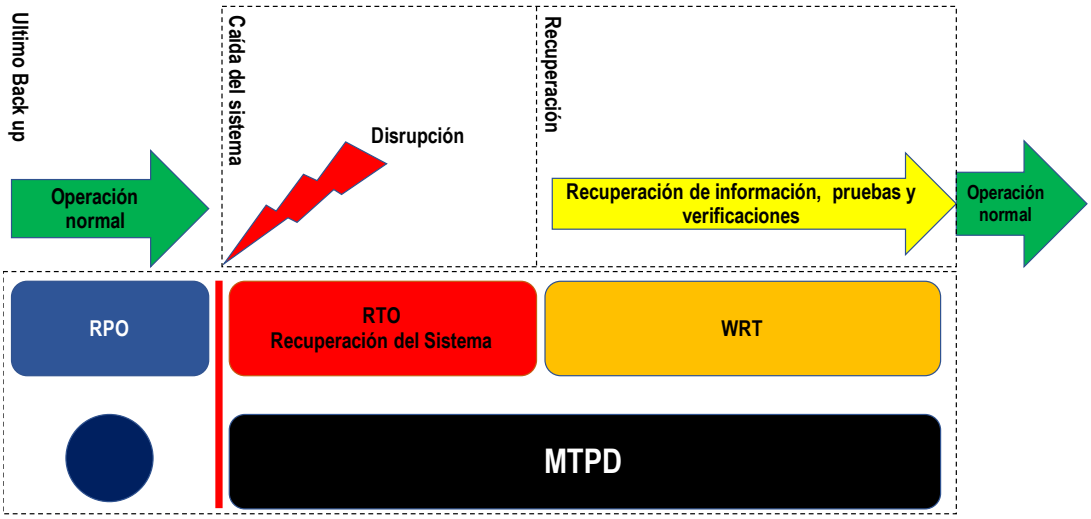
1.4. Aprobar y definir requerimientos de continuidad

Los requerimientos de continuidad son los resultados del análisis BIA una vez que estos son aprobados por la dirección. Entre los resultados que se obtienen de este análisis están:

1. MTPD	2. RTO
3. RPO	4. WRT

En la siguiente figura, se presentan los tiempos que se estiman y calculan como parte del BIA. El **MTPD** (Maximum Tolerable Period of Disruption, por sus siglas del inglés), o el Máximo Período Tolerable de Disrupción, el cual, en base a las entrevistas que se realicen, ayuda a estimar los tiempos máximos en que un producto, proceso, aplicación o servicio puede estar fuera de su operación normal sin afectar la supervivencia de la Entidad o servicio crítico. El **RTO** (Recovery Time Objective, por sus siglas del inglés), es el Tiempo Objetivo de Recuperación, el cual debe ser menor que el MTPD, y se aplica tanto para productos, procesos y recursos. El **RPO**, (Recovery Point Objective, de sus siglas del inglés) Punto Objetivo de Recuperación, el cual determina la máxima información que se puede perder, sin afectar la continuidad del negocio desde que ocurre un incidente. Finalmente, el **WRT** (Work Recovery Time), es el tiempo invertido en buscar datos perdidos y la realización de reparaciones. Se calcula como el tiempo entre la recuperación del sistema y la normalización de los procesos.

Figura No. 2. Tiempos de recuperación.



1.5. Establecer política de continuidad del negocio.

Con el fin de garantizar la efectividad y el entendimiento por parte del personal de los requerimientos de continuidad del negocio, el plan debe estar basado y apoyado en una política claramente definida y posteriormente aprobada formalmente. Entre los elementos principales a los que debe estar orientado esta política son:

1. Roles y responsabilidades	2. Objetivos
3. Requerimientos en general	4. Alcances
5. Recursos requeridos	6. Requerimientos de entrenamiento

1.6. Establecer partida presupuestal

Una vez se cuenta con el compromiso directivo y con la aprobación de la política de continuidad, se debe, como siguiente paso, establecer la partida presupuestal para los diferentes planes y actividades que conforman la gestión de la continuidad del negocio (BCM). Para establecer este presupuesto se deben considerar los siguientes aspectos que son los que más afectan este rubro:

1. Adquisición de sitio alterno	2. Software y hardware para sitio alterno
3. Herramienta para la continuidad	4. Herramienta para la gestión de riesgos
5. Actividades de consultoría contratada	6. Establecer proyecto de resiliencia

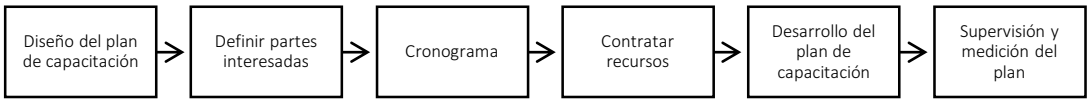
1.7. Capacitación y entrenamiento

La capacitación incluye, entre otros aspectos, el adiestramiento al personal en sus roles y responsabilidades relacionadas con el plan, así como el entrenamiento en habilidades

específicas que necesitarán para llevar a cabo sus roles efectivamente. El entrenamiento, como tal, es un proceso que involucra el aprendizaje de conceptos y términos utilizados en procesos de continuidad del negocio.

