



CONFERENCIA



COL·LEGI
D'ACTUARIS
DE CATALUNYA

EL PLAN DE CONTINUIDAD DE NEGOCIO EN COMPAÑÍAS ASEGURADORAS

Santiago Romera, Socio Director de AREA XXI.

Barcelona, 16 de septiembre de 2021

PLAN DE CONTINUIDAD





CURSO

1. INTRODUCCIÓN

Introducción
Situación Actual
Objetivo

2. MEJORES PRÁCTICAS

Marco Conceptual. Referencias Normativas
Definición de un BCP, Business Continuity Plan
Plan de Continuidad al Servicio

3. ADAPTACIÓN AL NEGOCIO ASEGURADOR. FASE I – DIAGNÓSTICO

Revisión y Análisis de BIA
Evaluación Riesgos y Controles
Análisis CAT

4. ADAPTACIÓN AL NEGOCIO ASEGURADOR. FASE II – IMPLEMENTACIÓN

Acciones Mitigación de Riesgo
Entrenamiento, Pruebas, Auditoría
Desarrollo del Plan de Continuidad al Servicio
Mantenimiento del Plan de Continuidad al Servicio



1. Introducción

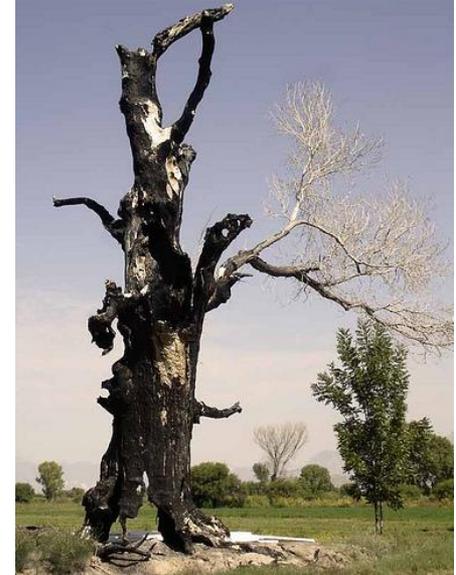
La información es uno de los activos más importantes para las empresas.

Los sistemas de información y la disponibilidad de estos juegan un rol preponderante para la continuidad de un negocio.

El objetivo de implementar lo que se conoce como BCP (Business Continuity Plan), es el de mantener la funcionalidad de una organización, a un nivel mínimo aceptable durante una contingencia.

Esto implica que un BCP debe contemplar todas las medidas preventivas y de recuperación para cuando se produzca una contingencia que afecte al negocio.

1. Introducción





1. Introducción

La Continuidad del Negocio es un concepto que engloba un buen planteamiento sobre:

Recuperación de Desastres:

Capacidad para responder a una interrupción de los servicios mediante la implementación de un plan para restablecer las funciones críticas de la organización en el menor tiempo posible.

Restablecimiento del Negocio:

Capacidad para volver a la situación previa al desastre en el menor tiempo posible.



1. Introducción

- Realizar un **Análisis de Impacto** evaluando el perjuicio económico para la compañía en caso de fallo tecnológico, humano, etc.... que impida el desarrollo normal de los procesos de la compañía.
- **Analizar los Riesgos** a los que la compañía esta expuesta y sobre todo aquellos que afecten a procesos críticos, previamente identificados al objeto de: eliminar, mitigar o asumir estos riesgos.
- Desarrollar **Estrategias de Continuidad** equilibrando gasto/beneficios
- **Realizar Procedimientos** que incluyan detalladamente la planificación de los recursos, la logística y la tecnología necesaria para recuperar los servicios mínimos.
- Comprobar el **Buen Funcionamiento** de las soluciones adoptadas para la recuperación, realizar ejercicios basados en el Plan para poder detectar los puntos débiles y corregirlos.
- **Formación de las personas involucradas en el BCP** y sensibilización de la importancia que éste tiene para el negocio.

Introducción

Normativa Solvencia II: Plan de continuidad del Negocio

SEGUNDO NIVEL → “Real Decreto 1060/2015, de 20 de noviembre, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.” (RDOSSSEAR):

□ Artículo 44. Requisitos generales del sistema de gobierno: *Las entidades aseguradoras y reaseguradoras adoptarán medidas razonables para asegurar la continuidad y la regularidad en la ejecución de sus actividades, incluida la elaboración de planes de contingencia. A tal fin, las entidades emplearán sistemas, recursos y procedimientos adecuados y proporcionados*

TERCER NIVEL → **Directrices Sobre el Sistema de Gobernanza:**

□ Directriz 8. Planes de contingencia: *La empresa debería identificar los riesgos materiales que deben abordarse mediante planes de contingencia, cubriendo las áreas en las que considere que es vulnerable, y revise, actualice y pruebe regularmente esos planes de contingencia.*



1. Introducción. Objetivo

- Conocer la **metodología** (exponemos la de AREA XXI) que se aplica en la elaboración de un BCP.
 - ✓ Análisis de Impacto en el Negocio (BIA).
 - ✓ Detección de Riesgos.
 - ✓ Análisis y Estrategias de Mitigación.
 - ✓ Construcción del Plan.
 - ✓ Pruebas.
 - ✓ Mantenimiento.



