Universitat de Barcelona

20

El plan de contingencias en la empresa de seguros

Estudio realizado por: Sergi Casas i del Alcázar
Tutor: Antonio Parra Eizagaetxebarría

Tesis del Master en Dirección de Entidades Aseguradoras y Financieras

Curso 2010/2011

Esta publicación ha sido posible gracias al patrocinio del Grupo Asegurador Catalana Occidente

Presentación

A Aram y Eva, por haber aguantado la falta de padre y compañero respectivamente durante tanto tiempo.

A Antonio, por haberle dedicado todo el tiempo necesario y estar siempre dispuesto a ayudarme.

Al resto, que no definiré porque sería incapaz de hacer una lista exhaustiva, y me dolería no mentarlos a todos.

Resumen

El negocio asegurador es el mejor conocedor de que las catástrofes ocurren, y que el impacto que estas tienen en la continuidad de un negocio puede ser nefasto si no se han tomado las medidas oportunas.

Un plan de contingencias es necesario en cualquier negocio, pero cuando hablamos de seguros, pasa a ser imprescindible. Uno de los departamentos que más vulnerable es a estos hechos es el de IT. La mayoría de empresas tiene como mínimo un sistema de copias para evitar perdida de datos, pero muchas de ellas se olvidan que no solo la informática es necesaria para continuar el negocio. Sin las personas que componen el negocio asegurador en sí, no tiene sentido restaurar todo lo demás.Por esto, esta tesis se divide en dos: El plan de contingencias en IT, y el plan de contingencia en las áreas de negocio propiamente dichas.

Resum

El negoci assegurador és el millor coneixedor de que les catàstrofes ocorren, i que l'impacte que aquestes tenen en la continuïtat d'un negoci pot ser nefast si no s'han pres les mesures adequades.

Un pla de contingències és necessari en qualsevol negocio, però quan parlem d'assegurances, passa a ser imprescindible. Un dels departaments que més vulnerable és a aquests fets és el de IT. La majoria d'empreses tenen com a mínim un sistema de copies per evitar pèrdua de dades, però moltes d'elles s'obliden que no només la informàtica és necessària per continuar el negoci. Sense les persones que composen el negoci assegurador en sí, no te sentit restaurar la resta. Per tot això, aquesta tesi es divideix en dos: El pla de contingències en IT, i el pla de contingència en les àrees de negoci pròpiament dites.

Summary

The Insurance sector is the best knower that catastrophic events happen, and that its impact on business continuity could be disastrous if no countermeasures have been taken.

A business continuity plan is necessary in any business, but when we are talking about insurance, it's essential. The most vulnerable department to catastrophic events is the IT department. Almost all companies have at least a backup system to avoid data loss, but most of them forget that not only IT is necessary for business continuity. Without people who work in the insurance business, it has no sense to restore all systems. That's the reason to divide this study in two sections: business continuity plan for the IT department, and business continuity plan for the rest of the departments.

Índice

Presentación 3
Resumen 5
Resum 5
Summary 5
Índice 7
El plan de contingencias en la empresa de seguros 9
1 Introducción 9
1.1 El plan de contingencias 9
1.2 Estructura de la tesis 12
2 Conceptos básicos y nomenclatura 13
3 El plan de contingencia en TI 19
3.1 Fase de análisis 20
3.2 Fase de diseño de la solución 23
3.2.1 Objetivos de la restauración 24
3.2.2 Equipos 31
3.2.3 Workflow del plan de contingencias 33
3.3 Implementación 37
3.4 Pruebas 38
3.5 Mantenimiento 39
4 El plan de contingencia en el resto de unidades de negocio 41
4.1 Fases del plan de contingencia 42
4.1.1 Fase de análisis 42
4.1.2 Fase de diseño de la solución 43
4.1.3 Fase de implementación 45
4.1.4 Fase de pruebas 46
4.1.5 Fase de mantenimiento 46
4.2 Departamentos 46
4.2.1 Suscripción 47
4.2.2 Siniestros 49
4.2.3 Tesorería 49
4.2.4 Área financiera 51
4.2.5 Contact Center 51
4.2.6 Otros profesionales 53
5 Conclusiones 55
6 Bibliografía 57
7 Anexos 59
7.1 Plantilla recogida de datos 59
8 Currículum: Sergi Casas i del Alcázar 63

El plan de contingencias en la empresa de seguros

1 Introducción

Esta tesis quiere servir de guía para poder implantar un plan de contingencias en una empresa de seguros.

Como lamentablemente se ha podido observar últimamente, hay que estar preparado para los grandes desastres. Incidentes como los atentados de las torres gemelas, el incendio del edificio Windsor, o las grandes catástrofes naturales que asolan cada vez más frecuentemente el planeta han acabado con centenares de empresas por no estar preparadas para hacer frente a dichos desastres.

Por todo esto, las empresas están tomando cada vez más conciencia de la importancia de los planes de contingencias. Muchas de las empresas más importantes que se hallaban en las torres gemelas, y que perdieron grandes cantidades de información, se han decantado ahora por sistemas de duplicidad de datos en diferentes áreas, para no verse afectadas por el mismo incidente en los dos sitios simultáneamente.

Así, empresas como Merrill Lynch, que perdió los dos CPD's que tenía en las torres gemelas, actualmente los tiene ubicados uno en Staten Island y el otro en Nueva York.

Morgan Stanley es otro buen ejemplo de empresa de finanzas que posteriormente al 11-S duplicó sus sistemas en lugares más alejados uno del otro, ya que perdió gran parte de sus archivos en el mismo atentado. También ha instaurado sistemas de prueba de planes de contingencia ante la pérdida total de uno de sus centros como una rutina más en su negocio.

1.1 El plan de contingencias

Un plan de contingencias identifica la exposición de la organización a amenazas externas e internas, y sintetiza las medidas a tomar para prevenir y recuperarse de dichas amenazas en caso de producirse. El objetivo de dicho plan es el de asegurar la continuidad del negocio en caso de desastre.

En otras palabras, el BCP (Business ContinuityPlanning) es una manera de trabajar para continuar con el negocio en caso de desastre. Ejemplos de desastre incluyen eventos locales como incendios de edificios, eventos regionales como te-

rremotos o inundaciones, o eventos nacionales, como enfermedades pandémicas. Además de todos estos, cualquier evento que potencialmente pueda provocar una perdida en la continuidad de negocio debe ser considerado, así como cualquier evento que afecte a un recurso del que depende el negocio, como falta de suministros, perdida de infraestructuras críticas (como una maquinaria específica, un servidor, una red), robos o vandalismo. Por todo esto, la administración de riesgos debe ser incorporada como una parte del BCP.

Un ciclo completo de BCP da como resultado un manual impreso disponible como referencia antes, durante y después de les disrupciones. Su objetivo es reducir el impacto negativo del evento tanto en el ámbito de disrupción (que y quien se ve afectado) como en la duración (horas, días, meses…).

Dicho ciclo se compone de 5 fases principales (Figura 1):

1. Análisis
2. Diseño de la solución
3. Implementación
4. Pruebas y aprobación por parte de la organización
5. Mantenimiento

A continuación se hace un repaso de cada una de ellas.

Figura 1

Análisis

Esta fase consiste de un análisis de impacto (BIA. Ver capítulo 2, Conceptos básicos y nomenclatura), un análisis de amenazas y unos escenarios de impacto, y da como resultado la documentación de requerimientos.

El análisis de amenazas consta de una lista de amenazas potenciales las cuales tengan pasos únicos de recuperación. Por ejemplo, no es lo mismo una recuperación de un terremoto, donde probablemente haya que reconstruir o trasladar el negocio, a una enfermedad, donde no hay que reconstruir nada, sino buscar perfiles humanos para sustituir a los afectados.

Por último se debe hacer una relación de escenarios de impacto. El terremoto anteriormente citado podría afectar el centro de proceso de datos, donde residen

todos los servidores de la empresa, o podría afectar un centro de servicios, donde solo hay personal y ordenadores personales. En cada caso, el impacto y las acciones a realizar serian diferentes.

Una vez completados estos pasos, se documenta todo para empezar las fases de diseño e implementación.

Diseño de la solución

El objetivo de esta fase es identificar las soluciones de recuperación ante desastres más efectivas en cada caso, que cumplan los dos requerimientos principales del BIA (RPO y RTO). Ver capítulo 2, Conceptos básicos y nomenclatura). En el caso de las aplicaciones de TI, normalmente son:

- Las mínimas aplicaciones y datos de aplicación requeridos para la continuidad del negocio
- El plazo de tiempo en que tienen que estar disponibles dichas aplicaciones y datos.

En el resto de unidades del negocio, será necesario contemplar como mínimo los siguientes puntos:

- Perfiles de usuario necesarios para desarrollar las actividades mínimas imprescindibles para mantener la continuidad de negocio.
- Instalaciones donde ubicar dichos perfiles.

En esta fase también se diseña el circuito de alertas y disparo del plan de contingencia, definiendo responsabilidades y equipos que llevarán a cabo dicho plan.

Implementación

Es sencillamente la implementación de los elementos identificados en la fase de diseño.

Pruebas y aprobación por parte de la organización

El propósito de las pruebas es alcanzar la aprobación por parte de la organización de la solución de continuidad de negocio, demostrando que con el seguimiento de dicho plan se cumplen los requisitos impuestos por el negocio. Las pruebas pueden incluir:

- Pruebas técnicas de traslado del negocio desde la ubicación primaria a la secundaria.
- Pruebas técnicas de traslado del negocio desde la ubicación secundaria a la primaria.
- Pruebas de aplicaciones
- Pruebas de procesos de negocio.

Como mínimo, estas pruebas se hacen 1 o dos veces al año. Los problemas encontrados durante las pruebas, son incorporados a la fase de mantenimiento, y vueltos a probar en la siguiente fase de pruebas.

Mantenimiento

El proceso de mantenimiento se divide en 3 actividades periódicas. La primera actividad es la confirmación de la información contenida en el manual, concienciar a todo el personal y formar a las personas con roles identificados como críticos en caso de desastre. La segunda es probar y verificar las soluciones técnicas establecidas para las operaciones de recuperación. Por último, se prueba y verifican los procedimientos de recuperación de la organización documentados. Normalmente este proceso se repite una o dos veces al año.

Es importante mantener la información actualizada puesto que la empresa cambia con el tiempo, y el BCP debe cambiar con ella para seguir siendo útil. Algunos de los cambios que deberían ser reflejados y actualizados en el manual son:

- Cambios en las responsabilidades del personal
- Cambios de personal
- Cambios de clientes importantes y en sus datos de contacto
- Cambios en proveedores y en sus datos de contactos
- Cambios departamentales

Según la empresa sobre la que se quiera implementar, habrá decisiones que no coincidirán con las propuestas en el modelo. No hay estrategias mejores que otras. En cada caso se podrán aplicar unas u otras según el entorno, los costes, etc.

1.2 Estructura de la tesis

Después de definir una serie de términos para poder comprender el resto del texto en el capítulo 2 (algunos de ellos ya apuntados en la descripción de un plan de negocio), se empezará a desglosar un plan de contingencia “modelo”, comentando en cada punto la solución propuesta, y el porqué de la elección.

Como se podrá observar, tanto el capítulo 3 como el capítulo 4 tienen la misma estructura, dado que se ha seguido el mismo procedimiento mencionado anteriormente, primero para las unidades de TI, y luego para el resto de procesos de negocio considerados críticos para la organización.

En el capítulo 4 no se ha pretendido hacer un análisis exhaustivo de todas las unidades de negocio de una empresa de seguros. Estas variarán según la empresa, sus prioridades y necesidades. Las que se muestran son un ejemplo, escogidas por sus particularidades, y extrapolar lo dicho aquí a otras unidades de negocio no debería ser un problema.

2 Conceptos básicos y nomenclatura

Este capítulo pretende ser una guía y una base para poder comprender el resto de capítulos de esta tesis.

Debido a la imposibilidad de poner un orden en las definiciones, dado que muchas de ellas hacen referencia a otras definiciones, he decidido ponerlas en orden alfabético, para facilitar su búsqueda.

En algunos casos he “adaptado” las definiciones al tema de la tesis, dado que algunas de ellas son empleadas en muchas áreas.

BIA: BussinessImpactAnalysis.

Un análisis de impacto de negocio da como resultado la diferenciación entre las funciones o actividades críticas y no críticas de la organización. Una función es considerada crítica si las implicaciones del daño a los afectados son inaceptables. La consideración de que una función sea o no crítica será modificada por el coste de establecer y mantener soluciones de recuperación apropiadas, tanto desde el punto de vista técnico como empresarial. Dicho de otro modo, si el coste de evitar la discontinuidad en la función es mayor que el valor que aporta la función al negocio, el proceso puede pasar a ser no crítico (ya que considerarlo crítico implicaría unos costes inaceptables para el negocio). Una función puede ser considerada crítica porque haya una ley que así lo establezca.

Por cada función crítica, se asignan dos valores:

- Recovery Point Objective (RPO): Latencia aceptable de datos que serán recuperados.
- Recovery Time Objective (RTO): Cantidad de tiempo aceptable para restaurar la función.

El RPO debe asegurar que la cantidad máxima aceptada de pérdida de datos para cada actividad no sea excedida. El RTO debe asegurar que el período de discontinuidad de negocio máximo aceptado para cada actividad no sea excedido.

El siguiente paso del BIA da como resultado los requerimientos de restauración para cada función crítica. Los requerimientos de restauración se dividen en requerimientos de negocio y en requerimientos técnicos. Trataremos estos requerimientos durante el resto de la tesis.

CPD(Centro de proceso de datos)

Se denomina centro de procesamiento de datos (CPD) a aquella ubicación donde se concentran los recursos necesarios para el procesamiento de la información de una organización. También se conoce como centro de cálculo o centro de datos, por su equivalente en inglés:data center.

Dichos recursos consisten esencialmente en unas dependencias debidamente acondicionadas, servidores y redes de comunicaciones.

Replicación síncrona y asíncrona de datos

En la copia síncrona de datos se asegura que todo dato escrito en el CPD principal también se escribe en el centro de respaldo antes de continuar con cualquier otra operación. Esto hace que la perdida de datos en caso de desastre sea nula (RPO igual a cero).

La desventaja en este sistema es que como la cabina principal debe esperar a que el dato se haya grabado en la cabina secundaria, se introduce un delay en la transacción, que hace que el sistema en general vaya más lento (afecta a la producción). Además, hay que tener en cuenta que a partir de ciertas distancias, la latencia que se produce al enviar el dato de un CPD al otro hace que este sistema sea inviable.

En la copia asíncrona de datos no se asegura que todos los datos escritos en el CPD principal se escriban inmediatamente en el centro derespaldo, por lo que puede existir un desfase temporal entre unos y otros. Esto hace que los RPO's sean de unos minutos.

La contrapartida es que como la cabina principal no debe esperar respuesta de la secundaria, no se pierde tiempo en la grabación del dato, y por tanto no afecta al rendimiento de producción. Como la copia no es al segundo, los delays provocados por distancias grandes entre CPD's no afectan tanto como en el caso de la copia síncrona (aunque puede llegar a afectar dependiendo de la distancia y la cantidad de datos enviados).

RPO: Recovery Point Objective.

Describe la cantidad aceptada de datos perdidos medidos en tiempo.

El RPO es el punto del tiempo definido por la organización en el que se deben recuperar los datos. Es lo que suele conocerse en la organización como "perdidas

aceptables” en caso de desastre. El RPO permite a una organización definir una ventana de tiempo antes de un desastre durante la cual puede haber pérdida de datos. El valor de los datos dentro de dicha ventana puede ser comparado con el coste adicional en medidas de prevención de desastres o de prevención de perdida de datos (copias de seguridad, replicación de datos, etc.) para hacer la ventana más pequeña (y por tanto perder menos datos).

El RPO es independiente del tiempo que se tarde en volver a tener en funcionamiento el sistema (el RTO). Si el RPO de una compañía es de dos horas, entonces, cuando el sistema vuelva a estar en línea después de un desastre, todos los datos deben ser restaurados en un punto del tiempo dentro de las dos horas anteriores al desastre. La compañía debe ser consciente de que los datos introducidos durante las dos horas anteriores al desastre se pueden haber perdido.

RTO: Recovery Time Objective.

Es el tiempo y el nivel de servicio en que un proceso de negocio ha de ser restaurado después de un desastre, para evitar consecuencias inaceptables para la continuidad del negocio.

Este indicador incluye el tiempo empleado para tratar de corregir el problema sin restaurar, la restauración en sí, las pruebas y la comunicación a los usuarios.

El RTO se establece durante el BIA por el propietario del proceso (usualmente con el responsable del plan de continuidad de negocio).