En la fase de desarrollo del plan de entrenamiento se busca capacitar a los coordinadores y líderes de equipo del Plan de Continuidad del Negocio en lo referente a la gestión y ejecución del BCP. También se darán a conocer las responsabilidades asociadas a cada uno de los roles definidos en el Plan.

Figura No. 3. Actividades del entrenamiento



Para realizar la capacitación se pueden utilizar múltiples formatos, entre ellos:

1. Presentación a grupos.	2. Conferencias telefónicas.
3. Documentos publicados en la Intranet.	4. Clases magistrales.
5. Conferencias.	6.

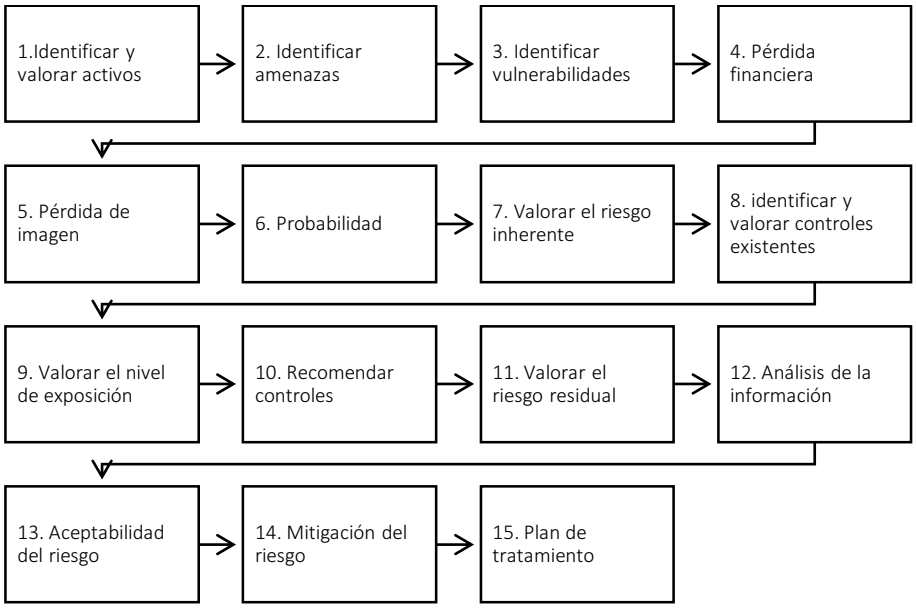
1.8. Establecer la gestión de riesgos

El propósito principal de esta fase es conocer cuáles amenazas o riesgos específicos enfrenta una organización en sus procesos críticos del negocio, identificados como resultado del Análisis de Impacto al Negocio (BIA), con el fin de determinar la forma en que algunos riesgos serán controlados y mitigados a un nivel aceptable según criterios previamente definidos.

Es conveniente mencionar que durante esta fase los riesgos (operativos) se analizarán desde la perspectiva de la continuidad del negocio considerando personas, impresoras, servidores, edificios, tecnología, entre otros, sin dejar de lado su relación directa con los procesos determinados como críticos. El tipo de vulnerabilidades y amenazas al que se ven expuestos estos activos varía dependiendo de la naturaleza de los mismos. Las amenazas y vulnerabilidades que se incluyen para el caso específico del proyecto, serán las relacionadas con la no disponibilidad (operación) de los activos asociados a los procesos críticos del negocio.

En la Figura No. 9 se observan las actividades sugeridas para el análisis de riesgo.

Figura No. 4. Actividades del análisis riesgos.



1.9. Establecer procedimiento de gestión de incidentes

La gestión de incidentes es un componente fundamental tanto de una estrategia de continuidad de negocio como de la seguridad de la información. Las actividades principales que debe considerar el procedimiento son:

1. Realizar monitorización de los sistemas internos o externos y de los eventos que ocurren a nivel nacional. Herramientas de software pueden contribuir a estar atentos ante eventos, con efectos operativos, tanto internos como externos.
2. Evaluar los incidentes de continuidad para toma de decisiones sobre activaciones de planes de continuidad.
3. Definir niveles de atención.
4. Aprender de los incidentes de seguridad y de la calidad de la respuesta.