CURSO

1. INTRODUCCIÓN

Introducción
Situación Actual
Objetivo

2. MEJORES PRÁCTICAS

Marco Conceptual. Referencias Normativas
Definición de un BCP, Business Continuity Plan
Plan de Continuidad al Servicio

3. ADAPTACIÓN AL NEGOCIO ASEGURADOR. FASE I – DIAGNÓSTICO

Revisión y Análisis de BIA
Evaluación Riesgos y Controles
Análisis CAT

4. ADAPTACIÓN AL NEGOCIO ASEGURADOR. FASE II – IMPLEMENTACIÓN

Acciones Mitigación de Riesgo
Entrenamiento, Pruebas, Auditoría
Desarrollo del Plan de Continuidad al Servicio
Mantenimiento del Plan de Continuidad al Servicio

2. Mejores prácticas. Marco conceptual

Conjunto de procedimientos y estrategias para asegurar la reanudación oportuna y ordenada de los procesos del negocio generando un impacto mínimo o nulo ante una contingencia.

*Administración de la Continuidad del
Negocio - BCM*

2. Mejores prácticas. Definición y objetivos del BCP

Proceso que permite identificar los posibles escenarios de crisis ó contingencias graves que afectan al negocio y que provee de un marco para construir las medidas de protección y la capacidad de respuesta, que garanticen la salvaguarda de los intereses de la compañía, la reputación, la marca y la creación de valor por parte del negocio.

- Proteger personas y activos de la compañía
- Reanudar los procesos críticos dentro de los tiempos establecidos
 - Asegurar la continuidad de las operaciones
- Decisiones preestablecidas que no ofrezcan duda en momentos de caos.

OBJETIVO:

Mantener el servicio al cliente



2. Mejores prácticas. Plan de Continuidad al Servicio

Con el objetivo de asignar y organizar los recursos necesarios para la **Gestión de la Continuidad del Servicio** se elaborarán una serie de documentos entre los que se incluyen :

Plan de prevención de riesgos

Políticas de back-ups.
Almacenamiento de datos distribuidos.
Sistemas de alimentación eléctrica UPS.
Sistemas críticos replicados.

Plan de gestión de emergencias

Evaluación del impacto de la contingencia en infraestructura TI.
Asignar funciones al personal de servicio TI.
Comunicación a los usuarios y clientes de incidencia grave.
Procedimientos de contacto con proveedores involucrados.
Protocolo puesta en marcha del plan de recuperación.

Plan de recuperación

Asignación de personal y recursos.
Instalaciones y hardware alternativos.
Procedimientos de recuperación e integridad de los datos.
Contratos de colaboración con otras organizaciones.
Protocolos de comunicación con los clientes.

CURSO

1. INTRODUCCIÓN

Introducción
Situación Actual
Objetivo

2. MEJORES PRÁCTICAS

Marco Conceptual. Referencias Normativas
Definición de un BCP, Business Continuity Plan
Plan de Continuidad al Servicio

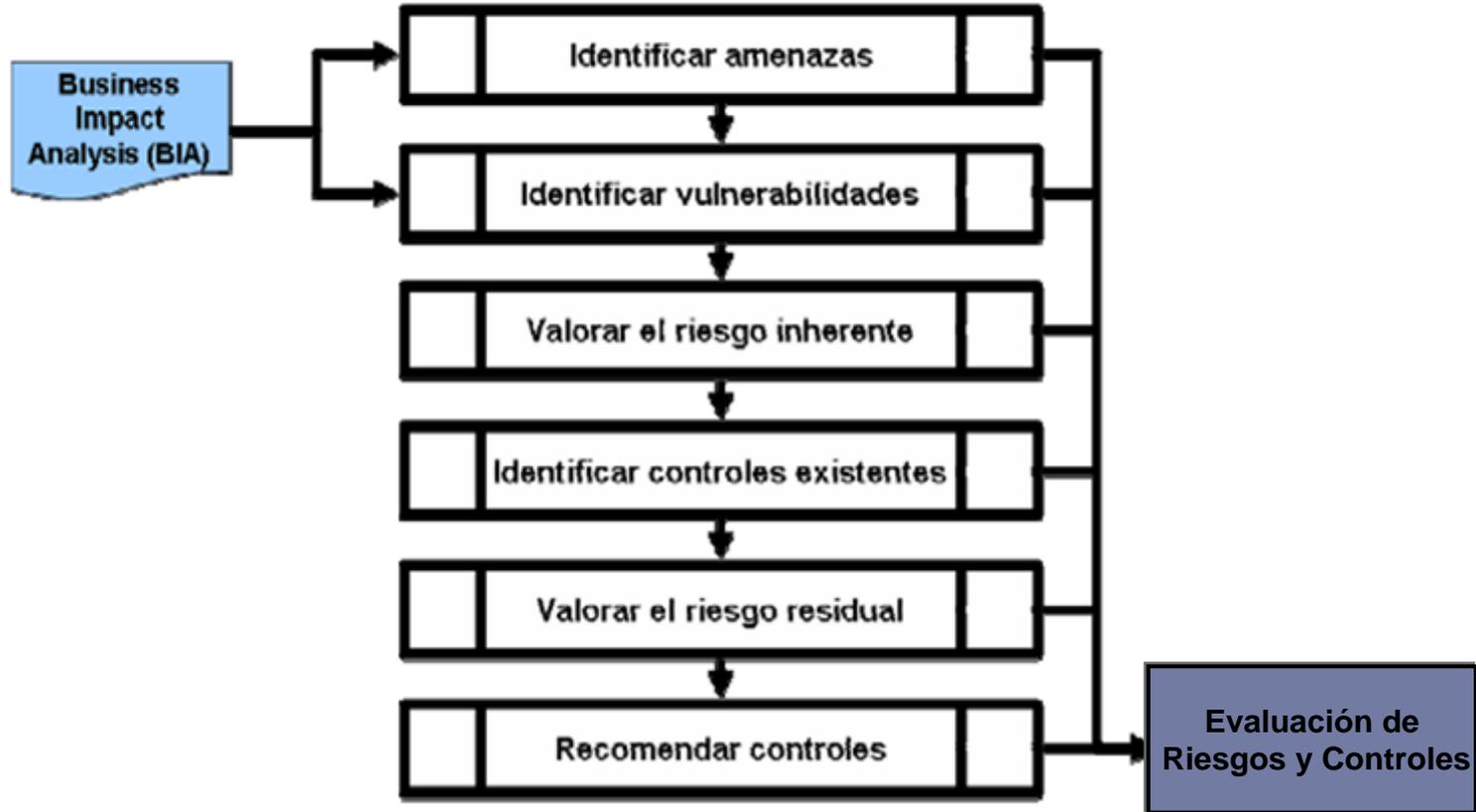
3. ADAPTACIÓN AL NEGOCIO ASEGURADOR. FASE I – DIAGNÓSTICO