El RTO y los resultados del BIA son la base para identificar y analizar estrategias viables para incluirlas posteriormente en el plan de continuidad de negocio. Una estrategia viable es cualquiera que consiga restablecer el proceso de negocio en un tiempo cercano al RTO.

SLA: ServiceLevelAgreement

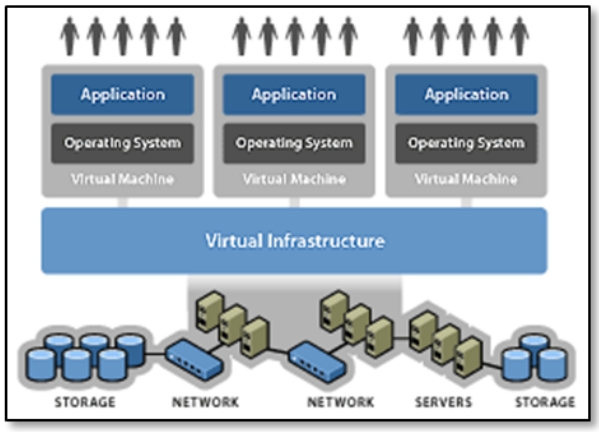
Un ServiceLevelAgreement, también conocido por las siglas SLA, es un contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio. El SLA es una herramienta que ayuda a ambas partes a llegar a un consenso en términos del nivel de calidad del servicio, en aspectos tales como tiempo de respuesta, disponibilidad horaria, documentación disponible, personal asignado al servicio, etc. Básicamente el SLA establece la relación entre ambas partes: proveedor y cliente. Un SLA identifica y define las necesidades del cliente a la vez que controla sus expectativas de servicio en relación a la capacidad del proveedor, proporciona un marco de entendimiento, simplifica asuntos complicados, reduce las áreas de conflicto y favorece el diálogo ante la disputa.

También constituye un punto de referencia para el mejoramiento continuo, ya que el poder medir adecuadamente los niveles de servicio es el primer paso para mejorarlos y de esa forma aumentar los índices de calidad.

Virtualización

Es una tecnología que permite instalar y configurar múltiples ordenadores y/o servidores completamente independientes (conocidas como “virtual machines” o “máquinas virtuales”) en una sola “caja” física, ya sea un ordenador, servidor, “appliance” (hardware específico de un fabricante para un uso concreto. Por ejemplo, existen appliance de antivirus, que son máquinas fabricadas solo para hacer de antivirus), etc.

A pesar de que estas máquinas virtuales comparten todos los recursos de un mismo “hardware”, cada una trabaja de manera totalmente independiente (con su propio sistema operativo, aplicaciones, configuraciones, etc.).



En otras palabras, en lugar de utilizar 5 servidores físicos, cada uno de ellos corriendo una aplicación que solo utiliza el 10% de los recursos de su servidor; podemos instalar 5 máquinas virtuales, cada una con su propia aplicación y configuraciones específicas, en un solo servidor y utilizar el 50-60% de los recursos del mismo.

Cabe señalar que cada una de estas máquinas virtuales, con la debida configuración, deberá funcionar exactamente igual que un servidor o PC físico (se podrá conectar a una red, introducirlo en un dominio, aplicarle políticas de seguridad, conectarse de manera remota, hacer un “restart” de manera independiente, etc.).

Al final obtenemos una implementación que será:

- **Más económica** – Requiere menos hardware, menos electricidad, menos enfriamiento, menos espacio, menos infraestructura, y menos tiempo de administración.

- **Menos compleja** – Por las mismas razones mencionadas en el punto anterior.

- **Consume menos energía y espacio** – Al necesitar menos hardware, y aprovechar este al máximo, se ahorra la energía de los servidores físicos que no se arrancan, el espacio que estos ocupan, y la refrigeración necesaria (tanto porque no se genera tanto calor, como por que las salas donde se ubican dichos servidores pueden ser más pequeñas).

- **Más segura** – Con los niveles de seguridad adecuados, una red virtual cuenta con menos puntos de ataque físicos, lo que la hace más segura. En adición a esto, la vitalización es una excelente estrategia de seguridad al momento de elaborar un plan de contingencias.

- **Más fácil de administrar** – Con el debido conocimiento de virtualización y evitando el conocido “temor al cambio”, administrar una red virtual debe ser más sencillo que administrar una red regular.

3 El plan de contingencia en TI

La actual estrategia de continuidad del negocio en una empresa de seguros está fundamentada principalmente en la recuperación de los servicios tecnológicos. Sin estos servicios, el negocio asegurador como tal no puede continuar, y por tanto es indispensable que se dediquen grandes recursos para garantizar no solo la recuperación en caso de desastres, sino también un alto grado de disponibilidad ininterrumpida, para evitar la recuperación.

Es por todo esto que el plan de continuidad de una empresa de seguros debe centrarse en contingencias que puedan producirse en los CPD's, contemplando para los centros de servicio únicamente aquellas acciones que permiten desviar su carga de servicio a otros centros alternativos.

Precisamente para facilitar la continuidad del negocio, se recomienda no solo tener un buen plan de contingencias, sino tomar también una serie de decisiones tecnológicas enfocadas a incrementar la disponibilidad de los sistemas, facilitar la movilidad de los puestos de trabajo y minimizar el impacto de cualquier tipo de contingencia. Entre estos podríamos destacar:

- La centralización de los servicios tecnológicos, cosa que permite simplificar los planes de recuperación (es más fácil restaurarlo todo que partes, y modificar lo que no ha caído para que se acople a lo restaurado)

- La virtualización de los entornos. Hoy día se habla mucho de la virtualización como una herramienta para facilitar la gestión y aprovechar los recursos Hardware, pero no solo tiene estas ventajas. Un sistema virtualizado es un sistema mucho más sencillo de restaurar, dado que es totalmente independiente del Hardware en que es restaurado.

- La no dependencia de plataformas físicas propietarias. Al igual que se consigue con la virtualización, existen métodos de "virtualizar" otros sistemas de la compañía, como podría ser la telefonía. En este sentido, la implantación de la VoIP puede ayudar a una recuperación más rápida y barata que si se tiene que restaurar una central telefónica estándar.

- Aunque las copias a cinta son indispensables hoy día, es muy recomendable la duplicidad de datos por otros medios, como podría ser a través de réplicas entre cabinas de disco en diferentes ubicaciones.Esto es, cuando un dato se escribe en uno de los servidores del CPD principal, es automáticamente copiado a un CPD de backup, desde donde se pueden recuperar todos los servicios en caso de desastre.

- Evitar en la medida de lo posible que las estaciones de trabajo tengan software especializado. Dando todos los servicios principales vía web, se evita que las máquinas clientes tengan que tener instalado nada más que el navegador. Gracias a esto, los usuarios pueden operar desde cualquier

PC con conexión a la red, sin tener que desplegar aplicaciones especiales. Obviamente esto no se puede conseguir al 100%, pero sí que nos permite marcar un camino, que deberíamos seguir siempre que se pueda.

A continuación se tratarán una por una las fases para generar un plan de contingencias, siguiendo el guión expuesto en el capítulo de introducción, y haciendo especial hincapié en las dos primeras fases (análisis y diseño de la solución), ya que son las que dan como resultado el plan de continuidad. Las últimas 3 (implementación, Pruebas y Mantenimiento) se plantearan como un ejercicio teórico, ya que no son el objetivo de esta tesis.

En cada decisión, se pretende dar las razones por las que se toma, así como exponer alternativas en los casos más significativos.

3.1 Fase de análisis

Con el objetivo de estar permanentemente preparados ante la eventualidad de algún suceso que pudiera provocar una interrupción del negocio, los riesgos potenciales son revisados periódicamente. Este proceso sirve para identificar nuevos riesgos, confirmar la vigencia de los ya existentes y proponer recomendaciones para la minimización de su posible impacto en la operativa diaria de la compañía. Esta fase y la de mantenimiento se superponen en muchos casos, ya que cuando se realiza el mantenimiento del plan, no se está haciendo otra cosa que analizar el plan actual y actualizarlo en caso necesario.

En todo negocio asegurador podemos dividir en 4 los entornos principales susceptibles de riesgo.

- Sistemas de información y aplicaciones. Este entorno engloba a todas las aplicaciones y bases de datos albergadas en los ordenadores centrales, ya sea en una cabina de discos o en un robot de cintas, así como las aplicaciones y bases de datos que estén albergadas en el sistema distribuido de servidores.

- Sistemas de comunicaciones y telefonía. Este entorno engloba todas las aplicaciones y sistemas hardware que posibilitan la comunicación de los sistemas informáticos de la compañía, tanto a nivel de la red interna, como de comunicación con sistemas exteriores. Incluye, asimismo, toda la infraestructura necesaria para el funcionamiento de la telefonía por IP o analógica.

- Puestos de trabajo. Esta categoría tiene en consideración solo la disponibilidad de estaciones de trabajo (Workstations), para que puedan llevar a cabo las actividades propias de su responsabilidad en la compañía. Los perfiles de usuario necesarios así como las ubicaciones y otras consideraciones se expondrán en el capítulo 4. Aún y así, se hará excepción de lo dicho anteriormente en el caso de los usuarios del área de IT. Es decir, se tendrá en cuenta qué perfiles de esta área serán necesarios en caso de contingencia.

- Instalaciones físicas. Aquí se engloban todas las instalaciones donde residen los equipos informáticos, de comunicaciones y workstations. Como en el caso anterior, solo se tiene en cuenta en este capítulo las instalaciones directamente relacionadas con el entorno IT (CPD's, salas de comunicaciones, salas de consolas, etc.).

Aunque dos de los puntos se podrían resumir en uno (sistemas de información y aplicaciones y sistemas de comunicaciones y telefonía), se han querido diferenciar debido a que en muchos casos las comunicaciones y la telefonía no son de responsabilidad directa de la compañía, sino de la empresa de comunicaciones que da el servicio, y por tanto corresponden a esta las medidas oportunas para su continuidad en caso de contingencia. Aún y así, es necesario mencionar en el plan de continuidad de negocio de la empresa aseguradora que estos elementos existen, que tienen un plan de continuidad, y que es responsabilidad de dicha compañía de telecomunicaciones.

Dentro de cada uno de estos entornos existen multitud de elementos, cada uno de los cuales debe ser evaluado para establecer su criticidad. Debido a la creciente complejidad de dichos entornos, normalmente se hace uso de software especializado para hacer dichos análisis (BIA). Dentro de estas herramientas se establece una estructura jerárquica como la que sigue, siendo la primera la base de la pirámide, y la última la cúspide:

- Instalaciones físicas: CPD's, salas de operación, etc.
- Hardware (Servidores, cabinas de discos, robots de cintas, elementos de comunicaciones, PC's, etc.
- Software base: Sistemas operativos, software de BBDD, sistemas ERP, etc.
- Aplicaciones de negocio: Software diseñado para un área de negocio en concreto. Estas aplicaciones corren sobre el software base antes mencionado.
- Procesos de negocio: Son las áreas del negocio propiamente dicho. Cada una de estas áreas está asociada a unas aplicaciones, las cuales son necesarias para desarrollar su actividad con normalidad.

Una vez establecida la jerarquía, se decide que procesos de negocio son críticos y cuáles no. El software tiene un sistema de valores acumulativos, que da como resultado un BIA, que indica que partes de la infraestructura se deben restaurar y que partes no, así como prioridades en su restauración.

Por ejemplo, si se decide que es crítico para la compañía que el área de autos esté en funcionamiento, el programa marca todos los recursos que quedan por debajo de este proceso de negocio como crítico. Así, las aplicaciones de autos serian críticas y las bases de datos donde estén los datos de dicha área también. Posteriormente dicha criticidad se trasladaría a las servidores que los soportaran, y por último repercutiría en el CPD donde se hallaran estos servidores.

Continuando con el ejemplo, se podría decidir que el proceso de negocio de vida también es crítico para la compañía. Esto afectaría a las aplicaciones de vida, así como a sus bases de datos, pero podría darse el caso que estas bases de datos fueran las mismas que las de autos (o que compartieran información con estas, como por ejemplo los clientes). En este punto, ya tendríamos un elemento de la infraestructura el doble de crítica que el resto. Si seguimos descendiendo en la pirámide, nos encontraremos servidores en común (los que tienen las bases de datos de clientes, como mínimo), y por tanto estarían ubicados en el mismo CPD.

En el ejemplo del gráfico (figura 2), la prioridad seria el CPD (un sitio donde poder instalar los servidores si el original está inutilizado), seguido por los servidores B y C, y posteriormente la base de datos de clientes.

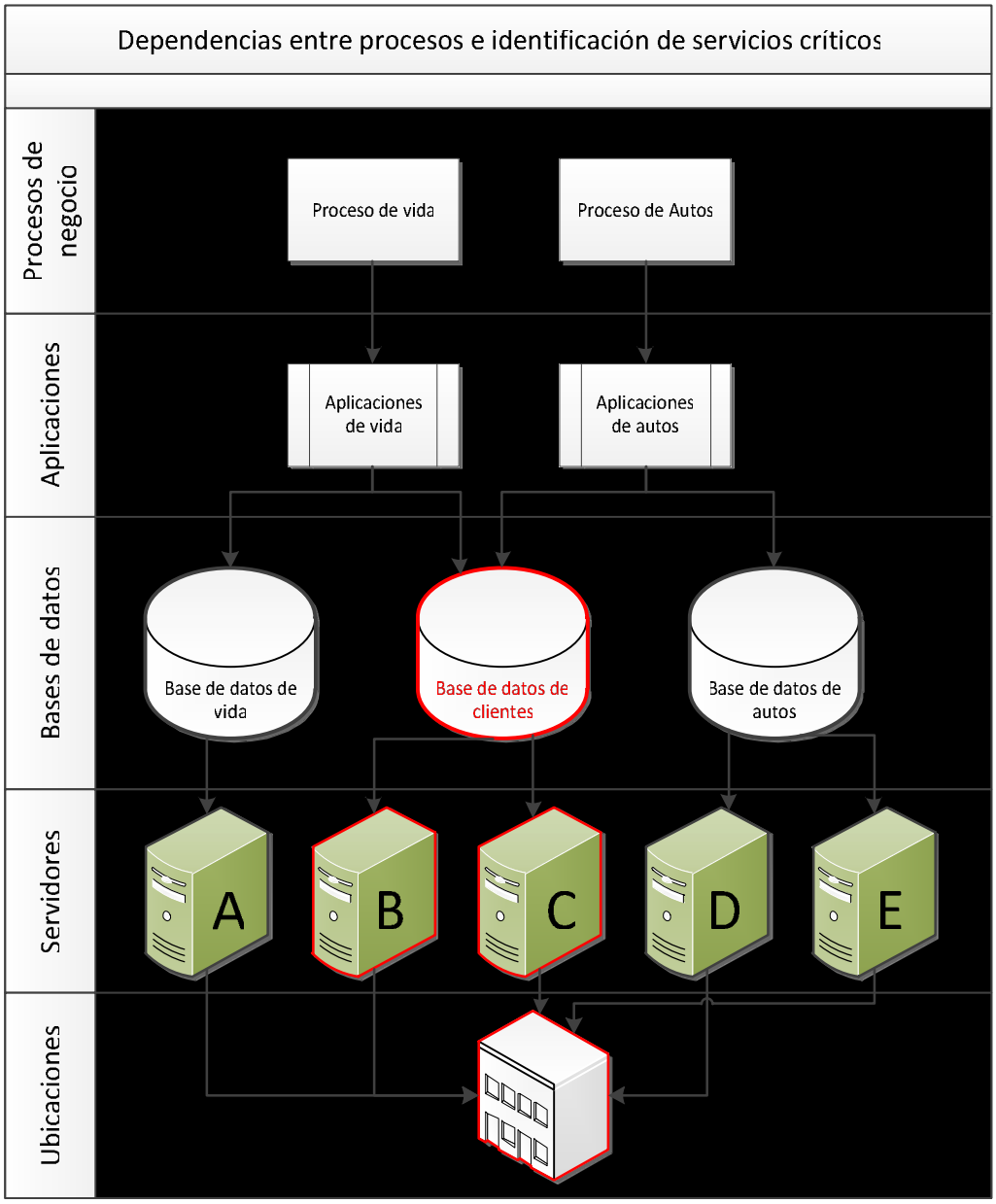


Figura 2

Como se podrá observar, al repetir dicho proceso para cada una de las áreas de negocio de la compañía, se obtendrán una serie de elementos comunes a muchas de ellas que deberán ser restaurados con absoluta prioridad.

Una vez finalizado el BIA, y obtenidos unos elementos críticos, hemos de analizar qué puede afectar a dichos elementos.