1.10. Herramienta

La gestión de riesgo, se según se expuso anteriormente, comprende una serie de actividades que conllevan a la implementación de controles de seguridad tanto preventivos como reactivos. Dada la complejidad de este proceso se recomienda contar con una herramienta que posea las siguientes características:

1. Compatibilidad con normas como ISO 31000 e ISO 27005.

2. Flexibilidad para adaptarse a diferentes contextos.
3. Generación de reportes de alto nivel.
4. Análisis de mapas de riesgo.

1.11. SGSI para recuperación de información

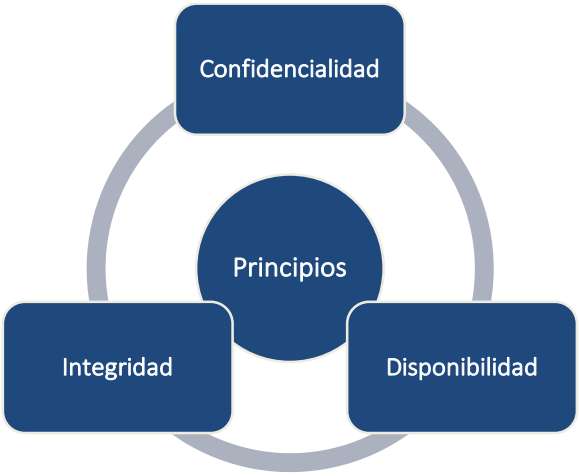
Contar con un Sistema de Gestión de la Seguridad de la Información es útil para la gestión de la continuidad del negocio, ya que la información es uno de los recursos que se deben tener en cuenta de ser recuperados durante un incidente (El dominio A.17 trata los aspectos de seguridad de la información para la continuidad). Por otra parte, es claro la importancia de la información para el cumplimiento de la misión. Este sistema debe contar con 4 etapas principales:

1. Planear
2. Hacer
3. Verificar
4. Actuar

Figura No. 5. Ciclo PHVA

Como se puede observar, la disponibilidad de la información es uno de los objetivos del SGSI.

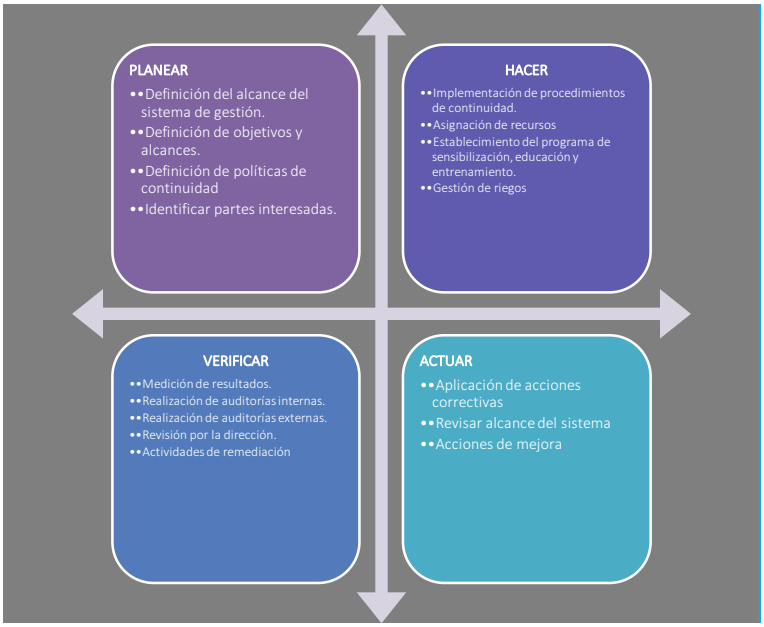
Figura No. 6. Objetivos de la Seguridad



1.12. Establecer Gestión de la Continuidad del Negocio (BCM)

La Gestión de la continuidad del negocio contempla también el ciclo de Planear, Hacer, Verificar y Actuar. El BCM es el componente que une todas las actividades de continuidad que se emprendan en el plan.