Revisión y Análisis de BIA
Evaluación Riesgos y Controles
Análisis CAT

4. ADAPTACIÓN AL NEGOCIO ASEGURADOR. FASE II – IMPLEMENTACIÓN

Acciones Mitigación de Riesgo
Entrenamiento, Pruebas, Auditoría
Desarrollo del Plan de Continuidad al Servicio
Mantenimiento del Plan de Continuidad al Servicio

EL TRABAJO A REALIZAR



¿Cómo lo hacemos?

Elaborar Bia's

Análisis de Riesgos

Estrategias de Mitigación

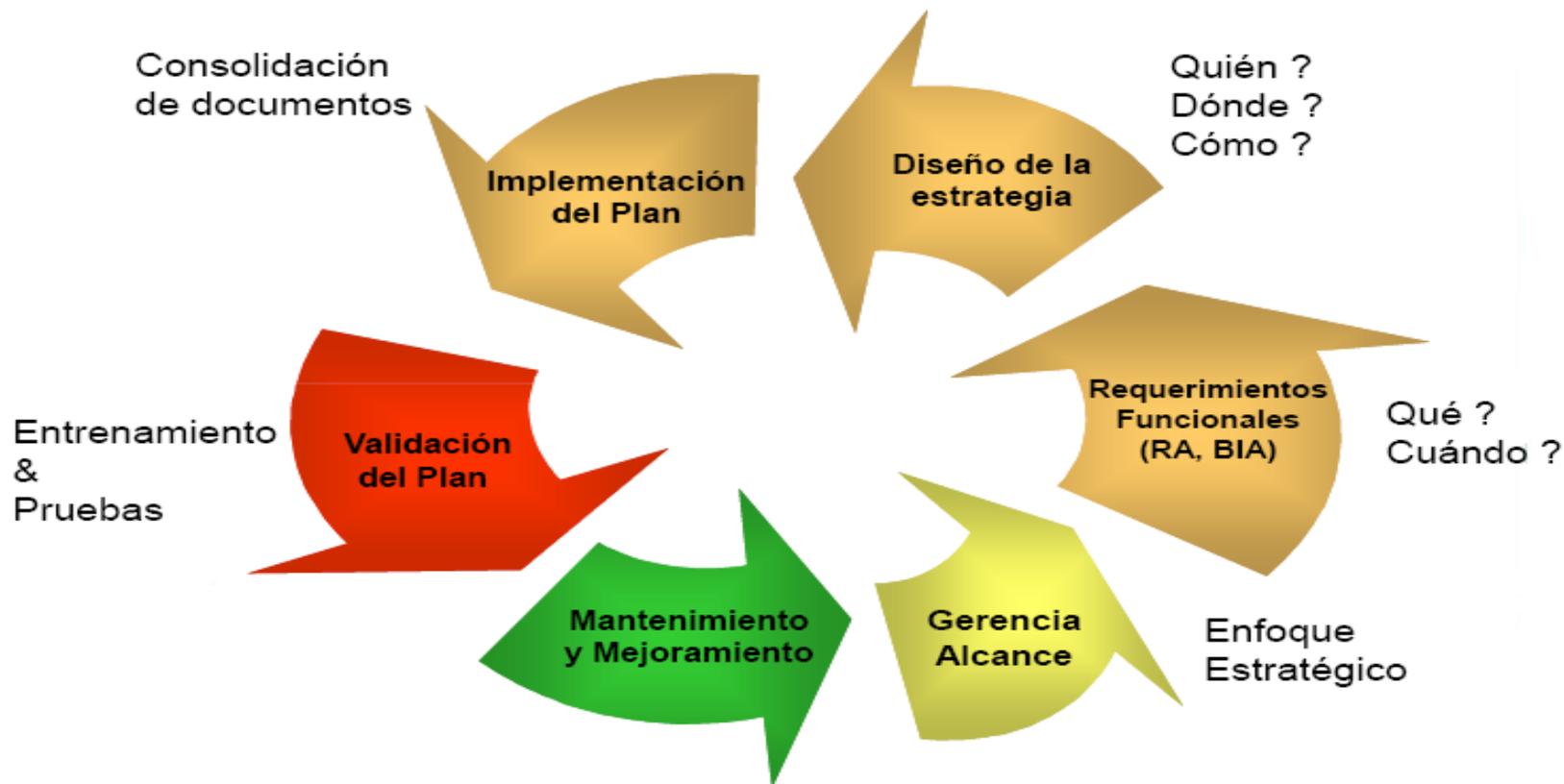
Desarrollar el Plan

**Pruebas y
Mantenimiento**

Concienciar

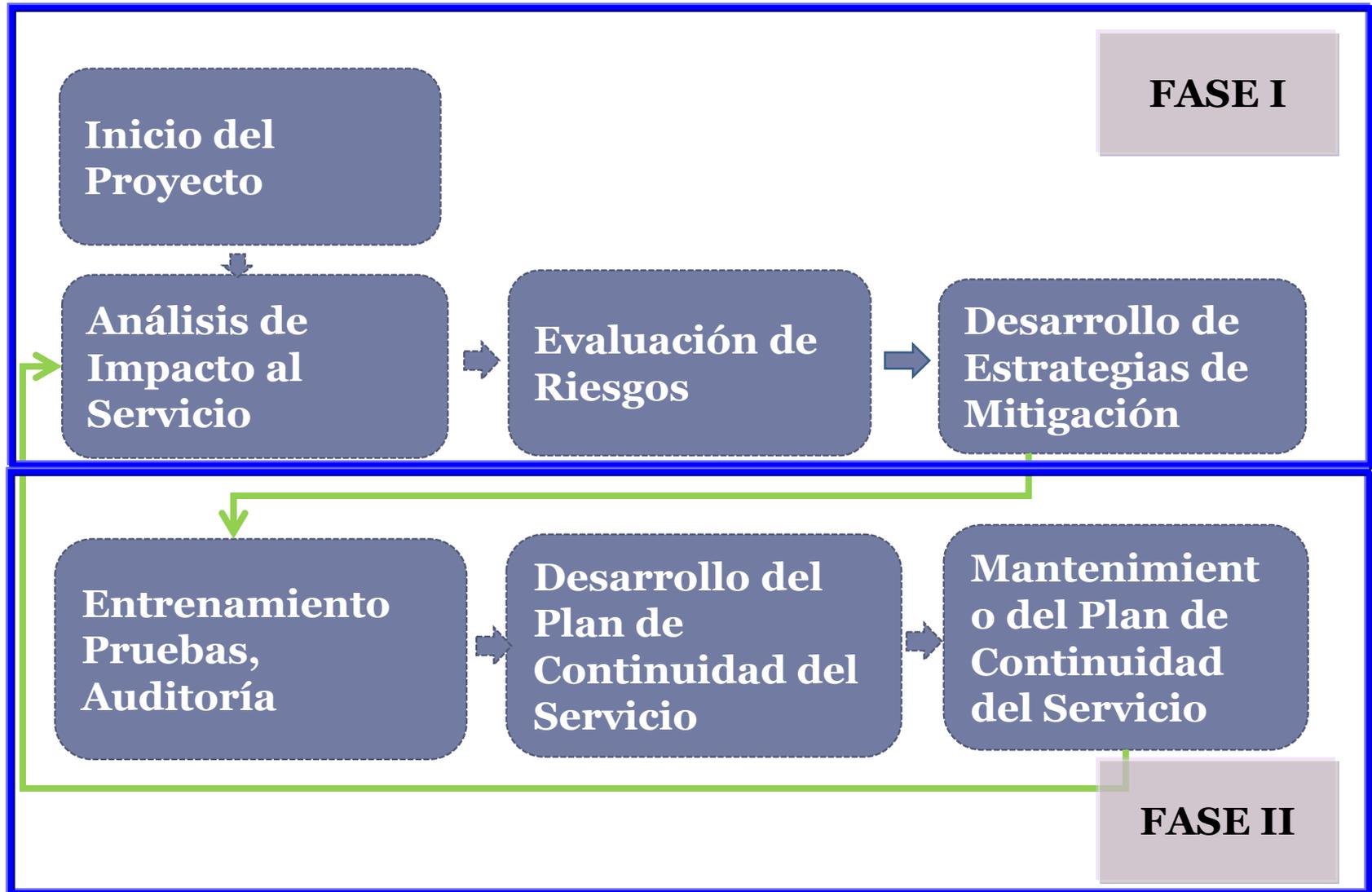


Metodología

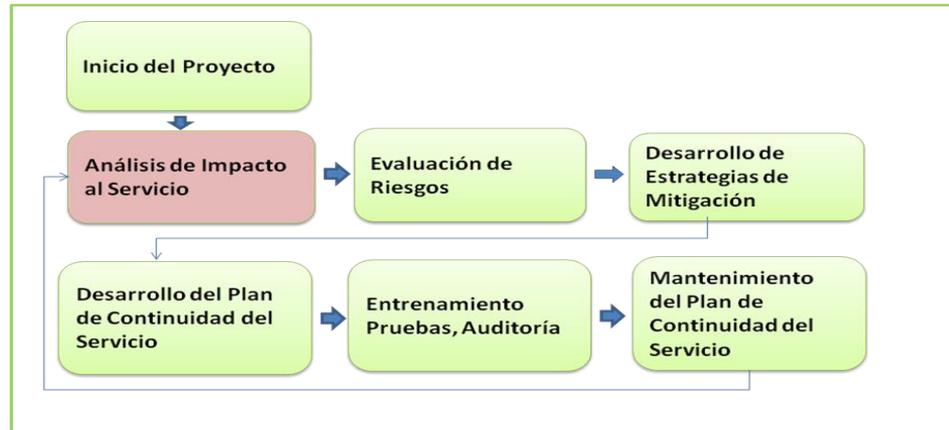


Norma del British Standard Institution (BSI) BS-25999