Las mismas herramientas utilizadas para el BIA suelen incorporar listas de amenazas que pueden afectar a los distintos elementos. Así, se analiza cada uno de los elementos mencionados, y se asigna una lista de amenazas a las que está expuesto.

Volviendo con el ejemplo anterior, en caso de inundación, un CPD se puede ver afectado. Como este contiene los servidores, esta amenaza también lo es para los servidores contenidos en él, y para el software y aplicaciones que corren en dichos servidores. Como se ve, en este caso la pirámide se recorre a la inversa.

Otra amenaza podría ser el borrado accidental de una base de datos. Ni el software ni los servidores donde corre ser verían afectados (como tampoco lo estaría el CPD, obviamente), pero las aplicaciones que usaran dicha base de datos si, y por tanto los procesos de negocios dependientes de esas aplicaciones también.

Gracias a este sistema, podemos saber a qué son susceptibles cada uno de nuestros procesos de negocio, ya que las amenazas son acumulativas, y por tanto podemos decidir cómo actuar en caso de producirse.

Normalmente todo esto se aprovecha no solo para hacer un plan de continuidad, sino también para establecer contramedidas para evitar que se produzcan dichas amenazas. Por ejemplo, si vemos que el hecho de que se inunde el CPD puede ser desastroso para nuestro negocio, podemos justificar la instalación de detectores de humedad para tratar de evitarlo.

Por último, teniendo en cuenta las amenazas más significativas para nuestro negocio, solo queda plantear los diferentes escenarios de impacto. Esto es, si se inunda, ¿Qué hacemos? No será lo mismo si hay un terremoto y se cae el edificio, que si hay una pandemia y nos quedamos sin personal. Tampoco será lo mismo si el terremoto, la inundación o la pandemia pasan donde tenemos el CPD o bien donde hay un centro de suscripción. El impacto es diferente, y las medidas a tomar también.

3.2 Fase de diseño de la solución

En esta fase se describe cual es la solución de recuperación más efectiva en cada caso. También se especifican los requisitos de RTO y RPO obtenidos en la fase de análisis, y de que medios se disponen para alcanzar dichos requisitos.

Se describirá para cada uno de los 4 entornos mencionados en el apartado anterior, con el objetivo de simplificar la explicación. En un caso real, dicho diseño se

debería extender sino a todos, a los elementos más críticos identificados en la fase de análisis.

A continuación, se describe el workflow que deberá seguir el plan, desde la fase de alerta, donde se decide si se dispara o no el plan, hasta la de disparo, en caso de que se haya decidido necesario en la fase anterior.

Por último, se especifican los equipos que participan en dicho plan, y las responsabilidades asignadas a cada equipo.

Por todo esto, este apartado se ha dividido en tres partes, a saber:

- Objetivos de la restauración
- Equipos implicados
- Workflow del plan de contingencias

3.2.1 Objetivos de la restauración

Este apartado hace referencia a los procesos y sistemas que se deben restaurar en caso de contingencia, resultado de la fase anterior de análisis.

Sistemas de Información y aplicaciones

Al principio del capítulo se destacaban una serie de consideraciones a tener en cuenta para simplificar el plan de contingencias, entre otras cosas. Una de ellas consistía en centralizar toda la informática en un solo punto o CPD. Este hecho por si solo hace que todos los sistemas de información y aplicaciones residan en un solo punto, haciendo mucho más efectivas todas las contramedidas de las que hablábamos anteriormente. Por ejemplo, no tenemos que instalar detectores de humedad en todos los edificios donde exista un servidor, sino solo uno donde residen todos los servidores, con el consecuente ahorro.

Como todo, tiene su contrapartida. El hecho de que esté todo en un mismo sitio, permite un solo punto de fallo, y por tanto que una sola amenaza afecte a todos los servicios. Aunque a priori parezca contraproducente, no tiene porqué serlo, pues es mucho más fácil administrar, restaurar y duplicar un solo punto que muchos dispersos por todo el territorio.

También la centralización permite tiempos de recuperación (RTO's) y perdidas de datos (RPO's) menores, ya que al estar la información centralizada, es mucho más fácil hacer copia de todo el conjunto, que tener que recoger las copias de diversos sitios para tratar de recuperarlos en uno solo.

Estrategia de respaldo

Una de las primeras cosas en que se piensa cuando se plantea un diseño de un plan de contingencias es: ¿Cómo se están protegiendo los datos?

Ya tenemos claro qué nos puede afectar (amenazas), e incluso hemos planteado qué podemos hacer para evitar que nos afecte (contramedidas), pero hagamos lo que hagamos, siempre tenemos que estar preparados para recuperar los datos en la misma ubicación o en otra, si la primera ha quedado inutilizable.

Es por esto que la estrategia de respaldo de la información debe ser nuestra prioridad número uno.

Estrategias de respaldo hay muchas, aunque las más utilizadas son las copias a cinta y las replicaciones de cabinas de discos (síncrona o asíncronamente).

La elección de un sistema u otro repercutirá directamente en los RTO's y RPO's fijados por la compañía, y hará que nos tengamos que decantar por uno, o bien por una combinación de ambos.

En el caso de las cintas, el proceso empieza con un volcado de los datos a copiar, normalmente hacia un robot de cintas. Una vez finalizado el proceso, se transportan dichas cintas al centro de recuperación, o bien a un centro de custodia fuera del centro donde residen los datos originales (figura 3). Este punto es importante, porque si se guardan los datos en el mismo sitio, la misma amenaza podría destruir los datos originales y las copias. En muchos casos, el volcado a cinta se hace por duplicado, para poder dejar una copia en el CPD y poder recuperar datos puntuales en caso de necesidad sin tener que traer la copia que se ha mandado fuera.

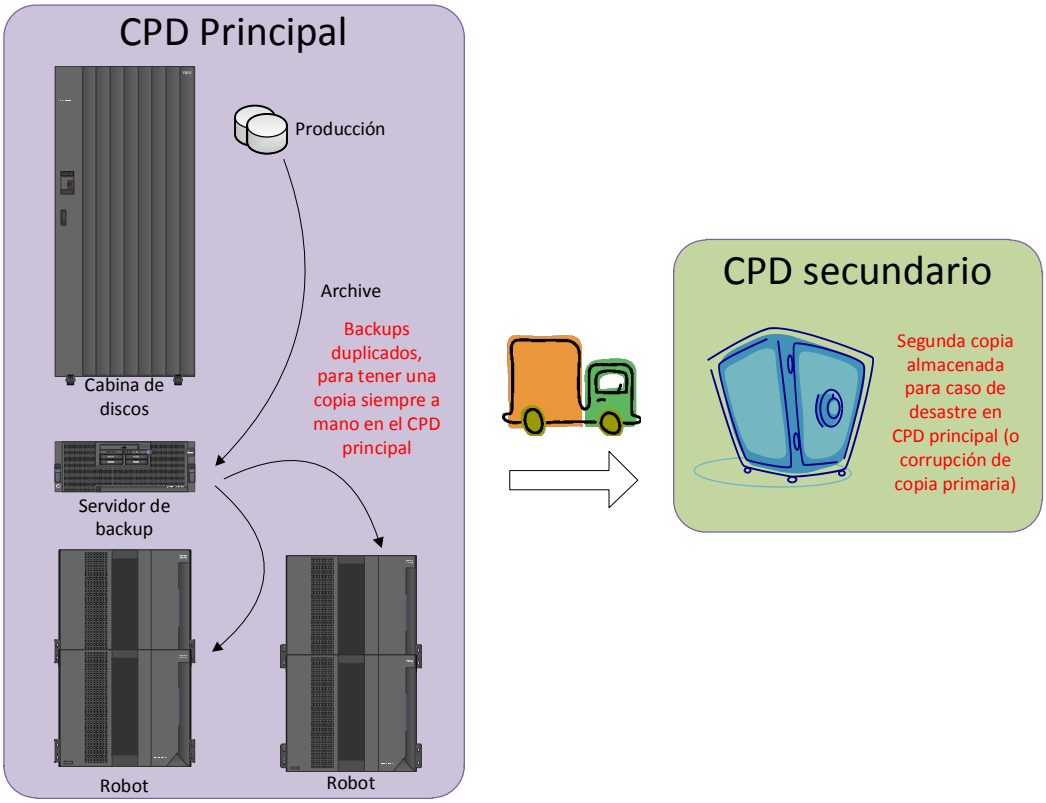


Figura 3

La copia de datos entre cabinas funciona a través de líneas de comunicaciones entre el CPD original y el de contingencia. Cada vez que se guarda un dato en la cabina original, este se copia automáticamente a la cabina en el centro de respaldo. En caso de continencia, o bien se puede invertir el proceso para restaurar la cabina original, o bien se pueden levantar los servicios en el centro de contingencia.

Independientemente de que haya una réplica entre cabinas, se tienen que sacar los datos a cinta igualmente (figura 4), porque este sistema no protege ante el borrado accidental de datos (cuando borráramos de la cabina principal, acto seguido se borraría de la secundaria, perdiendo dichos datos). Normalmente, aprovechando que se tienen los datos en ambos CPD's, se hacen las copias semanales (totales) en el centro de backup, y las diarias en el principal, ya que estas últimas son más necesarias para el día a día.

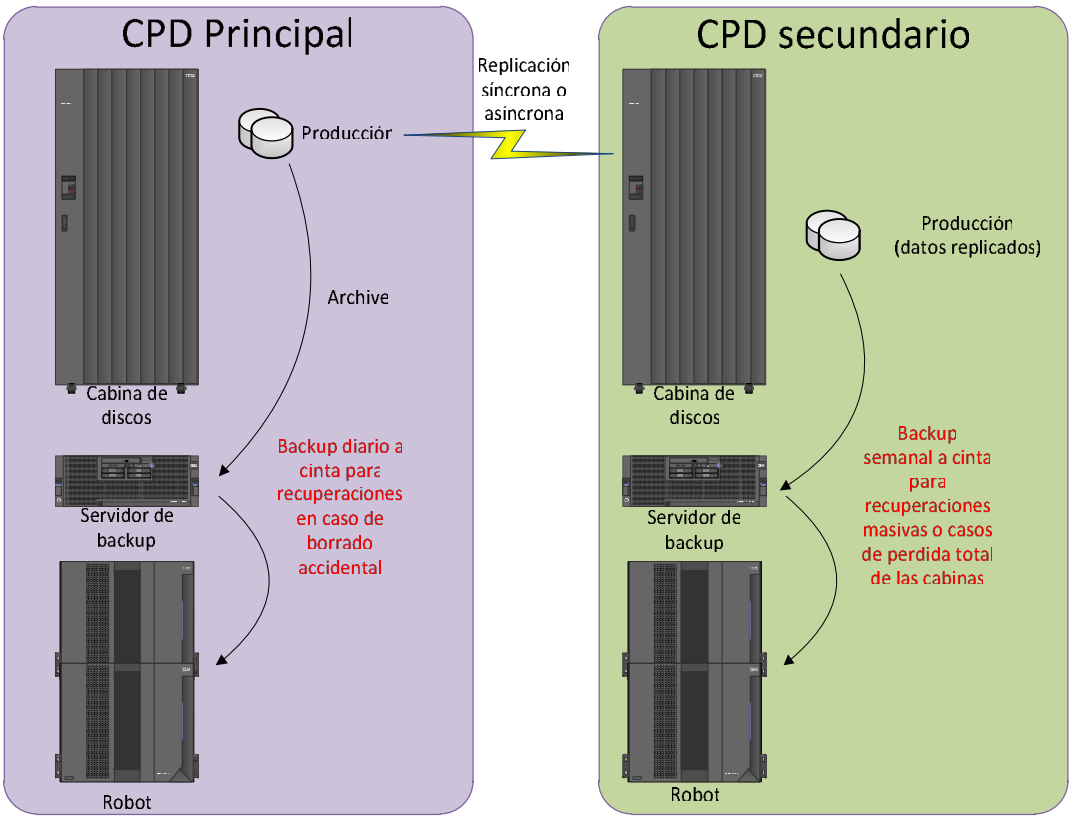


Figura 4

Tanto en un caso como en el otro, en el centro de respaldo deben existir las infraestructuras necesarias para restaurar los datos y luego poder dar servicio. Un ejemplo de los servicios que debería prestar el centro de contingencia es:

- Configuración de emergencia reservada suficiente para el proceso y tratamiento de la información, así como para el entorno de Comunicaciones (Voz y Datos) (con dimensionamiento y características de recursos actualizados periódicamente y/o en caso de cambios relevantes).

- Puestos de operación y administración de los sistemas; comunicaciones de voz y datos.
- Puestos de usuario con infraestructura de entorno de oficina; comunicaciones de voz y datos.
- Documentación de sistemas y productosusados en la recuperación
- Soporte técnico y operativo dedicado en escenario de desastre
- Coordinación de asistencia técnica y operativa.
- Hosting de servidores propiedad de la compañía o bien alquiler de servidores para dar servicio en caso de contingencia.
- Cabinas de almacenamiento de datos. Estas pueden ser de uso exclusivo de la compañía porque están conectadas a las que están en el CPD principal y se replican automáticamente, o bien de alquiler, si se decide utilizar el sistema de copia de cintas
- Robot de cintas, para poder restaurar de cinta en caso de pérdida de datos dentro de la cabina o bien para restaurar todo el entorno a partir de las copias a cinta.
- Electrónica de red

El CPD alternativo, debe ser un centro de servicios informáticos especializados, activo 24x7x365 y a una distancia suficiente de las oficinas principales. Esta distancia es fruto de dos circunstancias: No puede estar más cerca del CPD principal para no verse afectado por los mismos desastres a la vez (por ejemplo un terremoto). No puede estar más lejos porque a partir de ciertas distancias, las replicaciones de las cabinas entre los centros empiezan a perder efectividad por culpa de la latencia (tiempo que tardan los datos en ir de una cabina a la otra). Debe tener accesos disponibles por carretera y transporte público.

Tiempo objetivo de recuperación (RTO)

Aquí es donde se reflejan claramente las diferencias al optar por un sistema de respaldo u otro.

En la replicación por cabinas, normalmente se estima que el RTO correspondiente a los sistemas de información no supera las 6 horas. Esto es debido a que los datos ya están volcados en la cabina, y se evita el proceso de volcado desde cintas, que es lo que alarga más la puesta en marcha de un sistema de información. En este caso, el volumen de datos no afecta al RTO.

En caso que la restauración fuera debida a errores lógicos en la información, este tiempo puede sufrir variaciones en función de las copias disponibles, y de la cantidad de datos a restaurar.

En la restauración desde cintas, el RTO es muy variable, dependiendo sobretodo del volumen de datos a restaurar.

La única ventaja de este sistema es el precio, ya que la replicación por cabinas requiere de una fuerte inversión inicial (comprar el doble de cabinas de las que se necesitan) y un mantenimiento caro (las líneas a través de las cuales se replican dichas cabinas).

Pérdida de datos aceptable (RPO)

La utilización de la copia entre cabinas permite asumir una pérdida de datos como máximo correspondiente a los minutos inmediatamente anteriores al suceso que provoca la contingencia. Como los datos se están enviando cada pocos minutos al centro de respaldo, solo se perderán los datos que no se hayan podido enviar en el momento del desastre.

En caso que la restauración fuera debida a errores lógicos en la información, este tiempo puede sufrir variaciones en función de las copias disponibles, ya que como se ha comentado antes, se tendría que restaurar de cinta.

Si las copias son por cinta, los RPO's pueden variar mucho, pero no suelen bajar de las 24h. Hay que tener en cuenta que no se pueden sacar copias en cinta continuamente (entre otras cosas porque el sistema no daría abasto), y además hay que llevar físicamente dichas cintas al centro de contingencia o lugar de custodia. Esto imposibilita que en caso de desastre se puedan recuperar datos posteriores a la última copia a cinta disponible en el centro de respaldo (normalmente la del día anterior).

Sistemas de comunicaciones y telefonía

Estrategia de respaldo

Normalmente las líneas de comunicaciones están contratadas con un proveedor de servicios externo, que se encarga de gestionar y monitorizar dichas líneas. Es por esto que se debe establecer con dicho proveedor un contrato de prestación de servicio que ya contemple los supuestos de contingencia.

Aún y así, en el plan de contingencia de la compañía se debe hacer referencia a dicho contrato.

En el caso de la telefonía, si, como se ha comentado en un principio se ha optado por la telefonía IP, se deberá contar con las copias de seguridad correspondientes a los servidores ubicados en el CPD. Al ser todo software, la restauración se puede realizar en el centro de recuperación a partir de las cintas.