Figura No. 7. Ciclo PHVA

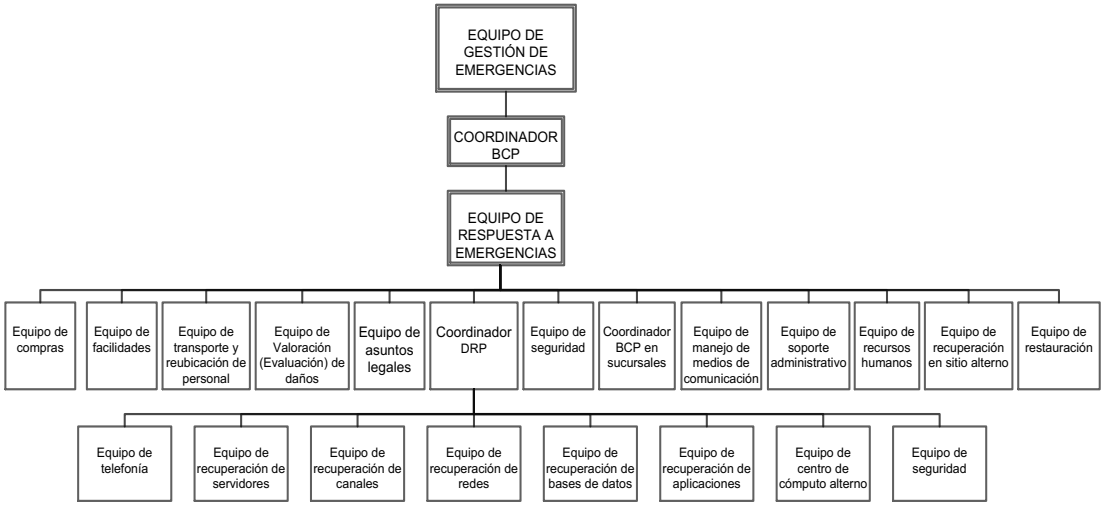


1.13. Definir y capacitar roles de continuidad

En esta actividad deben establecerse las estructuras organizacionales, los perfiles de los cargos y los procedimientos asociados que darán sostenibilidad a la continuidad del negocio. Entre los roles que se considerarán durante la ejecución del proyecto están:

1. Alta Dirección	2. Equipos de Contención Inicial y Logística	3. Equipo de gestión de la emergencia
4. Equipo de recuperación de TI	5. Equipo de relaciones públicas y comunicaciones	6. Equipos de recuperación de procesos
7. Equipos de Apoyo		

Figura No. 8. Equipos de Continuidad



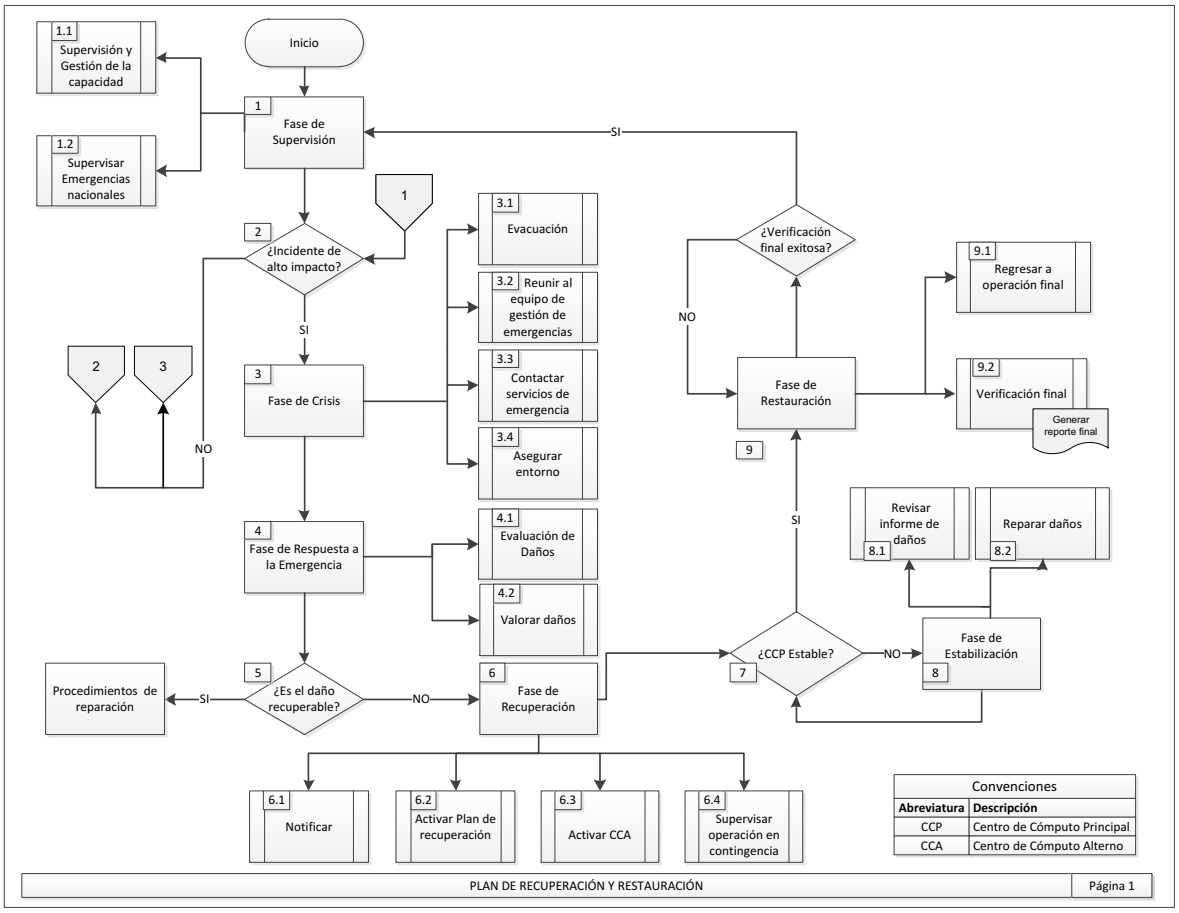
El diagrama aquí presentado es a manera de ejemplo, ya dependiendo de los requerimientos de continuidad este se ajustará para cumplir con la implementación del BCM.