British Standard for Business Continuity Manage
Guía de buenas prácticas BCI's Good Practice Guidelines

Fases del proyecto



Elaborar Bia's



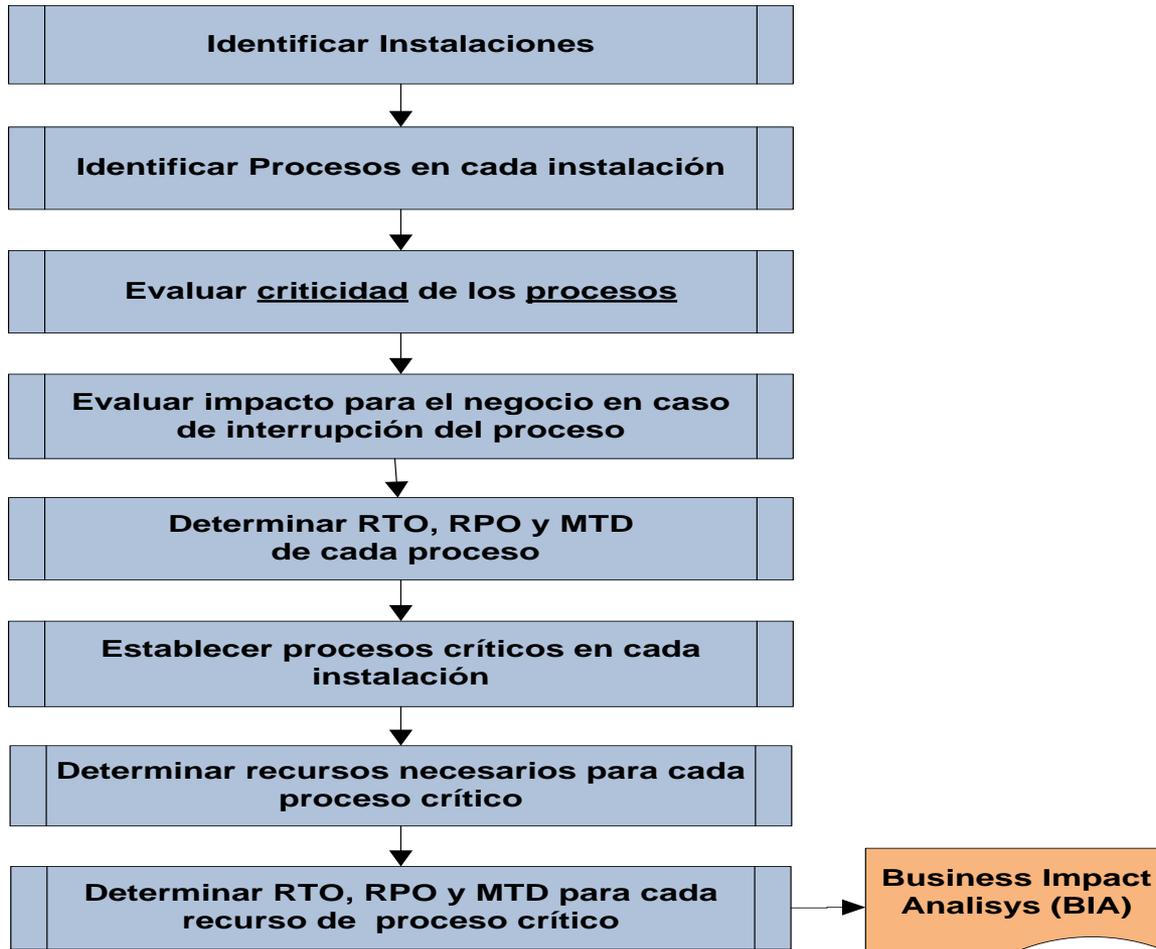
Identificar la urgencia de recuperación de cada función de negocio, determinando el impacto en caso de interrupción.