Si no se dispusiera de telefonía IP, se debería contratar una centralita con unas características similares, y tratar de volcar la configuración en esta, con las complicaciones técnicas y de presupuesto que esto comportaría (habría que tener una segunda centralita de características similares en el centro de respaldo, entre otras cosas).

Adicionalmente, y para los números públicos de la compañía (902 XX XX XX) se puede diseñar un plan que contemple su redirección tanto en caso de sobrecarga como de emergencia a una empresa de servicios. Este servicio podría ser dado por empresas de Contact Center, que suelen suplir a los Contact Center propios

de las compañías de seguros para dar servicio 24x7. En el capítulo 4 detallaremos más el plan de contingencia específico para este servicio.

Si los servicios de comunicaciones y telefonía no estuvieran subcontratados, se procedería igual que en el caso de los sistemas de información y aplicaciones.

A diferencia de los sistemas de información, en estos sistemas no hay datos de la compañía, por tanto no tiene sentido la replicación entre cabinas. Con una copia diaria o incluso semanal de todos los sistemas implicados debería ser suficiente.

Tiempo objetivo de recuperación (RTO)

En caso de interrupción de servicio el tiempo de recuperación del servicio dependería de la naturaleza de la contingencia sufrida, y en el peor de los casos sería la restauración de todos los servidores en el centro de recuperación. El RTO debería estar especificado en el contrato con la empresa proveedora del servicio.

En caso de no estar subcontratado, los RTO's dependerán del sistema de respaldo utilizado y de la infraestructura necesaria, tal y como se ha detallado en el apartado referente al RTO para sistemas de información y aplicaciones.

Pérdida de datos aceptable (RPO)

En el caso de las comunicaciones y la telefonía no suele haber pérdida de datos, ya que no hay información variable de la compañía. Los datos de las copias del día anterior no distaran mucho de los que había en el momento del desastre.

Puestos de trabajo

En este apartado solo tendremos en cuenta la restauración de los puestos de trabajo del departamento de IT. Como se comprenderá, estos requisitos no son tan grandes como serán los puestos de trabajo de toda la compañía, aunque en este último caso tampoco suele ser muy grande, dado que no todos los trabajadores de la compañía suelen estar ubicados en el mismo edificio.

Normalmente en el mismo centro de contingencias se dispone de una serie de puestos de trabajo para el personal de IT involucrado en la contingencia. La contratación de una serie de puestos de trabajo adicionales para ciertos perfiles de IT suele ser habitual, pero dado el reducido número de personal necesario, no suele ser problema ubicarlos en las mismas dependencias del centro de recuperación.

Estrategia de respaldo

Ya se ha comentado que el espacio disponible en el centro de recuperación debería ser suficiente para reubicar al personal de IT. Normalmente, se contrata también con el proveedor la disponibilidad de una serie workstations para poder no solo seguir el procedimiento de restauración, sino también dar servicio de IT al resto de departamentos.

Es recomendable disponer de copias de seguridad de algunas workstations clave, o bien por su especialización, o bien por ser un modelo apto para todos los perfiles. Estas copias deberían viajar junto con las copias del resto de sistemas.

Tiempo objetivo de recuperación (RTO)

El tiempo de recuperación oscilaría entre las 6h-12h, dependiendo del número de workstations a restaurar. Este tiempo no es el que se tardaría en restaurar las workstations necesarias para realizar la restauración de los sistemas de información, sino el que se necesita para que el departamento de IT como tal de servicio al resto de departamentos.

Pérdida de datos aceptable (RPO)

La estrategia corporativa de almacenamiento de datos requiere que los usuarios guarden toda su información en las unidades de red, que están sujetas al proceso de copias de seguridad. El cumplimiento de esta norma por parte de los usuarios hace que no exista pérdida significativa de datos.

A esto hay que sumar el hecho de que las aplicaciones y configuraciones de las workstations consideradas clave están copiadas en el centro de contingencia.

Instalaciones físicas

Dependiendo de dónde se hayan decidido restaurar los servicios en caso de contingencia, y de si esas instalaciones son propiedad de la compañía o bien alquiladas a un tercero para casos de contingencia, se deberá diseñar un plan de aviso y traslado a dicho centro u otro.

En el caso del alquiler, se suele contratar no solo las salas, sino también todos los equipos necesarios para la restauración del entorno, o un espacio donde ubicar los servidores de la compañía sin son propiedad de esta.

Además, dado que las instalaciones no son de la compañía, se deberá avisar a la empresa suministradora de la necesidad de ocupar dichas instalaciones, como se explicará en el siguiente apartado de la fase de diseño.

Si las instalaciones son propiedad de la compañía, estas deberán estar disponibles en todo momento, con todos los equipos revisados y a punto para funcionar. Esto hace que muchas compañías no utilicen esta solución, dado que tiene unos costes muy elevados.

Como en este apartado solo hacemos referencia a las instalaciones dedicadas a IT, normalmente con las salas donde se ubican los servidores es suficiente para que los técnicos puedan desarrollar su trabajo, haciendo innecesario otras salas específicas para ellos.

3.2.2 Equipos

En este apartado se definen los integrantes de los equipos que forman parte de una u otra forma del plan de contingencias de la organización, así como las funciones de dichos equipos.

Se da una idea de las funciones que desempeñarán dichos equipos, sus responsabilidades, así como cuál debería ser su composición desde el punto de vista de perfiles técnicos y de dirección.

Posteriormente se hará referencia a estos equipos en la fase de diseño del workflow del plan de contingencias.

Equipo director de continuidad de negocio

El equipo Director de Continuidad de Negocio suele estar formado por la misma jerarquía de la organización, partiendo del director de sistemas, y hacia arriba.

Un ejemplo podría ser:

- Director de sistemas
- Director de IT
- Director General

Una vez establecidos los componentes del equipo, suele disponerse de un listado de escalado de incidentes, empezando por el escalón más bajo de la jerarquía.

Así, en el ejemplo, cuando se diera un incidente grave, primero se intentaría localizar al director de sistemas. Si no fuera posible, se haría lo propio con el director de IT, y si no se encuentra ni a uno ni al otro, al director general.

Cada organización variará esta jerarquía según su estructura, pero es muy importante que esta quede reflejada en el plan de contingencia, así como los datos personales para contactar con ellos.

Las funciones típicas del equipo director de continuidad de negocio incluyen:

- Realizar evaluaciones de daños y de estado.
- Poner al resto de equipos en alerta.
- En su caso, avisar al centro de recuperación del inicio de la recuperación (preparación de equipos en centros de respaldo) por posible disparo del Plan (preparación de máquinas, comprobación de soportes e inicio de restauración).
- En su caso, disparar el Plan e informar al resto de Direcciones y áreas de la organización para la preparación de avisos y comunicados internos y externos (relaciones públicas y avisos al regulador).
- En su caso, desactivar la alerta (aviso al resto de equipos).
- Coordinar al resto de equipos (revisar la integridad de los equipos de emergencia y reasignar funciones si es necesario)

Responsables de operación y producción

Este equipo está formado por los operadores que trabajan diariamente en la monitorización de los sistemas.

Son los encargados de realizar las primeras evaluaciones cuando alguno de los sistemas monitorizados sufre algún percance.

En función del desastre deben realizar las siguientes funciones:

- Contactar con Seguridad Física para establecer daños y avisar a los servicios adecuados (Policía, Bomberos, SEM).
- Iniciar proceso de escalado y comunicación de incidentes graves (al equipo director del plan de contingencias).
- Establecer el estado de las instalaciones informáticas, los procesos y elementos de recuperación (Back-ups), además de verificar que los soportes han sido debidamente enviados.
- Establecer junto con el Equipo de logística y apoyo el centro de operaciones y reuniones

Equipo de Recuperación

El equipo de recuperación está formado por los técnicos y especialistas encargados de la restauración propiamente dicha.

Al igual que en el caso de los integrantes del equipo director, se debe disponer de una lista de personas exhaustiva, así como los datos personales de todos ellos para ponerse en contacto en caso de que el plan de contingencia sea disparado por el equipo director.

Esta lista debe obrar en poder del equipo director en todo momento.

Este equipo comparte las mismas funciones que el grupo de Responsables de Operación y Producción, y además es el responsable de, una vez disparado el Plan seguir los procedimientos de recuperación descritos en cada área de actuación.

Seguridad Física y PRL

Este equipo, aunque no directamente relacionado con el plan de continuidad de negocio de la organización, también debe ser mentado en dicho plan. Normalmente está compuesto por empleados escogidos por ubicaciones, y son los responsables de:

- Establecer y comunicar el estado de las infraestructuras físicas y accesos.
- Avisar a los servicios de emergencia.
- Coordinar acciones con servicios de emergencia (control de accesos y vigilancia, evacuación de personas).

Equipos de Logística y apoyo

Son los encargados de coordinar toda la logística en caso de contingencia. Según la organización, puede existir un departamento dedicado a la seguridad y la logística propiamente dicha, o bien una serie de personas designadas a tal efecto.

Las siguientes son algunas de sus responsabilidades:

- En coordinación con los Responsables de Operación y Producción, establecer el centro de operaciones y reuniones. Comunicar al resto de equipos la ubicación del centro de operaciones.
- Verificar y, en su caso, dotar al centro de reuniones de servicios de comunicaciones de emergencia.
- Dotar de comunicaciones de emergencia a los equipos (diferentes suministradores y/o medios)
- Centralizar la localización y comunicación de personas en caso de necesidad.
- Preparar credenciales y acreditaciones del equipo de recuperación.
- Habilitar medios de transporte de personas y materiales a los centros de recuperación (durante todas las fases).
- Disponer de avituallamiento (comida y bebida) para las primeras horas para los diferentes equipos.
- Disponer de zonas de descanso o alojamiento próximas a los centros (operaciones, desastre y recuperación).
- Poner fondos –o medios- a disposición del personal a desplazar.

3.2.3 Workflow del plan de contingencias

En este apartado se repasan los procedimientos a seguir en caso de contingencia. No solo hay que saber qué restaurar, cómo, y en qué plazo de tiempo, sino también qué procedimiento hay que seguir para decidir lanzar el plan de contingencias o no.

A diferencia de los apartados anteriores, estos workflows están bastante estandarizados, y más que diseñarlos, hay que implantarlos adecuadamente en cada organización. Es por esto que no se proponen métodos alternativos, sino que se explica en que consiste cada fase y como llevarla a cabo.

El workflow se divide en 2 fases:

- Fase de alerta
- Fase de disparo

A continuación se incluye una representación gráfica de las fases del plan de contingencia.

Fase de alerta

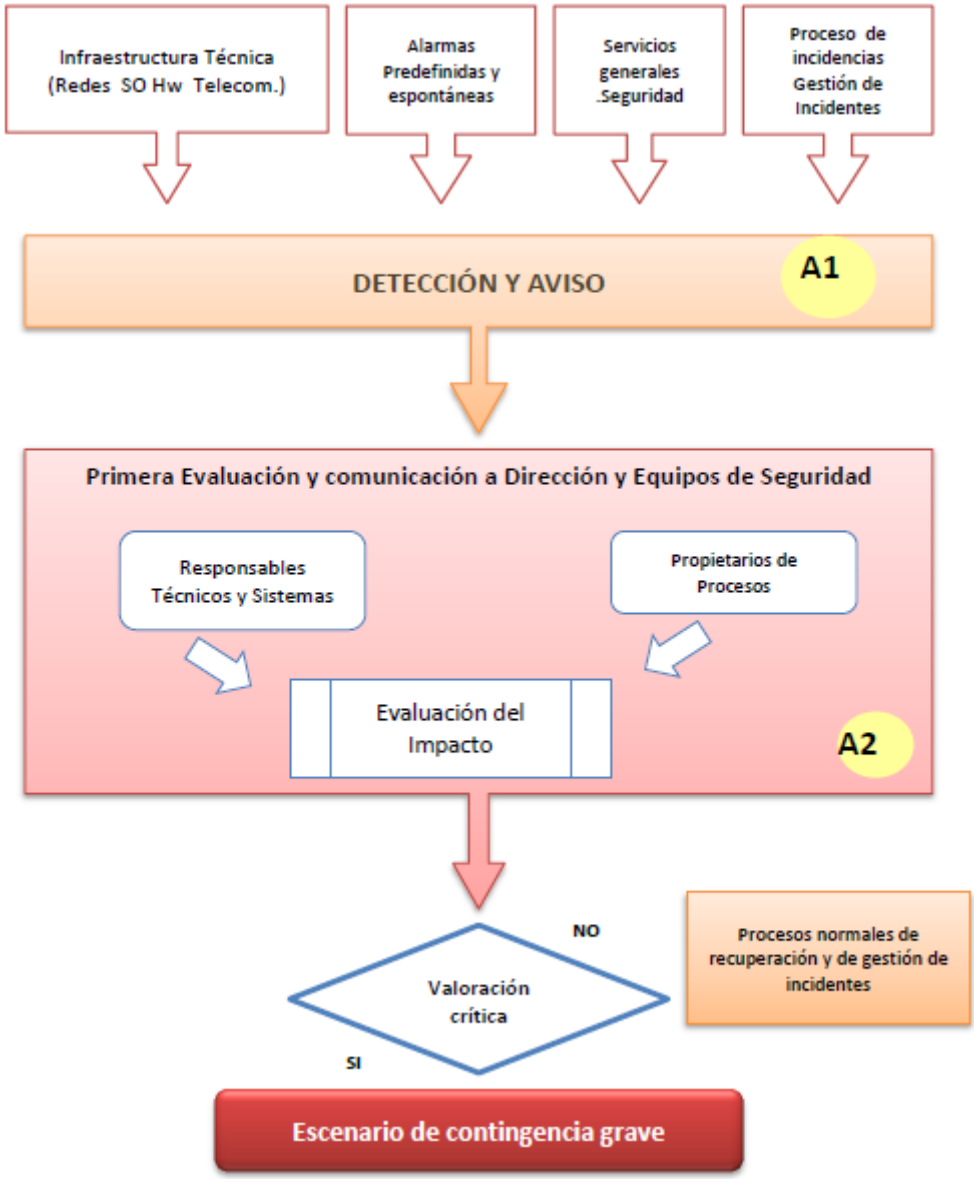


Figura 5

Tal y como se observa en la figura 3, existen dos acciones principales a realizar en la fase de alerta de un plan de contingencia:

- Detección y aviso (A1)
- Primera evaluación (A2)

Una vez realizadas estas dos acciones, y dependiendo del resultado, se pondrá en marcha el resto del plan, si se ha decidido que se está en un escenario de contingencia grave.

A1-Detección y aviso

Se genera por parte de los diferentes mecanismos de control existentes o por parte del personal implicado en los procesos u otros medios un aviso de la anomalía o falta de funcionamiento detectados.

La detección o anomalía puede deberse a muchos orígenes, de los cuales destacamos los más comunes:

- Infraestructuras físicas.
- Infraestructuras técnicas (incluye telecomunicaciones voz y datos redes, sistemas, HW, otros).
- Controles de seguridad física (detectores y otros sistemas).
- Alarmas predefinidas.
- Alarmas espontáneas del personal.
- Mantenimiento en general (Servicios y seguridad física).

A2- Primera evaluación

Una vez recibido el aviso, se efectúa una primera evaluación del evento y de su impacto en el/los procesos de negocio. Esta primera evaluación es realizada por:

- Usuarios.
- Propietarios de los procesos.
- Responsables técnicos de los procesos y Sistemas

Para ello se tendrán en cuenta:

- Tiempo previsto de duración del incidente (incluyendo la completa restauración del servicio).
- Elementos y Servicios afectados.
- Alcance del incidente.

Además de la propia experiencia aportada, deberán consultarse los esquemas de Procesos y servicios y Tiempos (Servicios afectados, tiempos aceptables de recuperación y tiempos totales de recuperación). Estos esquemas son los obtenidos en la fase de análisis, así como los tiempos de la fase de diseño (RTO y RPO).

En caso de que los tiempos previstos estuviesen dentro de los márgenes aceptados por la organización (Propietarios y Usuarios e Infraestructuras) con los procesos normales de recuperación y resolución de incidentes, se pasará a su resolución.

En caso de que el tiempo de recuperación de los procesos se desconociera o se previese excesivo, se procederá a comunicar la situación al Comité de Seguridad –Equipo de Continuidad de Negocio– aportando toda la información disponible en ese momento y se seguirá con el procedimiento especificado en la siguiente fase.