1.14. Definir procedimientos detallados de continuidad

Una vez declarada la activación del plan de continuidad, se debe seguir una secuencia predeterminada con el fin de realizar una recuperación ordenada y eficaz. Las fases en que se distribuyen estas actividades de recuperación son:

1. Supervisión	2. Crisis
3. Respuesta a la emergencia	4. Restauración
5. Recuperación	6. Estabilización

Figura No. 9. Procedimientos de Continuidad



1.15. Herramienta para la gestión de continuidad

El establecimiento de la gestión de continuidad requiere mantener disponibles y actualizados una gran cantidad de documentos. También se requiere contar con una herramienta automatizada que facilite realizar las siguientes actividades:

1. Análisis de impacto al negocio (BIA)
2. Gestión de riesgos
3. Análisis de las estrategias de continuidad

Entre las características deseables que esta herramienta tenga está:

1. Flexibilidad para adaptarse a diferentes contextos
2. Interfaz gráfica
3. Lenguaje español
4. Compatible con la norma ISO 22310 e ISO 31000.

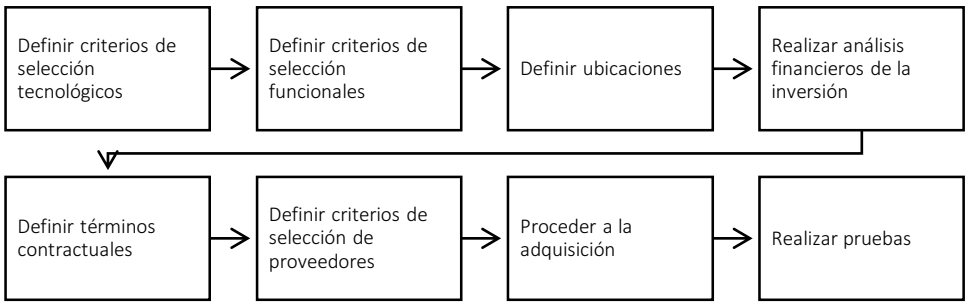
1.16. Adquisición sitio alterno

Esta fase tiene como objetivo primordial definir las tareas y asignar recursos con el fin de implementar las estrategias de mitigación. Es recomendable en esta fase contar con una metodología efectiva para la gestión de proyectos con el fin de lograr definir de manera precisa los recursos requeridos, los tiempos de adquisición, instalación, prueba y afinamiento de los controles definidos. Por ejemplo, en esta fase se puede decidir la adquisición y puesta en funcionamiento de un generador de potencia eléctrica, para ello se debe realizar una invitación a diferentes proveedores, realizar la selección del proveedor y marca del equipo, instalar, configurar, probar y llevarlo a producción.

Uno de los controles a implementar y en que normalmente y tradicionalmente se ha hecho una gran inversión es el tema de sitio alterno. Para esto se recomienda seguir los siguientes pasos:

1. Definir criterios de selección tecnológicos (nube o sitio alterno)
2. Definir criterios de selección funcionales
3. Definir ubicaciones
4. Realizar análisis financieros de la inversión
5. Definir términos contractuales

Figura No. 10. Adquisición de sitio alterno.