El nivel de criticidad de una actividad se mide en relación a la dependencia que tiene la compañía sobre ésta, y de cómo repercute sobre la organización el hecho de que no se pueda realizar dicha actividad.

En términos económicos esta valoración sería responder a la pregunta de **cuánto perdería la compañía** si la actividad/proceso no estuviera disponible.

Dentro del Análisis de Impacto deberíamos distinguir los siguientes grupos de cuestiones:

Elaborar Bia's



- Impacto Material:**
- Impacto económico directo
 - Lucro cesante
 - Coste de oportunidad
 - etc.
- Impacto Intangible:**
- s/Clientes
 - s/otras Compañías
 - Reputación
 - Legal
 - etc.
- RTO** – Objetivo de Tiempo de Recuperación

RTO y RPO

RTO es el tiempo en que precisa la empresa para que el servicio caído se restablezca. Ejemplo, un RTO de 5 minutos para el correo es que si el servicio cae, en 5 minutos ha de estar restablecido.

RPO es la cantidad de tiempo/información que estamos dispuestos a perder. Un RPO de 8 horas es el tiempo que la empresa puede permitirse el lujo de perder todos los cambios que se han efectuado durante ese tiempo.

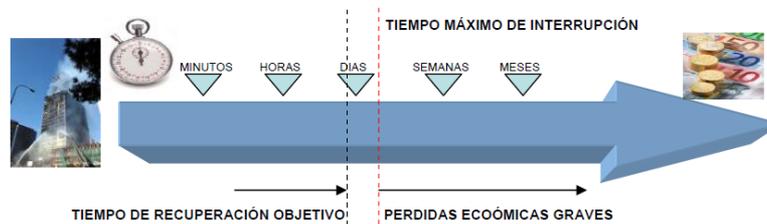


Figura 2. Tiempos de Recuperación

MTD

Se puede definir como Mejores Técnicas Disponibles aquellas tecnologías utilizadas en una instalación junto con la forma en que la instalación esté diseñada, construida, mantenida, explotada y paralizada, y siempre que sean las más eficaces para alcanzar un alto nivel de protección en su conjunto y que puedan ser aplicadas en condiciones económica y técnicamente viables.

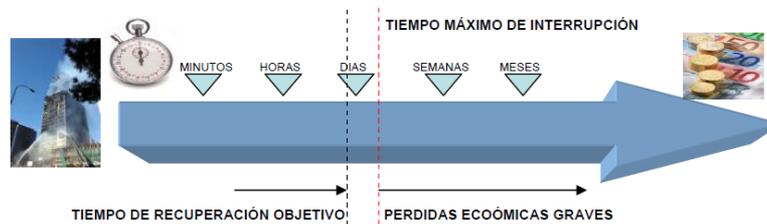


Figura 2. Tiempos de Recuperación

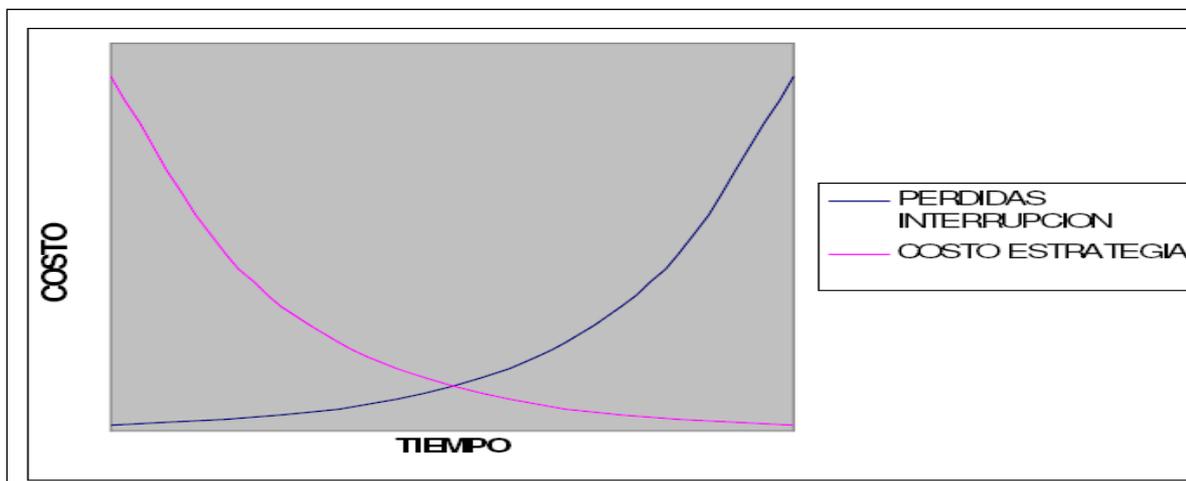
Elaborar Bia's

- Elaborar Bia's
- Análisis de Riesgos
- Estrategias de Mitigación
- Desarrollar el Plan
- Pruebas y Mantenimiento
- Concienciar



ANÁLISIS DE IMPACTO

Los datos obtenidos de los BIA's nos permitirán realizar este análisis.