Fase de disparo

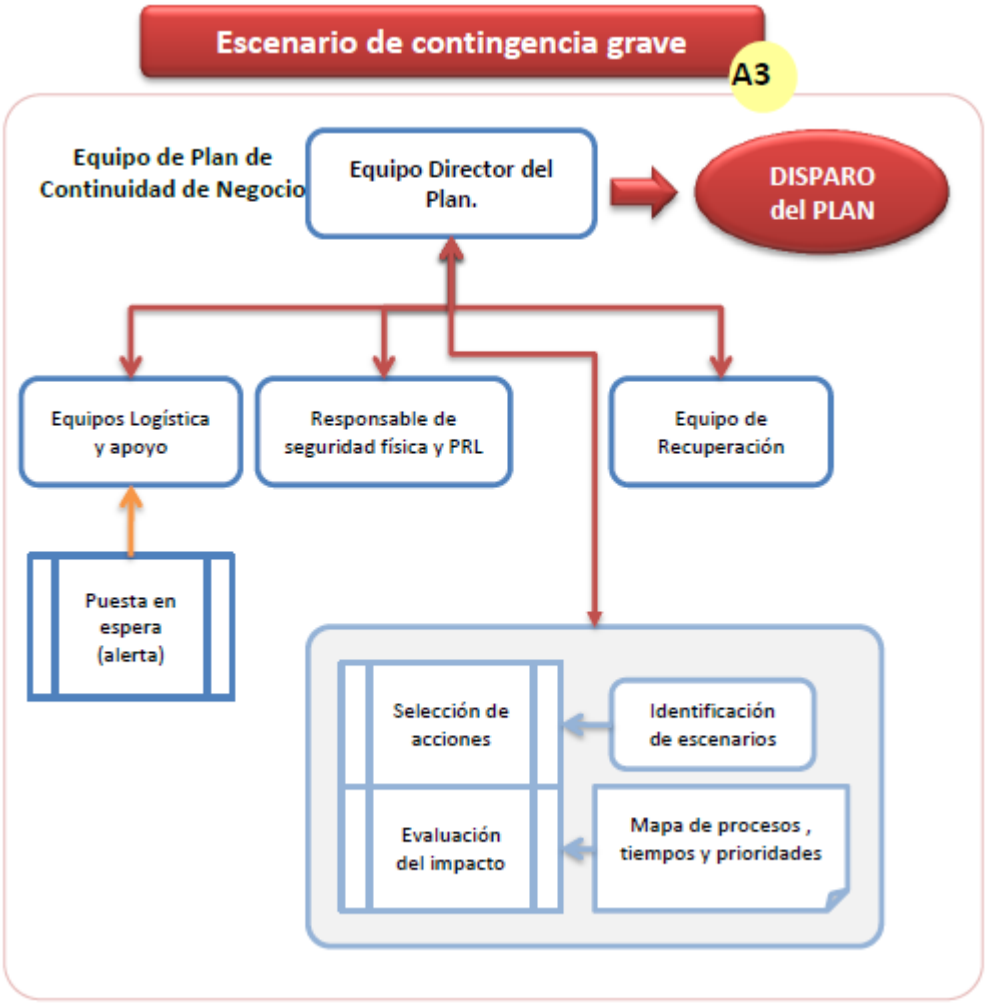


Figura 6

Una vez el equipo director del plan de contingencia recibe el encargo de disparar el plan, este empieza a evaluar el impacto, y a decidir qué acciones se deben llevar a cabo, de las descritas en el plan de continuidad.

A3- Evaluación del Impacto y Selección de acciones

El equipo Director del Plan analizará la información recogida y aportada en la fase previa, debiendo decidir en primer lugar si es completa y suficiente para determinar la gravedad del evento y seleccionar cualquier tipo de acción. En caso de no ser así deberá intentar completar la información.

Una vez analizada, se determinarán los posibles impactos tanto económicos como de imagen, tanto los ya ocurridos hasta el momento como los previstos, y una vez constatada la necesidad de activar el Plan, se procederá a su disparo elabo-

rando un resumen del proceso de decisión para ser usado como referencia en acciones posteriores.

Se informará a los componentes operativos del Comité de Seguridad de GCO

Se deberá analizar, dados los escenarios, la posibilidad de modificar las prioridades establecidas.

En todo caso, se deberá evaluar la necesidad de elaborar un informe para Secretaría y relaciones externas para que valoren la oportunidad de informar a reguladores u otros destinatarios que se estimen.

Una vez el equipo Director / Responsable del Plan haya decidido su disparo, se llevarán a cabo los siguientes procedimientos existentes,

- Notificación por parte de una persona autorizada a la empresa de servicios responsable del centro de contingencia de la entrada en contingencia de la empresa de acuerdo con el procedimiento.

- Puesta en marcha de los equipos de recuperación (Operación y sistemas), los cuales disponen de los procedimientos técnicos y operativos para la recuperación de todos los procesos en el centro alternativo. De estos procedimientos debe haber copia actualizada diaria en los centros de respaldo.

- Activación del equipo de apoyo y logística.

- Informar a seguridad del estado de contingencia para facilitar (controladamente) el movimiento de personas y materiales.

3.3 Implementación

Esta es la fase más fácil de explicar, y probablemente las más difícil de llevar a cabo. Se trata de implementar todas las medidas de prevención y de poner en práctica todas las decisiones tomadas en la fase de diseño.

Probablemente lo más complejo de todo sea llegar a tener un entorno que permita cumplir con los RTO’s y RPO’s requeridos por el negocio.

Al principio del capítulo se han expuesto una serie de medidas que ayudan en gran medida a mejorar la disponibilidad y eficacia de un plan de contingencias. Llegar a los niveles adecuados a los tiempos exigidos, puede significar años de cambios en el día a día.

Por ejemplo, virtualizar totalmente una infraestructura de una empresa de seguros, teniendo en cuenta la complejidad de los sistemas implicados, no es algo que se decida hacer y se ponga en práctica. Se empieza con algunos servicios no críticos, para comparar rendimientos (siempre son peores con la virtualización, aunque no importa, si son aceptables), para posteriormente empezar a migrar los de más importancia. Debido a esto, los efectos positivos de la virtualización en el

plan de contingencias no son apreciables hasta mucho después de haber empezado el proyecto de virtualizar, puesto que los primeros entornos virtualizados no son susceptibles de ser restaurados (precisamente porque no tienen una importancia relevante para el negocio).

El otro gran problema de la implantación son los costes. Cada vez se piden unos niveles de servicio más altos (SLA's), y a ciertos niveles, las inversiones en tecnología son muy elevados.

Otro ejemplo lo tenemos en las replicaciones de cabinas, o bien en su alternativa, las copias a cinta. La implantación de una replicación, requiere en la mayoría de casos doblar la inversión en storage de una compañía… y el resultado no es visible para esta, ya que no se da un mejor servicio, ni ninguna ventaja competitiva. A esto se le suma que esta tecnología no sustituye a las copias a cinta, por tanto no hay ningún ahorro asociado. Las copias a cinta son siempre necesarias, ya que son las únicas que protegen de un error lógico (por ejemplo un borrado accidental en la cabina principal, ya que automáticamente se borrarían los datos de la cabina de backup).

La implantación de un plan de contingencias, tiene la ventaja de destacar la necesidad de todas estas tecnologías para el negocio, que no son apreciables desde el punto de vista de la eficacia o la eficiencia.

3.4 Pruebas

Probablemente este sea el punto más importante en un plan de contingencias.

Tanto el análisis, como el diseño y la implantación, no sirven de nada si no se consigue restaurar lo deseado en el tiempo exigido. Es en este punto cuando todas las carencias tecnológicas y de organización salen a relucir.

Las pruebas se pueden hacer de varios niveles, desde una prueba puntual de la restauración de una aplicación, a una prueba total, restaurando todo el entorno, y trasladando a personal adecuado para comprobar su buen funcionamiento.

En este apartado, igual que en el resto del capítulo, solo se tiene en cuenta las pruebas desde el punto de vista de TI.

Es recomendable hacer dichas pruebas (las totales) una vez al año como mínimo, dado que la evolución de los entornos, y sus constantes cambios harían inútil el resultado de una prueba de 2 o más años atrás.

El objetivo final de estas pruebas es conseguir demostrar a la dirección de la organización que los RTO's y RPO's exigidos son alcanzados con las soluciones técnicas propuestas. Estas pruebas deben repetirse las veces necesarias hasta alcanzar dichas exigencias, o bien la organización debe asumir que con los recursos técnicos actuales no se es capaz de restaurar los entornos críticos en unos tiempos razonables.

3.5 Mantenimiento

Una vez analizado, diseñado, implementado y probado el plan, no se puede dejar de lado. Tal y como se ha comentado en la fase de pruebas, los entornos se modifican, las tecnologías cambian, y las personas también.

Se debe seguir un proceso de revisión periódico de toda la información detallada en el plan, para que en el momento en que sea necesaria, sea exacta, y no provoque situaciones de indecisión, sobre todo teniendo en cuenta que cuando se necesite dicha información se estará en una situación de crisis, y no habrá tiempo para pararse a pensar, sino para actual.

Se podría decir que la fase de mantenimiento en sí engloba las otras 4 fases, ya que se debe volver a hacer un análisis de la organización, comparándolo con el que se hizo en un principio por si ha habido cambios. Luego se debe diseñar una nueva solución que contemple dichos cambios, y se acople a los procedimientos ya establecidos. Finalmente hay que llevar a cabo dichos procedimientos (implantando las soluciones tecnológicas que se hayan decidido fruto del diseño) y probar de nuevo todo en conjunto.

4 El plan de contingencia en el resto de unidades de negocio

Una vez definido el plan de contingencias para el área de IT, pasaremos a detallar qué particularidades tienen el resto de áreas de una empresa de seguros.

En la mayoría de casos, gran parte del plan de contingencias de un área recae en el plan de contingencias del departamento de IT, ya que como hemos comentado al principio, sin los servicios informáticos la continuidad del negocio asegurador es inviable. Cuando esto ocurra, sencillamente se hará mención del hecho, y se remitirá al lector al capítulo que corresponda.

Como se ha podido observar a lo largo de la tesis, la continuidad de negocio en el sector asegurador se sustenta en 3 pilares principales:

- Infraestructura tecnológica
- Instalaciones físicas
- Personal.

El primer punto ha sido el objeto de estudio del capítulo 3, y los otros dos, se han mentado siempre en referencia al departamento de IT. En este capítulo se hará hincapié en los dos últimos.

Como no es objetivo de esta tesis detallar un plan para una empresa de seguros en concreto, se ha decidido tomar una serie de procesos de negocio como representativos, algunos por su importancia en cualquier empresa, otros por sus particularidades.

Así, a grandes rasgos, podríamos definir los siguientes procesos de negocio:

- Suscripción
- Siniestros
- Tesorería
- Área financiera
- Contact center
- Otros profesionales

No es ni mucho menos una lista exhaustiva de los departamentos que componen una empresa aseguradora, sea del tipo que sea, pero si son las áreas que, independientemente de la especialidad de la empresa, son imprescindibles para la continuidad del negocio.

Como se verá, faltan muchos otros departamentos comunes a cualquier empresa de seguros (control, RRHH, etc.), que se han obviado porque se considera que no son necesarios en un primer momento, en el cual hay que asegurar que el negocio pueda continuar (los que hemos considerado no críticos en la fase de BIA del

plan de contingencia de IT). Cualquier otro proceso que se haya considerado crítico en el BIA, debe ser tenido en cuenta aquí.

Por descontado, una vez restablecidos estos procesos principales, se ha de continuar con la restauración del resto de procesos de negocio, ya que la idea final es poder volver a la normalidad una vez superado el momento crítico.

Este capítulo está dividido en dos partes: La primera que será parecida al capítulo 3, en que se explicará que se debe hacer en cada una de las 5 fases para la creación del plan de contingencias, y la segunda servirá para ver las particularidades de cada proceso de negocio considerado crítico en el BIA (los que hemos mentado anteriormente), así como datos orientativos para un plan de continuidad teórico.

4.1 Fases del plan de contingencia

A continuación, pasaremos por cada una de las fases de creación del plan de contingencia, siguiendo el mismo guion empleado anteriormente para el departamento de IT. No se hará especial mención a ninguna de las áreas. El procedimiento es el mismo para todas. En el siguiente apartado, se describirán dichos departamentos, y se especificaran particularidades y ejemplos para cada uno de ellos.

En el apartado de anexos se incluye un cuestionario orientativo para obtener los datos necesarios de la fase de análisis.

4.1.1 Fase de análisis

Tal y como hemos hecho en la fase de análisis en el capítulo 3, deberemos analizar aquí que aspectos de estos departamentos son críticos y necesarios para el funcionamiento del negocio.

Descartado el problema de lidiar con los problemas tecnológicos, tema tratado ampliamente en el capítulo anterior, se deberá analizar qué perfiles humanos necesitamos en cada caso y donde los ubicaremos.

Será trabajo del departamento encargado de diseñar el plan de contingencias entrevistarse con los responsables de los departamentos considerados críticos, para establecer qué puestos se deben cubrir en caso de contingencia.

Tal y como se ha hecho con los elementos a restaurar en IT, se debe hacer un BIA, especificando la criticidad de cada perfil. Así, si se decide que la figura del tramitador es imprescindible, se deberá decidir qué número de estos se necesitan, y durante cuánto tiempo.

Esto último es importante, ya que no es lo mismo que la contingencia dure 12 horas, 1 día, 1 semana, 1 mes o más. El número de personas necesarias aumentará según vaya pasando el tiempo, llegando al total de componentes del depar-

tamento si la contingencia se alarga mucho en el tiempo (si no fuera así, querría decir que hay gente de más en el departamento).

Es por esto que se le pedirá al responsable del departamento una relación de perfiles, la cantidad y una escala de tiempo.

Una vez identificados los perfiles necesarios para que el departamento pueda continuar su actividad, se deberá recabar toda la información posible sobre el funcionamiento del departamento en sí, para identificar otras necesidades, a parte de las informáticas, que ya han sido tratadas anteriormente. Por ejemplo, podría ser necesario, en el caso de algunas estaciones de trabajo, escáneres especiales (normalmente se usan para indexar en la gestión documental de la empresa las nuevas pólizas en el caso de suscripción, y partes de siniestros en el caso del departamento de siniestros). Aunque es una necesidad informática, al ser dispositivos particulares de áreas concretas, y además no suelen estar centralizadas en los CPD's, es posible que no se hayan contemplado desde el análisis de IT. Aquí también podríamos incluir lectores de códigos de barras, impresoras especiales, fotocopiadoras, faxes, etc.

El siguiente paso en el análisis implicaría averiguar que amenazas pueden afectar a los elementos críticos. En IT, vimos que como amenazas tenemos inundaciones, terremotos, cortes en el suministro eléctrico, etc. En este caso, como hablamos de personas, también tendremos que fijarnos en elementos como las pandemias, las huelgas, etc.

No podemos olvidar que en la lista de amenazas habremos de incluir las que afecten a las instalaciones donde se encuentren dichos perfiles críticos.

Por último, se analizan los diferentes escenarios de impacto. Dependiendo de la distribución y estructura de la empresa, estos podrán diferir mucho, y tener impactos totalmente diferentes.

Si somos una empresa de seguros de internet, con todo nuestro personal centralizado en un solo punto, si hay un terremoto en dicho punto, no será lo mismo que si tenemos una red de sucursales y centros distribuidos por todo el país. Es mucho más difícil impactar gravemente la segunda que la primera, y las medidas en un caso y otro también serán diferentes. Mientras en la primera nos encontraremos que necesitamos un solo centro donde trasladar a nuestro personal, en el segundo quizá podamos redistribuir los usuarios afectados entre las sucursales y centros no impactados. En cada caso, una vez recabada la información de los responsables de los departamentos, se decidirá qué medidas son las más adecuadas.

4.1.2 Fase de diseño de la solución

Siguiendo el guión establecido, toca diseñar como se va a llevar a cabo la recuperación del negocio una vez sucedido el desastre. Especificaremos para cada caso el RTO y el RPO de restauración del servicio, teniendo en cuenta no solo que hay que localizar a las personas adecuadas, sino que también habrá que montar unas

instalaciones alternativas (o disponer de alguna que ya se tenga y acondicionarla) y transportar hasta allí a dichas personas.

Estrategia de respaldo

Como ya se ha comentado, dependiendo de la estructura organizativa de la empresa esta estrategia variará mucho. En todos los casos, se debe disponer de un emplazamiento alternativo claramente definido, así como de los contactos y métodos para poder trasladar al personal.

Además del lugar propiamente dicho, se necesitará trasladar a este sitio, si no está preparado de antemano, los elementos necesarios para que los empleados puedan trabajar. Así, debería haber PC's disponibles y configurados, una conexión con los servidores que sean necesarios para su trabajo, etc. y todas las particularidades identificadas en la fase de análisis.