1.17. Adquirir hardware y software para sitio alterno

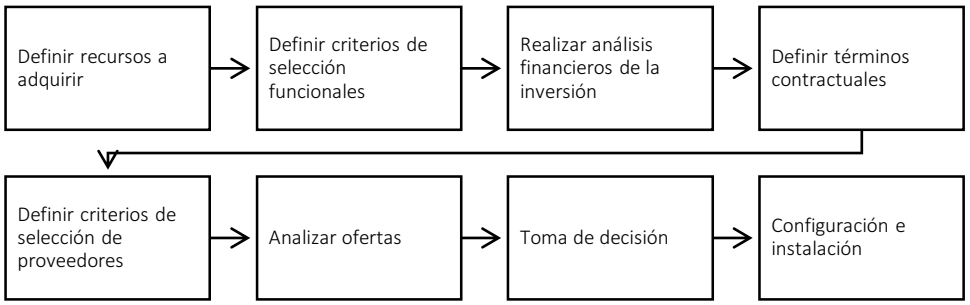
Esta fase tiene como objetivo primordial definir las tareas y asignar recursos con el fin de adquirir el hardware y el software requerido para el sitio alterno. Es recomendable en esta fase contar con una metodología efectiva para la gestión de proyectos con el fin de lograr definir de manera precisa los recursos requeridos, los tiempos de adquisición, instalación, prueba y afinamiento del hardware y el software adquirido. Por ejemplo,

en esta fase se puede decidir la adquisición y puesta en funcionamiento de un servidor de base de datos, firewalls, elementos de red, servidores, entre otros.

Se recomienda seguir la siguiente metodología para la adquisición del hardware y el software para sitio alterno:

1. Definir recursos a adquirir
2. Definir criterios de selección funcionales
3. Realizar análisis financieros de la inversión
4. Analizar ofertas
5. Toma de decisión
6. Configuración e instalación

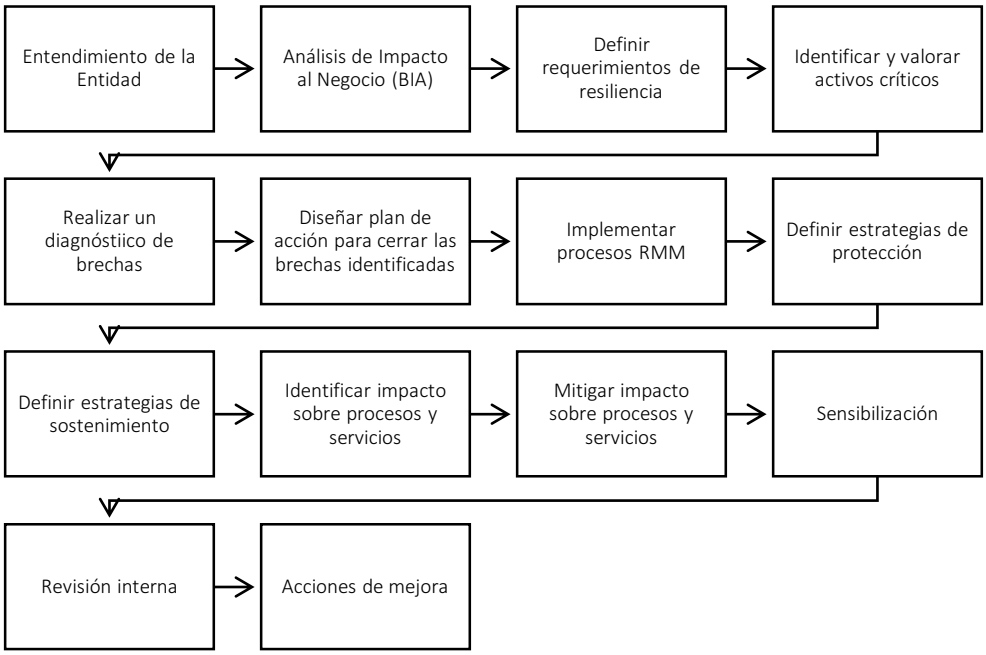
Figura No. 11. Adquisición de Hardware y Software.



1.18. Establecer proyecto de resiliencia

Con el fin de mejorar la resiliencia se sugiere contar con una metodología que apoye la implementación de este proceso. La metodología aquí propuesta está basada en el CERT RMM, la norma ISO 27031:2011, la norma ISO 22301:2012 y la Guía para la preparación de las TIC para la continuidad del negocio de MINTIC. En la siguiente figura se muestra las diferentes fases que la componen:

Figura No. 12. Metodología para la Resiliencia.



Considerando los aspectos más relevantes estudiados anteriormente se procede a elaborar la matriz de recomendaciones de resiliencia. Para ello, se consideraron los tres pilares fundamentales del concepto:

- Alta disponibilidad
- Estrategias de protección
- Estrategias de sostenimiento

Por alta disponibilidad se entiende el uso de tecnologías que permite que en el caso de falla de un componente otro componente entre a suplir sus funciones. Las estrategias de protección se definen como capacidades proactivas que previenen la generación de disrupciones en los procesos misionales, del mismo modo las estrategias de sostenimiento son capacidades que responden ante incidentes catastróficos.