COSTE MATERIAL		
0 - 250	1	BAJO
250 - 500	2	MEDIO
500 - 1M	3	ALTO
> 1M	4	MUY ALTO

TIEMPO	
> 2 SEMANAS	1
1 - 2 SEMANAS	2
72 HORAS - 1 SEMANA	3
24 - 72 HORAS	4
< 24 HORAS	5

(CLIENTES/ LEGAL/REPUTACION)		
BAJO	1	BAJO
MEDIO	2	MEDIO
ALTO	3	ALTO
MUY ALTO	4	MUY ALTO

ANALISIS DE IMPACTO

A raíz de lo anteriormente analizado podremos realizar un Mapa de Prioridades Departamentales, sumamente descriptivo:

AREA	CRITICIDAD COSTO / TIEMPO	TOTAL ACTIVIDADES	4 HORAS	<= 1 DIA	<= 3 DIAS	<= 1 SEMANA	<= 2 SEMANAS	<= 3 SEMANAS	> 1 MES
RRHH	3,04	4		4					
SINIESTROS RCP	2,80	6		4		1		1	
SINIESTROS AUTOS	2,69	4		3		1			
ASESORIA JURIDICA	3,03	5		2	3				
COMPRAS Y SSGG	1,74	11		1	3		5	2	
PRODUCCION AUTOS	2,95	4			4				
PRODUCCION RAMOS DIVERSOS	2,94	1			1				
CONTABILIDAD	2,85	4			1	1	1	1	
SINIESTROS RAMOS DIVERSOS	1,91	2				2			
FINANCIERO	1,83	4				1	3		
MARKETING Y PRODUCTOS	1,91	3		1			2		
COMERCIAL	1,50	3						3	
TECNICO - ACTUARIAL	1,03	2						2	
Total General	2,33	53	0	15	12	6	11	9	0

Análisis de Riesgos



El objetivo es detectar y analizar las **amenazas** que potencialmente puedan afectar a las actividades que queremos proteger en la entidad.

La evaluación de riesgos supone **anticipar** lo que puede ir mal y a continuación **estimar el impacto** que supondría para la organización.

Análisis de Riesgos



En lo fundamental, la evaluación de riesgos que se ha de llevar a cabo ha de contestar, con la mayor fiabilidad posible, a las siguientes preguntas:

- ❖ ¿Qué se intenta proteger?
- ❖ ¿Cuál es su valor?
- ❖ ¿Cuál es la probabilidad de que ocurra?

Y con esta evaluación proceder a:

- ❖ Identificación de Activos
- ❖ Identificar Amenazas
- ❖ Evaluar Probabilidades de Ocurrencia de Amenazas
- ❖ Evaluar Impacto
- ❖ Evaluar Riesgo
- ❖ Evaluar Alternativas

3. PROBABILIDAD DE OCURRENCIA

Las amenazas tendrán una probabilidad de ocurrencia que dependerá de la **existencia de una vulnerabilidad** que pueda ser explotada, para materializarse en un incidente.



Por ejemplo una amenaza del tipo de desastre natural como es un terremoto, tendrá una mayor probabilidad de ocurrencia en una empresa con oficinas en Japón, donde los terremotos ocurren con mayor frecuencia.

4. IMPACTO

Los incidentes causan un **impacto** dentro de la organización, que también deberá tomarse en cuenta a la hora de calcular los riesgos.

La valoración del impacto puede realizarse de forma **cuantitativa**, estimando las pérdidas económicas,



O de forma **cualitativa**, asignando un valor dentro de una escala (p.e. alto, medio, bajo).



ANALISIS DE RIESGOS

Daremos diferentes “Pesos” o ponderaciones a los distintos Activos definidos, en función de lo estudiado en la Identificación de Activos de la Compañía. Por ejemplo:

PONDERACION GLOBAL	
COMPLEJO	28%
SISTEMAS	47%
PROVEEDORES	17%
CAPITAL HUMANO	8%

Los pesos han sido determinados en base a:

- Compañía con poca rotabilidad de personal. El peso del capital humano expuesto al riesgo es bajo.
- Posee un edificio nuevo dotado de altas medidas de seguridad mitigadoras de accidentes, que hacen que el riesgo de complejo tampoco sea excesivamente alto.
- El mayor peso se le da a los sistemas, por tener pocas medidas de seguridad en el CPD.
- Existen acuerdos con proveedores (SLA's) y barajan diferentes alternativas de ahí un peso no muy excesivo

CURSO

1. INTRODUCCIÓN

Introducción
Situación Actual
Objetivo

2. MEJORES PRÁCTICAS

Marco Conceptual. Referencias Normativas
Definición de un BCP, Business Continuity Plan
Plan de Continuidad al Servicio

3. ADAPTACIÓN AL NEGOCIO ASEGURADOR. FASE I – DIAGNÓSTICO

Revisión y Análisis de BIA
Evaluación Riesgos y Controles
Análisis CAT

4. ADAPTACIÓN AL NEGOCIO ASEGURADOR. FASE II – IMPLEMENTACIÓN

Acciones Mitigación de Riesgo
Entrenamiento, Pruebas, Auditoría
Desarrollo del Plan de Continuidad al Servicio
Mantenimiento del Plan de Continuidad al Servicio

Estrategias de Mitigación



Detectar los riesgos, mitigarlos puede llegar a evitar la ejecución del BCP. Implementar medidas tales como:

- **Controles Preventivos**, copias de seguridad, control accesos físicos y lógicos ...
- **Controles Detectivos**, monitorización, auditorías, sensores de humo ...
- **Controles Correctivos**, Recuperación de datos perdidos, corrección de datos dañados (virus) ...