Otro punto a tener en cuenta en esta fase es la duplicidad de puestos. En la fase de análisis se debe haber identificado los perfiles y "key-positions" existentes. En la fase de diseño, se debe especificar como vamos a tratar dichos puestos.

Por ejemplo, si tenemos un especialista en suscripción de prestaciones de vida, se debe buscar la manera de transmitir la información de dicha persona a otras, o bien documentar sus conocimientos, para que, en caso de desastre, su tarea pueda ser desempeñada por otro. Es el equivalente a las copias de seguridad en IT. Sin ellas, el resto no tiene sentido. Si nos preocupamos por restaurar todos los datos, puesto de trabajo, etc., y luego resulta que la persona que debe hacer el trabajo no tiene los conocimientos, el resto no sirve para nada.

Tiempo objetivo de recuperación (RTO)

Dependerá de muchas cosas, pero si la afectación a la empresa ha sido total (ha caído el CPD, por ejemplo), este tiempo no tendría sentido que fuera inferior al especificado en el apartado de IT, ya que por mucho que los empleados estén listos para trabajar, si no hay infraestructura informática, poco pueden hacer.

Aún y así, disponer de las instalaciones adecuadas y trasladar el personal y los equipos a estas no debería superar normalmente las 48h, si está todo correctamente diseñado.

Perdida aceptable de datos (RPO)

Hoy día todos los datos suelen guardarse en los servidores, y la mayoría de compañías son bastante exigentes al respecto, ya que los datos que maneja una aseguradora pueden ser considerados de nivel alto por la LOPD, y por tanto no pueden ser almacenados en las workstations de los usuarios. Es por esto que no debería haber pérdida de datos en caso de caída de un centro o sucursal. La única pérdida de datos real se debería producir solo en el caso de que se vieran afectados los servidores, y esto ya lo hemos abordado en el capítulo anterior.

Tanto los equipos de personas que llevan a cabo el plan de contingencias como el workflow que sigue dicho plan ya han sido definidos en el capítulo 3. Solo queda añadir que dichos equipos son los responsables, tal y como se ha explicado, de ponerse en contacto con los usuarios necesarios, y facilitarles todo lo que necesiten para que puedan volver a desempeñar su función.

Equipos y Workflow

Ya se ha descrito en el capítulo anterior todo el workflow que debe seguir al disparo del plan de contingencias, y los equipos que deben participar y que funciones deben desarrollar.

En ese apartado se obvió deliberadamente la definición de un equipo, ya que no pertenecía en ningún caso a la estructura de IT.

El equipo referido es el que podríamos llamar “Equipo de relaciones públicas”, o de comunicaciones.

Este equipo debe ser el encargado de informar al resto de la organización, proveedores, profesionales afines y clientes del estado de la situación.

Todo el trabajo de restauración realizado por el resto de equipos de poco servirá si los agentes no saben que se está restaurando, y por tanto no continúan con su labor, o si los clientes creen que la empresa no podrá responder a sus necesidades, o si los empleados de los centros y sucursales están convencidos que no podrán trabajar porque ha caído un meteorito en la sede central.

La labor de este equipo es la de estar informado de los progresos del resto de equipos, y de transmitir estos progresos y estimaciones a las personas que puedan necesitar dicha información.

Uno de los canales más habituales para realizar las comunicaciones, dado que suele ser el punto de entrada de las peticiones de información es el Contact Center. El equipo de comunicaciones debe tener siempre actualizada la información en el Contact Center para que la gente que llama sepa a qué atenerse. Obviamente los canales de información habituales también deben ser utilizados, en caso necesario (prensa, radio, TV, redes sociales, etc.). El daño que puede ocasionar la falta de información sobre lo que se está haciendo para restablecer la situación puede ser peor que el incidente en sí.

4.1.3 Fase de implementación

No difiere en nada a lo explicado en el capítulo 3. Se trata de poner los medios necesarios para tener todo preparado en caso de contingencia. Esto incluye la compra de ordenadores para tener stock en caso necesario, el alquiler de salas en caso necesario, etc.

Matizar qué, como volvemos a hablar de personas, también se tendrá que tener en cuenta como trasladarlas en caso necesario, y poner los medios para ello (con-

tratos con medios de transporte, o definición de qué transporte público se debe utilizar para llegar a las instalaciones de contingencia en caso necesario).

4.1.4 Fase de pruebas

Igual que se hace con la restauración periódica de los servidores, se debe hacer un simulacro de contingencia cada cierto tiempo para detectar posibles errores en la implantación o el diseño.

Es importante implicar a todos los empleados afectados por dicho plan, para que estén informados de qué se espera de ellos, y estén preparados en caso necesario.

En esta fase se deberían probar, junto con las pruebas informáticas que ya se comentaron anteriormente, todas las particularidades del departamento que se han detallado en la fase de análisis: Traslados al centro de contingencia, desvío de llamadas a la nueva ubicación, funcionamiento de los puestos de trabajo (pruebas de aplicativos, etc.), hardware específico (escáneres, faxes, etc.).

4.1.5 Fase de mantenimiento

Esta fase se superpone en muchos casos con la de prueba, dado que el objetivo es el mismo: Asegurarse que el plan de contingencias sigue siendo válido con el paso del tiempo.

Hay que tener en cuenta que la empresa cambia con el tiempo, y sobre todo las personas. Hemos analizado en la primera fase qué perfiles necesitamos, pero si llegado el momento somos incapaces de dar con ellos porque los que hacían dicho trabajo cuando se hizo el análisis ahora desempeñan otras labores, de poco nos va a servir la lista de perfiles.

En esta fase se debería incluir el mantenimiento de los contratos de los sitios si fuera el caso, y del alquiler o compra de las workstations necesarias en cada momento.

4.2 Departamentos

Trataremos a continuación las áreas mencionadas al principio del capítulo:

- Suscripción
- Siniestros
- Tesorería
- Área financiera
- Contact center
- Otros profesionales

En cada uno de los departamentos, aparte de explicar el porqué de sus necesidades de restauración, también se expondrá una taula a modo de ejemplo. En nin-

gún caso trata esto de ser una guía sobre los tiempos y personas necesarias en caso de contingencia en estos departamentos. La idea es poder ver las diferencias en la inmediatez o no, y las consecuencias del paso del tiempo cuando se está en precario.

Es precisamente trabajo del equipo de análisis y diseño del plan de contingencia de cada empresa obtener información de todos los departamentos implicados para poder hacer unas estimaciones de tiempo y personal lo más precisas posibles.

Como se verá, en todos los ejemplos se tienen en cuenta dos valores: Tiempo de duración de la contingencia y personal necesario según este tiempo.

Para cada departamento, tanto un valor como otro variará, y ni siquiera las escalas de tiempo tienen porqué coincidir. Un departamento, por su necesidad de inmediatez, tendrá una escala donde según pasan las horas vayan variando sus necesidades de recurso, mientras otro podría pasar días con un mínimo de personal sin afectar mucho al negocio.

El otro parámetro medido, el del personal, también puede variar mucho, e incluso se puede dar el caso que, según pasa el tiempo, los perfiles necesarios vayan cambiando, y hasta se pueda necesitar la externalización temporal del servicio en casos de contingencias muy largas. Por ejemplo, se podría dar el caso que en un primer momento de la contingencia, se necesiten suscriptores para atender las peticiones de póliza nuevas y tratar las que ya estén en curso, pero cuando empieza a pasar el tiempo, quizá se necesite incorporar no solo suscriptores, sino también técnicos para evaluar grandes riesgos, etc.

4.2.1 Suscripción

En estos procesos se engloban muchas de las actividades del negocio asegurador propiamente dicho. Trataremos aquí tanto la suscripción de vida como la de no vida, señalando las diferentes casuísticas que afectan a cada departamento.

El ejemplo siguiente podría aplicarse al departamento de suscripción de vida:

Duración de la contingencia	Personal necesario	
12 horas	2 suscriptores	Personas mínimas que necesita el departamento para funcionar. Solo se atienden las tareas urgentes.
1 día	2 suscriptores	
2 días	2 suscriptores	
1 semana	3 suscriptores	El volumen acumulado empieza a crecer, y se hace necesaria otra persona para evitar retrasos que puedan afectar al cliente.

2 semanas	El equipo completo	A partir de aquí no solo se necesitará todo el departamento, sino que es posible que se necesite personal extra (o horas extras) para recuperar todo el trabajo no realizado en la primera semana.
1 mes o más	El equipo completo + personal adicional temporal	

Este ejemplo sobre el departamento de suscripción de vida, sería muy diferente al de suscripción de autos. Suscripción autos es un departamento que no podría permitirse el lujo de funcionar a medio gas durante una semana, ya que el cliente, cuando pide una póliza de autos, normalmente la quiere para ya (es probable que esté en el concesionario esperando tenerla para estrenar el coche), y si no se le atiende, se irá a otra compañía. El departamento de vida en cambio, puede postergar una suscripción, pues no suele ser una necesidad urgente. Un ejemplo de la misma escala para el departamento de autos podría ser el que sigue:

Duración de la contingencia	Personal necesario	
12 horas	2 suscriptores	Personas mínimas que necesita el departamento para funcionar. Solo se atienden las tareas urgentes.
1 día	3 suscriptores	En este departamento, no estar al día significa perder muchas pólizas, y por tanto la necesidad de personal aumenta exponencialmente con el paso de tiempo.
2 días	5 suscriptores	
1 semana o más	El equipo completo + personal adicional temporal	A partir de aquí no solo se necesitará todo el departamento, sino que es posible que se necesite personal extra (o horas extras) para recuperar todo el trabajo no realizado en los dos días anteriores.

4.2.2 Siniestros

En este departamento tendríamos algo parecido al departamento de suscripción autos. No se pueden aceptar retrasos en la tramitación de los siniestros, ya que la imagen de la compañía se vería seriamente afectada. Una compañía de seguros existe para el momento en que el cliente tiene un problema, y si no se responde de inmediato, pierde toda credibilidad. Una escala para este departamento podría ser:

Duración de la contingencia	Personal necesario	
8 horas	2 tramitadores	Personas mínimas que necesita el departamento para funcionar. Solo se atienden las tareas urgentes.
12 horas	3 tramitadores	En este departamento, no estar al día significa no existir para el cliente cuando este lo necesita, y por tanto la necesidad de personal aumenta exponencialmente con el paso de tiempo.
1 día	5 tramitadores	
2 o más días	El equipo completo + personal adicional temporal	A partir de aquí no solo se necesitará todo el departamento, sino que es posible que se necesite personal extra (o horas extras) para recuperar todo el trabajo no realizado en los dos días anteriores.

4.2.3 Tesorería

Este departamento, según la empresa, puede estar totalmente centralizado, o bien desglosado en dos: La parte de pagos y cobros en los departamentos de siniestros y suscripción, y la parte de contabilidad propiamente dicha centralizada.

Si este fuera el caso, lo que se expone a continuación solo afectaría a la parte de contabilidad, ya que son los datos que posee este departamento lo que necesita el área de finanzas para trabajar.

Aquí pasa algo parecido al departamento de suscripción vida. Nadie va a dejar de cobrar si se retrasan algunas horas algunos pagos, pero no se puede dejar "ineternum" sin pagarlas, dado que las repercusiones económicas para la empresa podrían ser muy negativas.

Dicho esto, podría parecer que el tiempo de criticidad no tenga que ser tan elevado como el del Contact Center o el de suscripción auto, pero hay que tener en cuenta que hay otro departamento crítico que depende de este para realizar su trabajo: el área financiera.

Este es el típico caso de dependencias cruzadas entre departamentos, y debería ser detectado en la fase de análisis, durante las entrevistas realizadas a los responsables de departamento (ver anexos).

Decimos que hay una dependencia porque el área financiera, sin los datos que recibe de tesorería, no puede saber que puede y que no puede invertir, etc. Puesto que como se explicará en el siguiente apartado, el departamento financiero tiene un tiempo de criticidad alto, el departamento de tesorería también ha de tenerlo.

Una posible estimación de tiempo podría ser la siguiente:

Duración de la contingencia	Personal necesario	
12 horas	2 administrativos	Personas mínimas que necesita el departamento para funcionar. Solo se atienden las tareas urgentes.
1 día	2 administrativos	
2 días	2 administrativos	
1 semana	2administrativos	El volumen acumulado empieza a crecer, y se hace necesaria otra persona para evitar retrasos que puedan afectar al cliente o las inversiones propias.
2 semanas	3 administrativos	A partir de aquí no solo se necesitará todo el departamento, sino que es posible que se necesite personal extra (o horas extras) para recuperar todo el trabajo no realizado en la primera semana.
1 mes o más	El equipo completo + personal adicional temporal	

Como se verá más adelante, coincide en las escalas de tiempo con el del área financiera, no porque este departamento lo necesite, sino porque el área financiera depende del el para funcionar.

4.2.4 Área financiera

Este departamento tiene la particularidad de necesitar información interna (ver punto anterior) y externa en tiempo real para tomar muchas de las decisiones.

Al igual que suscripción autos, se necesita una respuesta casi inmediata una vez acaecido el incidente, dado que los mercados no dejan de fluctuar, y no atender las inversiones en un periodo de tiempo muy largo sería muy perjudicial para la empresa.

Se estima unos tiempos parecidos al departamento de suscripción de autos, pero por motivos diferentes, como ya se ha explicado.

Duración de la contingencia	Personal necesario	
12 horas	2 técnicos	Personas mínimas que necesita el departamento para funcionar. Solo se atienden las tareas urgentes.
1 día	2 técnicos	
2 días	2 técnicos	
1 semana	3 técnicos	El volumen acumulado empieza a crecer, y se hace necesaria otra persona para evitar retrasos que puedan afectar al cliente o las inversiones propias.
2 semanas	El equipo completo	A partir de aquí no solo se necesitará todo el departamento, sino que es posible que se necesite personal extra (o horas extras) para recuperar todo el trabajo no realizado en la primera semana.
1 mes o más	El equipo completo. Posible necesidad de contratar a un broker externo	

4.2.5 Contact Center

La principal diferencia entre este proceso de negocio y el resto es la necesidad de inmediatez. Como ya se ha comentado, el Contact Center de una empresa de seguros es su imagen, y el hecho de que un cliente se intente poner en contacto con la empresa en la cual ha confiado para cuando tiene problema y no sea atendido, es lo peor que le puede pasar a la empresa.

Por esto, la mayoría de Contact Centers suelen tener planes de contingencia especiales, y que son lanzados con mucha más frecuencia que los planes de contingencia globales de la empresa (es mucho más común quedarse sin líneas telefónicas, por ejemplo, que qué se incendie un CPD).

Como para un Contact Center quedarse sin comunicaciones con el exterior es como quedarse sin nada, entrar en contingencia es una práctica relativamente común, y normalmente está muy probado (con casos reales, en este caso).

La gran ventaja de la recuperación del servicio del Contact Center es que normalmente las funciones que realiza el personal están muy pautadas, debido a la gran rotación existente en el sector. Esto facilita enormemente la formación de nuevo personal en caso necesario, y la subcontratación de empresas de servicio que atiendan las peticiones en casos de contingencia. Es por esto que más que escoger qué perfiles son necesarios, necesitamos tener muy procedimentadas las respuestas a dar a los clientes, y que estos procedimientos se encuentren en poder de la empresa o empresas que nos den el servicio en caso de contingencia.

Por descontado, el funcionamiento en caso de contingencia solo puede ser temporal, y en caso de una contingencia de más duración en el tiempo, se debe tener un plan de recuperación integral, que se incluirá en el plan general de la compañía.

El gran punto débil del departamento de Contact Center son las centralitas telefónicas, y las líneas de comunicaciones. Ambos elementos ya han sido tenidos en cuenta en el capítulo dedicado a IT, por tanto no hace falta repetir qué partes son críticas y qué partes no.

Otra gran ventaja es la facilidad que hay hoy en día para desviar las comunicaciones entrantes a cualquier otra parte, facilitando enormemente la atención telefónica alternativa sin tener que hacer montajes técnicos de última hora.

A continuación, se expone un posible cuadro de tiempos de respuesta de este tipo de departamentos:

Duración de la contingencia	Personal necesario	
1 hora	Desvío de llamadas a call center alternativo.	Aunque dicho call center puede no tener acceso a los datos de clientes, recogen las llamadas para luego ser procesadas una vez restablecido el sistema.
4 horas	5 operadores	En este departamento, no estar al día significa no existir para el cliente cuando este lo necesita,
1 día	El equipo completo	

		y por tanto la necesidad de personal aumenta exponencialmente con el paso de tiempo.
2 o más días	El equipo completo	Llegados a este punto, se debe haber restablecido el servicio en el call center principal, o bien haber transferido todos los roles y funciones al secundario, dado que no pueden seguir trabajando en precario por más tiempo (intervención de IT).