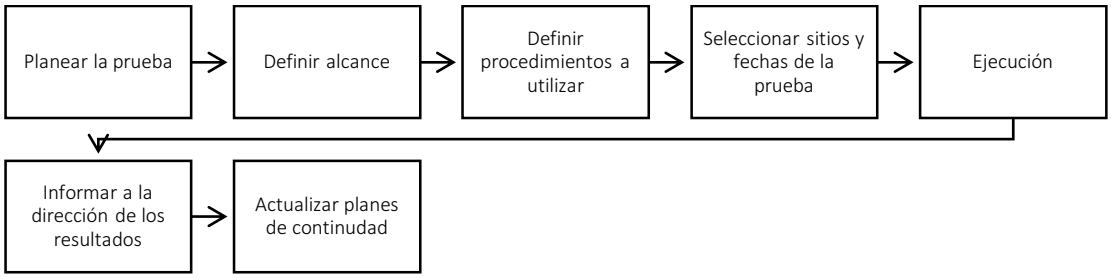
1.19. Realizar pruebas

La efectividad del BCP en situaciones de desastre se puede comprobar mediante un plan de prueba que permita revisar dicha efectividad antes de enfrentarse a una situación real. Es también importante que las pruebas se lleven a cabo por las personas que serían responsables de esas actividades en una crisis según su rol. Estas pruebas deben estar dirigidas por el Coordinador del BCP y deben realizarse mínimo una vez al año o antes si existe un cambio sustancial en las condiciones del Plan, según lo sugerido por las mejores prácticas y recomendaciones internacionales. También es importante anotar que es posible realizar pruebas ya no simuladas, sino, que los activos

que soportan los procesos se pongan fuera de servicio y de esta manera contar con una prueba más real, sin embargo, este tipo de pruebas pueden convertirse en un desastre y por eso es importante hacer siempre antes una planeación muy detallada de este tipo de pruebas y analizar sus riesgos inherentes.

En la Figura, se muestran las actividades que se deben seguir para realizar la fase de pruebas.

Figura No. 13. Pruebas del BCP.

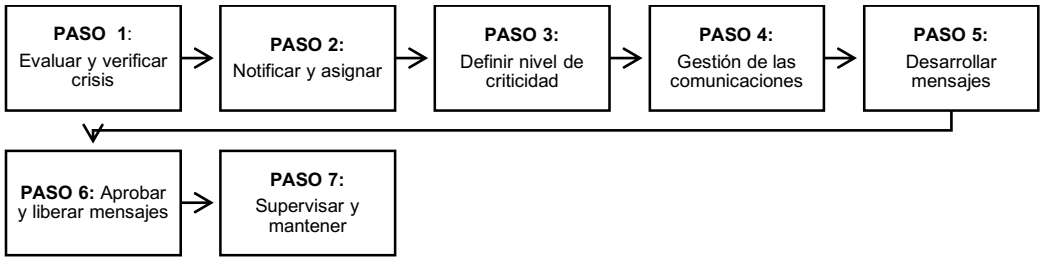


1.20. Definir e implementar plan de comunicación de crisis

Contar con un plan de comunicaciones de crisis antes, durante y después de una interrupción permite dar una respuesta efectiva y ordenada, no solamente cuando se esté expuesto a los medios de comunicación, sino también para mantener informados a los empleados, los miembros de la familia y las partes interesadas de la entidad. Se debe evaluar la crisis, notificar a las partes interesadas, priorizar, y contar con mensajes predefinidos con el fin de ofrecer información veraz, precisa y que no exponga a la entidad a futuras demandas legales. El siguiente es un enfoque de siete pasos para para el plan:

- **PASO 1**:
  Evaluar y verificar crisis
- **PASO 2:**
  Notificar y asignar
- **PASO 3:**
  Definir nivel de criticidad
- **PASO 4:**
  Gestión de las comunicaciones
- **PASO 5:**
  Desarrollar mensajes
- **PASO 6:**
  Aprobar y liberar mensajes
- **PASO 7:**
  Supervisar y mantener

Figura No. 14. Plan de Crisis



1.21. Auditoría internas y externas

La auditoría del Plan (planes) es un proceso en el que se revisa el BCP (DRP) contra requerimientos específicos estandarizados por la industria (BCI, DRII, ISACA). La auditoría también es una revisión imparcial para verificar si él cumple con las necesidades de la organización. Por otro lado, la auditoría debe ser realizada como un proyecto estándar y un plan de auditoría debe ser creado antes de su realización.

En el proceso de auditoría se deben tener en cuenta varios elementos importantes, entre los cuales se encuentran:

1. Revisar el BIA y verificar que esté actualizado.
2. Revisar la metodología del Análisis de Riesgo.
3. Revisar que el análisis de riesgo esté actualizado.
4. Asegurarse de que las estrategias de mitigación de riesgos hayan sido implementadas apropiadamente.
5. Revisar la efectividad de los controles implementados.
6. Revisar el Plan de Pruebas y Entrenamiento.
7. Revisar cómo se hace el mantenimiento del Plan.
8. Revisar los procesos y documentos de sensibilización.
9. Recolectar evidencias sobre las actividades realizadas relacionadas con el BCP.
10. Entrevistar al coordinador del BCP y a otros integrantes del equipo sobre las actividades que desempeñan dentro del Plan.