Esto es desarrollar **Estrategias de Mitigación**.

Estrategias de Mitigación



EVALUAR PERIODICAMENTE EN FUNCIÓN DE COSTE BENEFICIO

Un ejemplo de las diferentes estrategias para reubicación funcional:

- No hacer nada. Asumir el Riesgo.
- Utilización de espacios propios.
- Reutilización de recursos.
- Trabajo Remoto o Teletrabajo.
- Acuerdos Recíprocos.
- Sitio alternativo subcontratado a terceros:
 - ✓ Espacios dedicados.
 - ✓ Espacios compartidos.
 - ✓ Móviles.
 - ✓ Módulos prefabricados.
 - ✓ Replica de instalaciones...

Estrategias de Mitigación



Siguiendo con la distribución de Recursos que habíamos planteado ofrecemos por cada uno de ellos Estrategias de Mitigación:

Complejo:

Trabajo en Remoto

En Centro Alternativo

Replicar ubicaciones de trabajo

Sistemas:

CPD alternativo

Pruebas de restauración de datos

Conexión a Internet en domicilio personal crítico

Proveedores:

Acuerdos SLA's

Proveedores Alternativos

Datos de contacto con proveedores actualizado

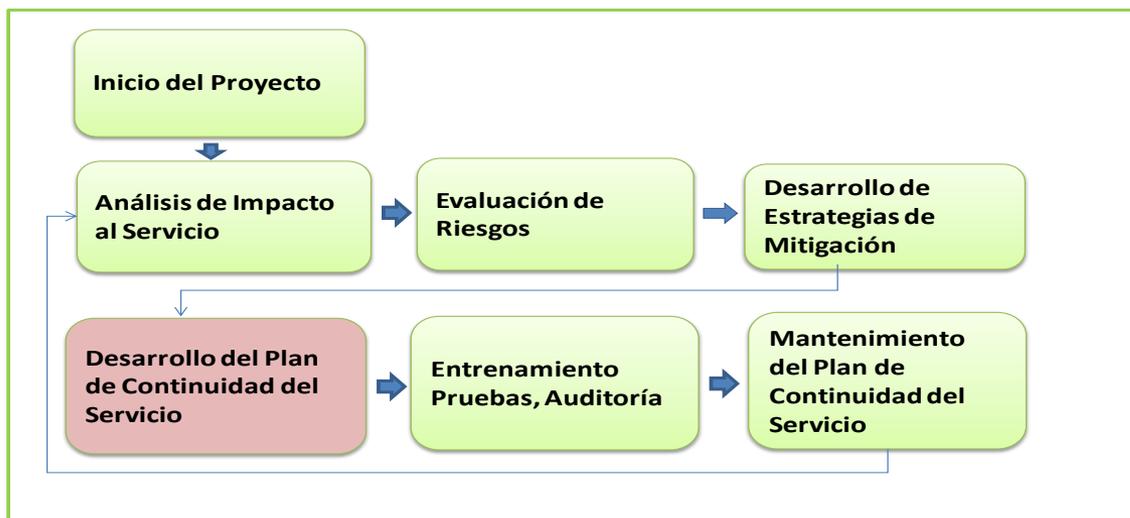
Capital Humano:

Formación multiarea

Documentación de procesos

Back-up para Apoderados, Consejeros con certificados digitales , claces etc...

Desarrollar el Plan



Esta fase del proyecto pasa por definir:

- Los **equipos** necesarios para su desarrollo.
- **Responsabilidades y funciones** de cada uno de los diferentes equipos.
- Nivel de **Dependencias** entre los diferentes equipos.
- Desarrollar los diversos **procedimientos de alerta y actuación** ante los diferentes eventos que puedan activar el Plan.
- La estrategia de **vuelta a la normalidad** de negocio previo a la situación que originó el marco de actuación.

Desarrollar el Plan



Probar y Mantener



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

Probar y Mantener



Probar y Mantener



Mantenimiento

Igualmente el documento en si mismo deberá ser revisado cada vez que la compañía, por su propia dinámica de negocio, vaya incorporando nuevas soluciones a los Sistemas de Información y los activos informáticos, así el BCP irá evolucionando para dar respuesta a las necesidades planteadas

Durante las pruebas se detectarán mejoras a implementar en el BCP de cara a una mayor efectividad. La baja de un empleado o el cambio de Departamento, el cambio de teléfono de contacto de un usuario que forma parte del BCP, significará una revisión del mismo.

Concienciar



Un BCP es un concepto aplicable a todo tipo de empresa y debe considerarse como un plan vivo y dinámico.

El beneficio más importante es el conocimiento de la operación y de todos y cada uno de quienes participan en cada proceso crítico.

No sólo es para los directivos, sino para todos los elementos que forman parte de la organización, aunque la decisión de elaborar un plan de contingencia debe partir del equipo directivo ya que involucra la supervivencia de la misma.



COL·LEGI D'ACTUARIS DE CATALUNYA

www.actuaris.org
actuaris@actuaris.org