Como se podrá observar, las duraciones de contingencia son mucho más cortas que el resto de los departamentos.

4.2.6 Otros profesionales

En este apartadose incluirán las figuras de los profesionales afines a una compañía de seguros, como podrían ser:

- Peritos
- Abogados
- Médicos
- Mediadores
- Talleres
- Etc.

Debido al gran número de profesionales, diversidad y distribución geográfica, no se suele especificar en el plan de contingencias de la empresa como recuperarse ante la pérdida de profesionales en casos de contingencia. No obstante, lo que sí debería hacerse, es especificar en los planes de continuidad como se piensa seguir dando servicio a todos ellos.

Si en algunos casos la operativa del día a día de estos profesionales se viera afectado por una contingencia, el plan debe especificar como informar a los afectados, o qué medidas tomar para que la afectación sea subsanada o minimizada.

5 Conclusiones

Como se ha visto a lo largo de todo el estudio, un plan de contingencias es imprescindible. La continuidad de la empresa depende de ello, y no hace falta decir, teniendo en cuenta el sector en el que trabajamos, que no se puede estar seguro de nada en un mundo cada vez más complejo y cambiante. Es por esto que hay que estar preparados para las eventualidades, sean del tipo que sean.

Implantar un plan de contingencia en cualquier empresa no es fácil. No solo por la complejidad técnica, sino por el hecho de que hay que implicar a todos y cada uno de los departamentos que conforman la organización. Es vital para la empresa que cada departamento tenga claro que hacer cuando se produce una catástrofe, y por tanto que esté todo procedimentado y estipulado de manera que no se tengan que tomar decisiones precipitadas en situaciones en las que todos están bajo presión.

Para no mezclar conceptos, esta tesis está claramente dividida en 2, pero en ningún caso se quiere dar a entender que se deben hacer dos planes de contingencia por separado. El plan de contingencia ha de ser único, y ha de englobar a todos los elementos necesarios para seguir desarrollando la actividad después del incidente. Es muy importante que la coordinación entre los diferentes departamentos implicados en la restauración sea total.

Por todo esto, concluimos asegurando que una empresa con un plan de contingencias adecuado y actualizado, es una empresa que tiene asegurada su continuidad más allá de cualquier imprevisto.

6 Bibliografía

Barquero Cabrero, José Daniel (2001): Manual de banca, finanzas y seguros. Ediciones Gestión 2000 S.A.

Gaspar Martinez, Juan (2006): El plan de continuidad de negocio. Guía práctica para su elaboración. Ediciones Díaz de Santos.

Kamath, John-Paul (2007): Disasterplanning and businesscontinuityafter 9/11 http://www.computerweekly.com/Articles/2007/09/07/226632/Disaster-planning-and-business-continuity-after-911.htm

BIT (2002): Seguridad en los datos, una necesidad globalizadora. http://www.coit.es/publicac/publbit/bit135/cafe.pdf

WillianToigo, Jon (2003):*Disaster Recovery Planning: Preparing for the Unthinkable*.Prentice Hall PTR.

Maiwald, Eric (2002):Security Planning and Disaster Recovery. McGraw-Hill

JeetSandhu, Roopendra (2002):Disaster Recovery Planning**.**Premier Press.

Wikipedia: Business continuity planning. http://en.wikipedia.org/wiki/Business_continuity_planning

Wikipedia: Impact Analysis (Business Impact Analysis, BIA) http://en.wikipedia.org/wiki/Business_continuity_planning#Impact_analysis_.28Business_Impact_Analysis.2C_BIA.29

Wikipedia: Recovery time objective http://en.wikipedia.org/wiki/Recovery_time_objective

Wikipedia: Recovery point objective http://en.wikipedia.org/wiki/Recovery_point_objective

Eddie (2009): Introducción al tema de la virtualización http://www.consultaunitpro.com/tag/definicion-de-virtualizacion

Wikipedia: Service Level Agreement http://es.wikipedia.org/wiki/Acuerdo_de_nivel_de_servicio

Wikipedia: El sincronismo de datos http://es.wikipedia.org/wiki/Centro_de_respaldo#El_sincronismo_de_datos

7 Anexos

7.1 Plantilla recogida de datos

FECHA REUNIÓN:
LUGAR:
ASISTENTES:

IDENTIFICACIÓN DE PROCESO DE NEGOCIO Y RESPONSABLE	
Compañía:	
Dirección/Área:	
Proceso:	
Responsable de Negocio:	
Responsable en SISTEMAS:	

PERFIL BIA		
	Actual	**Consideraciones, cambios, otros.**
CRITICIDAD:		
Tiempo Máximo sin servicio (RTO y / RPO)		

DATOS de ÁREAS USUARIAS y/o PROPIETARIAS	
Identificación Áreas usuarias y Personas o Funciones Responsables	
Procesos de negocio no identificados previamente en el mapa general (Principales o auxiliares) Con estimaciones de RTO y RPO	
Dependencia funcional directa de otras Áreas. (detectar también si es una dependencia crítica, aunque sea de servicios generales)	
Procedimientos actuales de Trabajo en contingencia (identificar e indicar)	

Procedimientos alternativos de trabajo – fuera del alcance del BRS actual o en caso de que el BRS no cubra las funciones y/o necesidades-. Pueden ser manuales o semi - manuales.	
Tiempo máximo de funcionamiento del proceso o unidad usuaria con procedimientos alternativos	

REQUERIMIENTOS DEL PROCESO EN CONTINGENCIA	
Puestos de Trabajo necesarios en contingencia	
Perfiles de personas	
Detección de Key-Positions (conocimiento del proceso solamente en poder de una persona)	
Espacio Físico (locales, puestos de trabajo, servicios auxiliares - alimentación, sanidad, higiene, descanso-.	
Infraestructura Técnica Específica (incluyendo UPS, Telefonía fija y Móvil, Comunicaciones, Fax etc., copiadoras, impresoras, otros)	
Procedimientos informáticos específicos de emergencia para trabajar on-line u off-line según escenario de contingencia.	
Documentación off-line (papel o similar). *Tablas, tarifas, procedimientos operativos y auxiliares de trabajo, Algoritmos, procedimientos de comunicación y escalado de incidentes, otros.*	
Acreditaciones y autorizaciones de entrada y salida de personas, documentación, pre-impresos, documentos pre-firmados, Material Informático, otros.	
Formación previa en contingencia *(acciones y procedimientos no habituales en caso de contingencia y/o emergencia)*	
Procedimientos de vuelta a la normalidad específicos del Pro-	

ceso tanto logísticos – transporte de documentación, material y personas- como técnicos y de negocio (incluyendo autorización, verificación, consolidación y carga de información tratada o creada en contingencia). Incluyendo rutinas específicas de la aplicación en caso de contingencia o similar.	

TAREAS GENERALES (No específicas) A TENER EN CUENTA ESPECIALMENTE PARA ESTE PROCESO

Logística de personas, soportes, recursos monetarios y materiales	
Recuperación de Datos y Aplicaciones	
Seguridad Física	
Preparación de un entorno de HW y SW	
Decisión de Acciones	

8 Currículum: Sergi Casas i del Alcázar

FORMACIÓN ACADÉMICA

- Ingeniería Técnica en Informática de Sistemas, UOC (UniversitatOberta de Catalunya)

FORMACIÓN PROFESIONAL

- Curso programación COBOL y RPG en AS/400
- Microsoft CertifiedSystemsEngineer
- Cisco Certified Network Associate
- Curso VMwareInfraestructure 3
- Curso de dirección de equipos de trabajo

EXPERIENCIA PROFESIONAL

Responsable departamento Redes y Aplicaciones, Seguros Catalana Occidente 1/1/2005 — Actualidad

SantCugat del Vallés

- Dirijo un equipo de 8 personas.
- El principal objetivo del departamento es mantener toda la infraestructura de servidores, redes y comunicaciones del grupo Catalana Occidente.
- Regularmente se realizan proyectos con empresas de servicios que se coordinan y dirigen desde este departamento.

Técnico de sistemas, Seguros Catalana Occidente 1/6/2001 — 31/12/2004

SantCugat del Vallés

- Administración del entorno Windows i VMware de la compañía (unos 300 servidores virtuales).
- Administración de la infraestructura de red, así como de las comunicaciones (routers, switch, líneas).
- Investigación e implantación de nuevas tecnologías.

Programador, S2 Solucions i ServeisInformàtics 1/11/2000 — 31/5/2001

SantCugat del Vallés

- Proyecto para Catalana Occidente.
- Programación de páginas Web para la intranet del grupo Catalana Occidente.
- Programación en COBOL 390.

Técnico de sistemas, S2 Solucions i ServeisInformàtics 1/7/2000 — 31/10/2000

Barcelona

- Proyecto para IRISBUS (fabricante de autobuses y camiones).
- Diseño de la red de la sede central de IRISBUS en Barcelona.
- Configuración e implantación de servidores IBM.

Programador, S2 Solucions i ServeisInformàtics 6/3/2000 — 30/6/2000

Barcelona

- Proyecto para el Ajuntament de Barcelona.
- Realización de un producto para gestionar stocks.
- Programación en COBOL para AS/400

Programador y Técnico de sistemas AS/400, ANDEP 1/12/1998 — 1/3/2000

Barcelona

- Múltiples proyectos de servicios para pequeñas y medianas empresas.
- Programación en COBOL para AS/400
- Instalación y configuración de sistemas AS/400

Informático, IMC (Headhunting) 1995 — 1998

Barcelona

- Diversas tareas de ofimática y administrativas.
- Mantenimiento de los equipos informáticos.
- Impartición de formación en herramientas de ofimática.

IDIOMAS

- Catalán y castellano nativos.
- Inglés leído y escrito alto. Hablado medio.

COLECCIÓN "CUADERNOS DE DIRECCIÓN ASEGURADORA"

Master en Dirección de Entidades Aseguradoras y Financieras
Facultad de Economía y Empresa. Universidad de Barcelona

PUBLICACIONES

1.- Francisco Abián Rodríguez: "Modelo Global de un Servicio de Prestaciones Vida y su interrelación con Suscripción" 2005/2006

2.- Erika Johanna Aguilar Olaya: "Gobierno Corporativo en las Mutualidades de Seguros" 2005/2006

3.- Alex Aguyé Casademunt: "La Entidad Multicanal. Elementos clave para la implantación de la Estrategia Multicanal en una entidad aseguradora" 2009/2010

4.- José María Alonso-Rodríguez Piedra: "Creación de una plataforma de servicios de siniestros orientada al cliente" 2007/2008

5.- Jorge Alvez Jiménez: "innovación y excelencia en retención de clientes" 2009/2010

6.- Anna Aragonés Palom: "El Cuadro de Mando Integral en el Entorno de los seguros Multirriesgo" 2008/2009

7.- Maribel Avila Ostos: "La tele-suscripción de Riesgos en los Seguros de Vida" 2009/20010

8.- Mercé Bascompte Riquelme: "El Seguro de Hogar en España. Análisis y tendencias" 2005/2006

9.- Aurelio Beltrán Cortés: "Bancaseguros. Canal Estratégico de crecimiento del sector asegurador" 2010/2011

10.- Manuel Blanco Alpuente:"Delimitación temporal de cobertura en el seguro de responsabilidad civil. Las cláusulas claims made" 2008/2009

11.- Eduard Blanxart Raventós: "El Gobierno Corporativo y el Seguro D & O" 2004/2005

12.- Rubén Bouso López: "El Sector Industrial en España y su respuesta aseguradora: el Multirriesgo Industrial. Protección de la empresa frente a las grandes pérdidas patrimoniales"2006/2007

13.- Kevin van den Boom:"El Mercado Reasegurador (Cedentes, Brokers y Reaseguradores). Nuevas Tendencias y Retos Futuros" 2008/2009

14.- Laia Bruno Sazatornil: "L'ètica i la rentabilitat en les companyies asseguradores. Proposta de codi deontològic" 2004/2005

15.- María Dolores Caldés LLopis: "Centro Integral de Operaciones Vida" 2007/2008

16.- Adolfo Calvo Llorca: "Instrumentos legales para el recobro en el marco del seguro de crédito" 2010/2011

17.- Ferran Camprubí Baiges: "La gestión de las inversiones en las entidades aseguradoras. Selección de inversiones" 2010/2011

18.- Joan Antoni Carbonell Aregall: "La Gestió Internacional de Sinistres d'Automòbil amb Resultat de Danys Materials" 2003-2004

19.- Susana Carmona Llevadot: "Viabilidad de la creación de un sistema de Obra Social en una entidad aseguradora" 2007/2008

20.- Sergi Casas del Alcazar: “El PLan de Contingencias en la Empresa de Seguros” 2010/2011

21.- Francisco Javier Cortés Martínez: “Análisis Global del Seguro de Decesos” 2003-2004

22.- María Carmen Ceña Nogué:“El Seguro de Comunidades y su Gestión” 2009/2010

23.- Jordi Cots Paltor: “Control Interno. El auto-control en los Centros de Siniestros de Automóviles” 2007/2008

24.- Montserrat Cunillé Salgado: “Los riesgos operacionales en las Entidades Aseguradoras” 2003-2004

25.- Ricard Doménech Pagés: “La realidad 2.0. La percepción del cliente, más importante que nunca” 2010/2011

26.- Luis Domínguez Martínez: “Formas alternativas para la Cobertura de Riesgos” 2003-2004

27.- Marta Escudero Cutal: “Solvencia II. Aplicación práctica en una entidad de Vida” 2007/2008

28.- Salvador Esteve Casablancas: “La Dirección de Reaseguro. Manual de Reaseguro” 2005/2006

29.- Alvaro de Falguera Gaminde: “Plan Estratégico de una Correduría de Seguros Náuticos” 2004/2005

30.- Isabel Mª Fernández García: “Nuevos aires para las Rentas Vitalicias” 2006/2007

31.- Eduard Fillet Catarina: “Contratación y Gestión de un Programa Internacional de Seguros” 2009/2010

32.- Pablo Follana Murcia: “Métodos de Valoración de una Compañía de Seguros. Modelos Financieros de Proyección y Valoración consistentes” 2004/2005

33.- Juan Fuentes Jassé: “El fraude en el seguro del Automóvil” 2007/2008

34.- Xavier Gabarró Navarro: ""El Seguro de Protección Jurídica. Una oportunidad de Negocio"" 2009/2010

35.- Josep María Galcerá Gombau: “La Responsabilidad Civil del Automóvil y el Daño Corporal. La gestión de siniestros. Adaptación a los cambios legislativos y propuestas de futuro” 2003-2004

36.- Luisa García Martínez: “El Carácter tuitivo de la LCS y los sistemas de Defensa del Asegurado. Perspectiva de un Operador de Banca Seguros” 2006/2007

37.- Fernando García Giralt: “Control de Gestión en las Entidades Aseguradoras” 2006/2007

38.- Jordi García-Muret Ubis: “Dirección de la Sucursal. D. A. F. O.” 2006/2007

39.- David Giménez Rodríguez: “El seguro de Crédito: Evolución y sus Canales de Distribución” 2008/2009

40.- Juan Antonio González Arriete: “Línea de Descuento Asegurada” 2007/2008

41.- Miquel Gotés Grau: “Assegurances Agràries a BancaSeguros. Potencial i Sistema de Comercialització” 2010/2011

42.- Jesús Gracia León: “Los Centros de Siniestros de Seguros Generales. De Centros Operativos a Centros Resolutivos. De la optimización de recursos a la calidad de servicio” 2006/2007

43.- José Antonio Guerra Díez: “Creación de unas Tablas de Mortalidad Dinámicas” 2007/2008

44.- Santiago Guerrero Caballero: “La politización de las pensiones en España” 2010/2011

45.- Francisco J. Herencia Conde: “El Seguro de Dependencia. Estudio comparativo a nivel internacional y posibilidades de desarrollo en España” 2006/2007

46.- Francisco Javier Herrera Ruiz:“Selección de riesgos en el seguro de Salud” 2009/2010

47.- Alicia Hoya Hernández:“Impacto del cambio climático en el reaseguro” 2008/2009

48.- Jordi Jiménez Baena: “Creación de una Red de Agentes Exclusivos” 2007/2008

49.- Oriol Jorba Cartoixà:“La oportunidad aseguradora en el sector de las energías renovables” 2008/2009

50.- Anna Juncá Puig: “Una nueva metodología de fidelización en el sector asegurador” 2003/2004

51.- Ignacio Lacalle Goría: “El artículo 38 Ley Contrato de Seguro en la Gestión de Siniestros. El procedimiento de peritos” 2004/2005