1.22. Realizar sensibilización

Se deben realizar campañas de sensibilización con el objetivo que todos los funcionarios o contratistas comprendan la importancia de responder efectivamente a una disrupción que afecte el logro de la misión. Entre los temas que debe comprender estas campañas están:

1. Contexto
2. Conceptos de continuidad del negocio
3. Resultados del BIA

4. Sistemas de información con que se cuenta
5. Concepto de disrupción
6. Riesgos operativos típicos
7. Controles preventivos
8. Controles reactivos
9. Beneficios de contar con un BCM

1.23. Realizar mediciones de la efectividad del plan

Con el fin de contar con una mejora continua de los planes de continuidad se requiere que estos sean evaluados con el fin de medir su nivel de desempeño. Para esto se debe tener en cuenta lo siguiente:

1. Seleccionar métricas acordes con la misión y la visión de la entidad
2. Determinar lo que debe ser monitorizado según la misión
3. Determinar el método o técnica de monitorización
4. Determinar los momentos en que se hará la monitorización
5. Evaluar el cumplimiento de la política de continuidad

2. GLOSARIO DE TERMINOS DEL BCP

ACTIVO: En relación con la seguridad de la información se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas) que tenga valor para la organización. (ISO/IEC 27000)
AMENAZAS: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000)
ANÁLISIS DEL IMPACTO DEL NEGOCIO: Proceso del análisis de actividades y el efecto que una interrupción del negocio podría tener sobre ellas. (ISO 22301)
ANÁLISIS DE RIESGO: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000)
APETITO DE RIESGO (RA)[1]: Se refiere a la cantidad de exposición a impactos adversos potenciales que la empresa está dispuesta a aceptar para alcanzar sus objetivos.
CIBERESPACIO[2]: Ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética.
DISRUPCIÓN[3]: Término que procede del inglés "disruptive" y que se utiliza para nombrar a aquello que produce una ruptura brusca. Por lo general el término se utiliza en un sentido simbólico, en referencia a algo que genera un cambio muy importante o determinante.
MTPD: (Maximum Tolerable Period of Disruption), o el Máximo Período Tolerable de Disrupción. Espacio de tiempo durante el cual un proceso puede estar inoperante hasta que la empresa empiece a tener pérdidas y colapse. (ISO 22301)
PLAN DE CONTINUIDAD DE NEGOCIO: Procedimientos documentados que guían a las organizaciones para responder, recuperar, reanudar y restaurar a un nivel predefinido de operación debido a la interrupción. (ISO 22301)
RPO: (Recovery Point Objective) o Punto de Recuperación Objetivo. Es el rango de tolerancia que la entidad puede tener sobre la pérdida de datos y el evento de desastre. (ISO 22301)
RTO: (Recovery Time Objective) o Tiempo de Recuperación Objetivo. Es el tiempo transcurrido entre una interrupción y la recuperación del servicio. Indica el tiempo disponible para recuperar sistemas y recursos interrumpidos. (ISO 22301)
SEGURIDAD DE LA INFORMACIÓN: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000)
SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000)

1 www.auditool.org

2 (CONPES 3701, Tomado de la Academia de la lengua española).

3 Definición de disruptivo-https://definicion.de/disruptivo/

VULNERABILIDAD: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000)
WRT: (Work Recovery Time): Es el tiempo invertido en buscar datos perdidos y la realización de reparaciones. Se calcula como el tiempo entre la recuperación del sistema y la normalización de los procesos. (ISO 22301)

3. BIBLIOGRAFÍA

Business Continuity Institute (2013) *Good Practice Guidelines: A guide to global good practice in business continuity*, Business Continuity Institute, Caversham.

Disaster Recovery Institute International (DRII) (2012) *Professional Practices for Business Continuity Practitioners*, DRII, New York.

ISO 22301 (2012) – Societal security – Business continuity management systems – Requirements

ISO 22301 (2012) – Societal security – Business continuity management systems – Guidance

ISO 22301 (2012) – Societal security – Terminology

Guía para la preparación de las TIC para la continuidad del negocio de Mintic (2010)

ISO 27031 (2011) – Guidelines for information and communication technology readiness for business continuity

Metodología para la Gestión de la Continuidad del Negocio de CINTEL – (2013)

National Institute of Standards and Technology (NIST), SP800-34