52.- Mª Carmen Lara Ortíz: “Solvencia II. Riesgo de ALM en Vida” 2003/2004

53.- Haydée Noemí Lara Téllez: “El nuevo sistema de Pensiones en México” 2004/2005

54.- Marta Leiva Costa: “La reforma de pensiones públicas y el impacto que esta modificación supone en la previsión social” 2010/2011

55.- Victoria León Rodríguez: “Problemàtica del aseguramiento de los Jóvenes en la política comercial de las aseguradoras” 2010/2011

56.- Pilar Lindín Soriano: “Gestión eficiente de pólizas colectivas de vida” 2003/2004

57.- Victor Lombardero Guarner: “La Dirección Económico Financiera en el Sector Asegurador” 2010/2011

58.- Maite López Aladros: “Análisis de los Comercios en España. Composición, Evolución y Oportunidades de negocio para el mercado asegurador” 2008/2009

59.- Josep March Arranz: “Los Riesgos Personales de Autónomos y Trabajadores por cuenta propia. Una visión de la oferta aseguradora” 2005/2006

60.- Miquel Maresch Camprubí: “Necesidades de organización en las estructuras de distribución por mediadores” 2010/2011

61.- José Luis Marín de Alcaraz: “El seguro de impago de alquiler de viviendas” 2007/2008

62.- Miguel Ángel Martínez Boix: “Creatividad, innovación y tecnología en la empresa de seguros” 2005/2006

63.- Susana Martínez Corveira: “Propuesta de Reforma del Baremo de Autos” 2009/2010

64.- Inmaculada Martínez Lozano: “La Tributación en el mundo del seguro” 2008/2009

65.- Dolors Melero Montero: “Distribución en bancaseguros: Actuación en productos de empresas y gerencia de riesgos" 2008/2009

66.- Josep Mena Font: “La Internalización de la Empresa Española” 2009/2010

67.- Angela Milla Molina: “La Gestión de la Previsión Social Complementaria en las Compañías de Seguros. Hacia un nuevo modelo de Gestión” 2004/2005

68.- Montserrat Montull Rossón: “Control de entidades aseguradoras” 2004/2005

69.- Eugenio Morales González: “Oferta de licuación de patrimonio inmobiliario en España” 2007/2008

70.- Lluis Morales Navarro: “Plan de Marketing. División de Bancaseguros” 2003/2004

71.- Sonia Moya Fernández: “Creación de un seguro de vida. El éxito de su diseño” 2006/2007

72.- Rocio Moya Morón: “Creación y desarrollo de nuevos Modelos de Facturación Electrónica en el Seguro de Salud y ampliación de los modelos existentes” 2008/2009

73.- María Eugenia Muguerza Goya: “Bancaseguros. La comercialización de Productos de Seguros No Vida a través de redes bancarias” 2005/2006

74.- Ana Isabel Mullor Cabo: “Impacto del Envejecimiento en el Seguro” 2003/2004

75.- Estefanía Nicolás Ramos: “Programas Multinacionales de Seguros” 2003/2004

76.- Santiago de la Nogal Mesa: “Control interno en las Entidades Aseguradoras” 2005/2006

77.- Antonio Nolasco Gutiérrez: “Venta Cruzada. Mediación de Seguros de Riesgo en la Entidad Financiera” 2006/2007

78.- Francesc Ocaña Herrera: “Bonus-Malus en seguros de asistencia sanitaria” 2006/2007

79.- Antonio Olmos Francino: “El Cuadro de Mando Integral: Perspectiva Presente y Futura” 2004/2005

80.- Luis Palacios García: “El Contrato de Prestación de Servicios Logísticos y la Gerencia de Riesgos en Operadores Logísticos” 2004/2005

81.- Jaume Paris Martínez: “Segmento Discapacitados. Una oportunidad de Negocio” 2009/2010

82.- Martín Pascual San Martín: “El incremento de la Longevidad y sus efectos colaterales” 2004/2005

83.- Montserrat Pascual Villacampa: “Proceso de Tarificación en el Seguro del Automóvil. Una perspectiva técnica” 2005/2006

84.- Marco Antonio Payo Aguirre: “La Gerencia de Riesgos. Las Compañías Cautivas como alternativa y tendencia en el Risk Management” 2006/2007

85.- Patricia Pérez Julián: “Impacto de las nuevas tecnologías en el sector asegurador” 2008/2009

86.- María Felicidad Pérez Soro: “La atención telefónica como transmisora de imagen” 2009/2010

87.- Marco José Piccirillo: “Ley de Ordenación de la Edificación y Seguro. Garantía Decenal de Daños” 2006/2007

88.- Irene Plana Güell: “Sistemas d’Informació Geogràfica en el Sector Assegurador” 2010/2011

89.- Sonia Plaza López: “La Ley 15/1999 de Protección de Datos de carácter personal” 2003/2004

90.- Pere Pons Pena: “Identificación de Oportunidades comerciales en la Provincia de Tarragona” 2007/2008

91.- María Luisa Postigo Díaz: “La Responsabilidad Civil Empresarial por accidentes del trabajo. La Prevención de Riesgos Laborales, una asignatura pendiente” 2006/2007

92.- Jordi Pozo Tamarit: “Gerencia de Riesgos de Terminales Marítimas” 2003/2004

93.- Francesc Pujol Niñerola: “La Gerencia de Riesgos en los grupos multisectoriales” 2003-2004

94.- Mª del Carmen Puyol Rodríguez: “Recursos Humanos. Breve mirada en el sector de Seguros” 2003/2004

95.- Antonio Miguel Reina Vidal: “Sistema de Control Interno, Compañía de Vida. Bancaseguros” 2006/2007

96.- Marta Rodríguez Carreiras: “Internet en el Sector Asegurador” 2003/2004

97.- Juan Carlos Rodríguez García: “Seguro de Asistencia Sanitaria. Análisis del proceso de tramitación de Actos Médicos” 2004/2005

98.- Mónica Rodríguez Nogueiras: “La Cobertura de Riesgos Catastróficos en el Mundo y soluciones alternativas en el sector asegurador” 2005/2006

99.- Susana Roquet Palma: “Fusiones y Adquisiciones. La integración y su impacto cultural” 2008/2009

100.- Santiago Rovira Obradors: “El Servei d’Assegurances. Identificació de les variables clau” 2007/2008

101.- Carlos Ruano Espí: “Microseguro. Una oportunidad para todos” 2008/2009

102.- Mireia Rubio Cantisano: “El Comercio Electrónico en el sector asegurador” 2009/2010

103.- María Elena Ruíz Rodríguez: “Análisis del sistema español de Pensiones. Evolución hacia un modelo europeo de Pensiones único y viabilidad del mismo” 2005/2006

104.- Eduardo Ruiz-Cuevas García: “Fases y etapas en el desarrollo de un nuevo producto. El Taller de Productos” 2006/2007

105.- Pablo Martín Sáenz de la Pascua: “Solvencia II y Modelos de Solvencia en Latinoamérica. Sistemas de Seguros de Chile, México y Perú” 2005/2006

106.- Carlos Sala Farré: “Distribución de seguros. Pasado, presente y tendencias de futuro” 2008/2009

107.- Ana Isabel Salguero Matarín: “Quién es quién en el mundo del Plan de Pensiones de Empleo en España” 2006/2007

108.- Jorge Sánchez García: “El Riesgo Operacional en los Procesos de Fusión y Adquisición de Entidades Aseguradoras” 2006/2007

109.- María Angels Serral Floreta: “El lucro cesante derivado de los daños personales en un accidente de circulación” 2010/2011

110.- David Serrano Solano: “Metodología para planificar acciones comerciales mediante el análisis de su impacto en los resultados de una compañía aseguradora de No Vida” 2003/2004

111.- Jaume Siberta Durán: “Calidad. Obtención de la Normativa ISO 9000 en un centro de Atención Telefónica” 2003/2004

112.- María Jesús Suárez González: “Los Poolings Multinacionales” 2005/2006

113.- Miguel Torres Juan: “Los siniestros IBNR y el Seguro de Responsabilidad Civil” 2004/2005

114.- Carlos Travé Babiano: “Provisiones Técnicas en Solvencia II. Valoración de las provisiones de siniestros” 2010/2011

115.- Rosa Viciana García: “Banca-Seguros. Evolución, regulación y nuevos retos” 2007/2008

116.- Ramón Vidal Escobosa: “El baremo de Daños Personales en el Seguro de Automóviles” 2009/2010

117.- Tomás Wong-Kit Ching: “Análisis del Reaseguro como mitigador del capital de riesgo” 2008/2009

118.- Yibo Xiong: “Estudio del mercado chino de Seguros: La actualidad y la tendencia” 2005/2006

119.- Beatriz Bernal Callizo: “Póliza de Servicios Asistenciales” 2003/2004

120.- Marta Bové Badell: “Estudio comparativo de evaluación del Riesgo de Incendio en la Industria Química” 2003/2004

121.- Ernest Castellón Texidó: “La edificación. Fases del proceso, riesgos y seguros” 2004/2005

122.- Sandra Clusella Giménez: “Gestió d’Actius i Passius. Inmunització Financera” 2004/2005

123.- Miquel Crespí Argemí: “El Seguro de Todo Riesgo Construcción” 2005/2006

124.- Yolanda Dengra Martínez: “Modelos para la oferta de seguros de Hogar en una Caja de Ahorros” 2007/2008

125.- Marta Fernández Ayala: “El futuro del Seguro. Bancaseguros” 2003/2004

126.- Antonio Galí Isus: “Inclusión de las Energías Renovables en el sistema Eléctrico Español” 2009/2010

127.- Gloria Gorbea Bretones: “El control interno en una entidad aseguradora” 2006/2007

128.- Marta Jiménez Rubio: “El procedimiento de tramitación de siniestros de daños materiales de automóvil: análisis, ventajas y desventajas” 2008/2009

129.- Lorena Alejandra Libson: “Protección de las víctimas de los accidentes de circulación. Comparación entre el sistema español y el argentino” 2003/2004

130.- Mario Manzano Gómez: “La responsabilidad civil por productos defectuosos. Solución aseguradora” 2005/2006

131.- Àlvar Martín Botí: “El Ahorro Previsión en España y Europa. Retos y Oportunidades de Futuro” 2006/2007

132.- Sergio Martínez Olivé: “Construcción de un modelo de previsión de resultados en una Entidad Aseguradora de Seguros No Vida” 2003/2004

133.- Pilar Miracle Vázquez: “Alternativas de implementación de un Departamento de Gestión Global del Riesgo. Aplicado a empresas industriales de mediana dimensión” 2003/2004

134.- María José Morales Muñoz: “La Gestión de los Servicios de Asistencia en los Multirriesgo de Hogar” 2007/2008

135.- Juan Luis Moreno Pedroso: "El Seguro de Caución. Situación actual y perspectivas" 2003/2004

136.- Rosario Isabel Pastrana Gutiérrez: “Creació d'una empresa de serveis socials d'atenció a la dependència de les persones grans enfocada a productes d'assegurances” 2007/2008

137.- Joan Prat Rifá: "La Previsió Social Complementaria a l'Empresa" 2003/2004

138.- Alberto Sanz Moreno: “Beneficios del Seguro de Protección de Pagos” 2004/2005

139.- Judith Safont González: “Efectes de la contaminació i del estils de vida sobre les assegurances de salut i vida” 2009/2010

140.- Carles Soldevila Mejías: “Models de gestió en companyies d’assegurances. Outsourcing / Insourcing” 2005/2006

141.- Olga Torrente Pascual: “IFRS-19 Retribuciones post-empleo” 2003/2004

142.- Annabel Roig Navarro: “La importancia de las mutualidades de previsión social como complementarias al sistema publico” 2009/2010

143.- José Angel Ansón Tortosa: “Gerencia de Riesgos en la Empresa española” 2011/2012

144.- María Mecedes Bernués Burillo: “El permiso por puntos y su solución aseguradora” 2011/2012

145.- Sònia Beulas Boix: “Prevención del blanqueo de capitales en el seguro de vida” 2011/2012

146.- Ana Borràs Pons: “Teletrabajo y Recursos Humanos en el sector Asegurador” 2011/2012

147.- María Asunción Cabezas Bono: “La gestión del cliente en el sector de bancaseguros” 2011/2012

148.- María Carrasco Mora: “Matching Premium. New approach to calculate technical provisions Life insurance companies” 2011/2012

149.- Eduard Huguet Palouzie: “Las redes sociales en el Sector Asegurador. Plan social-media. El Community Manager” 2011/2012

150.- Laura Monedero Ramírez: “Tratamiento del Riesgo Operacional en los 3 pilares de Solvencia II” 2011/2012

151.- Salvador Obregón Gomá: “La Gestión de Intangibles en la Empresa de Seguros” 2011/2012

152.- Elisabet Ordóñez Somolinos: “El sistema de control Interno de la Información Financiera en las Entidades Cotizadas” 2011/2012

153.- Gemma Ortega Vidal: “La Mediación. Técnica de resolución de conflictos aplicada al Sector Asegurador” 2011/2012

154.- Miguel Ángel Pino García: “Seguro de Crédito: Implantación en una aseguradora multirramo” 2011/2012

155.- Genevieve Thibault: “The Costumer Experience as a Sorce of Competitive Advantage” 2011/2012

156.- Francesc Vidal Bueno: “La Mediación como método alternativo de gestión de conflictos y su aplicación en el ámbito asegurador” 2011/2012

157.- Mireia Arenas López: “El Fraude en los Seguros de Asistencia. Asistencia en Carretera, Viaje y Multirriesgo” 2012/2013

158.- Lluis Fernández Rabat: “El proyecto de contratos de Seguro-IFRS4. Expectativas y realidades” 2012/2013

159.- Josep Ferrer Arilla: “El seguro de decesos. Presente y tendencias de futuro” 2012/2013

160.- Alicia García Rodríguez: “El Cuadro de Mando Integral en el Ramo de Defensa Jurídica” 2012/2013

161.- David Jarque Solsona: “Nuevos sistemas de suscripción en el negocio de vida. Aplicación en el canal bancaseguros” 2012/2013

162.- Kamal Mustafá Gondolbeu: “Estrategias de Expansión en el Sector Asegurador. Matriz de Madurez del Mercado de Seguros Mundial” 2012/2013

163.- Jordi Núñez García: “Redes Periciales. Eficacia de la Red y Calidad en el Servicio” 2012/2013

164.- Paula Núñez García: “Benchmarking de Autoevaluación del Control en un Centro de Siniestros Diversos” 2012/2013

165.- Cristina Riera Asensio: “Agregadores. Nuevo modelo de negocio en el Sector Asegurador” 2012/2013

166.- Joan Carles Simón Robles: “Responsabilidad Social Empresarial. Propuesta para el canal de agentes y agencias de una compañía de seguros generalista” 2012/2013

167.- Marc Vilardebó Miró: “La política de inversión de las compañías aseguradoras ¿Influirá Solvencia II en la toma de decisiones?” 2012/2013

168.- Josep María Bertrán Aranés: “Segmentación de la oferta aseguradora para el sector agrícola en la provincia de Lleida” 2013/2014

169.- María Buendía Pérez: “Estrategia: Formulación, implementación, valoración y control” 2013/2014

170.- Gabriella Fernández Andrade: “Oportunidades de mejora en el mercado de seguros de Panamá” 2013/2014

171.- Alejandro Galcerán Rosal: “El Plan Estratégico de la Mediación: cómo una Entidad Aseguradora puede ayudar a un Mediador a implementar el PEM” 2013/2014

172.- Raquel Gómez Fernández: “La Previsión Social Complementaria: una apuesta de futuro” 2013/2014

173.- Xoan Jovaní Guiral: “Combinaciones de negocios en entidades aseguradoras: una aproximación práctica” 2013/2014

174.- Àlex Lansac Font: “Visión 360 de cliente: desarrollo, gestión y fidelización” 2013/2014

175.- Albert Llambrich Moreno: “Distribución: Evolución y retos de futuro: la evolución tecnológica” 2013/2014

176.- Montserrat Pastor Ventura: “Gestión de la Red de Mediadores en una Entidad Aseguradora. Presente y futuro de los agentes exclusivos” 2013/2014

177.- Javier Portalés Pau: “El impacto de Solvencia II en el área de TI” 2013/2014

178.- Jesús Rey Pulido: “El Seguro de Impago de Alquileres: Nuevas Tendencias” 2013/2014

179.- Anna Solé Serra: “Del cliente satisfecho al cliente entusiasmado. La experiencia cliente en los seguros de vida” 2013/2014

180.- Eva Tejedor Escorihuela: “Implantación de un Programa Internacional de Seguro por una compañía española sin sucursales o filiales propias en el extranjero. Caso práctico: Seguro de Daños Materiales y RC” 2013/2014