PROYECTO FIN DE CARRERA

PLANES DE CONTINGENCIA Y SU AUDITORÍA

Rodrigo Herrero Pizarro

100029972

2. Agradecimientos:

Después de este largo y laborioso proyecto agradezco en primer lugar a Miguel Ángel Ramos mi tutor director del proyecto por su paciencia y comprensión durante la elaboración de este proyecto. A mis padres por apoyarme en la consecución del mismo. No quería terminar sin mencionar a algunos de los que me acompañaron durante el estudio de esta carrera: Valeriano, Jorge, Elena Vega, Jaime, Alberto, Juanra, Elena Gómez, etc.

3. Índice

Planes de contingencia y su auditoría

4. Introducción

Génesis de los planes de contingencia: Evitar “apagar fuegos” de forma aleatoria cuando se produzcan problemas en sistemas informáticos, es decir, se buscó la manera de tener todo previsto para obtener una respuesta rápida y eficaz frente a eventos perjudiciales del sistema; anteriormente a que existiesen los planes de contingencia se iban solucionando los problemas sobre la marcha e improvisadamente con las consecuentes pérdidas de tiempo y dinero.

Entendemos plan de contingencia o continuidad del “servicio” ó “negocio” en las organizaciones como un enfoque global de la actividad que crea un marco estratégico para revisar y modificar cuando sea necesario la forma en que la organización proporciona sus servicios, aumentando su resistencia frente a interrupciones o pérdidas. Es decir un plan cuyos medios ya sean propios o contratados nos permiten obtener unas respuestas específicas en momentos críticos y de emergencia para salvaguardar nuestro negocio y tenerlo operativo hasta la restitución de la situación anterior al evento perjudicial.

El plan de contingencia no es una mera adición de algo que se debe hacer sino que es una parte integral de toda la organización. Es importante hacer comprender a los responsables de la organización acerca de la necesidad de un plan de contingencia adecuado y que no es “algo más” que hay que hacer sino que es igual de importante o más que las otras partes del proyecto. Es reconocida como una buena práctica profesional y es parte integral del buen gobierno de las organizaciones, de esta forma toma una dimensión estratégica y no debería ser considerado una mera herramienta operativa.

Identifica los impactos y amenazas potenciales que pueden perjudicar a la organización y proporciona un marco para construir y reforzar la capacidad

de una respuesta efectiva. El plan de contingencia nos permite en caso de incidencia grave:

- Mitigar los riesgos de colapso del negocio
- Mantener los procesos críticos del negocio
- Todo ello en un tiempo prefijado

Los planes de contingencia fueron revisados antes del efecto 2000 y también después de los ataques terroristas de América. También el incremento de ataques electrónicos etc., ha provocado la revisión de los planes de contingencia para poder responder a las nuevas amenazas que se plantean.

Como ejemplo podemos poner lo ocurrido en el World Trade Center en el que se vio claramente la necesidad de un plan de contingencia que permita la supervivencia del negocio a pesar del desastre. Nadie puede anticipar un desastre, otros sólo se pueden anticipar con poca antelación, en cualquier caso, tenemos que tener previsto cual será su impacto en caso de producirse y la manera que tenemos para responder en ese hipotético caso.

Para ello tenemos que tener completamente estudiado y previsto en qué casos se activarán los planes de contingencia y durante qué período estarán operativos.

La idiosincrasia no solo del mundo electrónico sino de la sociedad actual impone una rápida respuesta. Por ejemplo, los clientes esperan una respuesta inmediata, los accionistas quieren que el control de la organización se mantenga a pesar de la crisis, los empleados quieren que sus empleos no corran riesgos, los proveedores esperan que sus ingresos sean satisfechos en los plazos establecidos, las agencias reguladoras esperan que la empresa cumpla con todos los requisitos legales, etc.

Un plan de contingencia siempre ha sido necesario, pero ahora se manifiesta como un elemento crítico de seguridad de la empresa, ya que al depender ésta en gran medida de los sistemas de información basados en el

uso de tecnologías de la información se hacen completamente imprescindibles. Un plan de contingencia se activaría solo cuando existe una situación de emergencia y las demás medidas de seguridad hayan fallado. Es decir, forma parte del plan de seguridad general pero sólo cuando las demás medidas se hayan sobrepasado, no funcionen y no quede otra alternativa; entonces se activará el plan, esto querrá decir que la situación es de emergencia y ha existido una amenaza seria para la organización.

Nos percatamos que un plan de contingencia y su alcance son más importantes de lo que a priori podría parecer. A pesar de ello incluso entre las organizaciones con plan de contingencia, según un estudio de KPMG, menos de la mitad reconoce tener un plan de contingencia adecuado. Según un estudio de Datapro, de 1113 entidades solo el 42% declara tener un plan de recuperación ante desastres, y solo el 65 % reconoce tener copia de datos en otro lugar.

¿Por qué un plan de contingencia?

El 67% de las compañías que tienen un desastre por más de 2 semanas, están fuera del negocio en los 2 años siguientes. (Sun Systems).

Gartner group estima, que de 5 empresas que sufren una contingencia, 2 de ellas saldrán del negocio en los 5 años siguientes.

El 40% de las empresas dicen que tomará más de un día regresar o “poner” en línea los sistemas en caso de que un desastre destruya una localidad principal. (Information Week Research).

El coste de estar fuera de servicio por una hora es de $84.000 en un Call Center. (IDC)

El costo estimado por una hora de un empleado de no operar en caso de contingencia de acuerdo a la información de la industria aseguradora es de $370 USD. (Meta Group).

El 45% de las contingencias de los centros de cómputo en EUA es debido a fallos de energía eléctrica. (Contingency Planning Research).

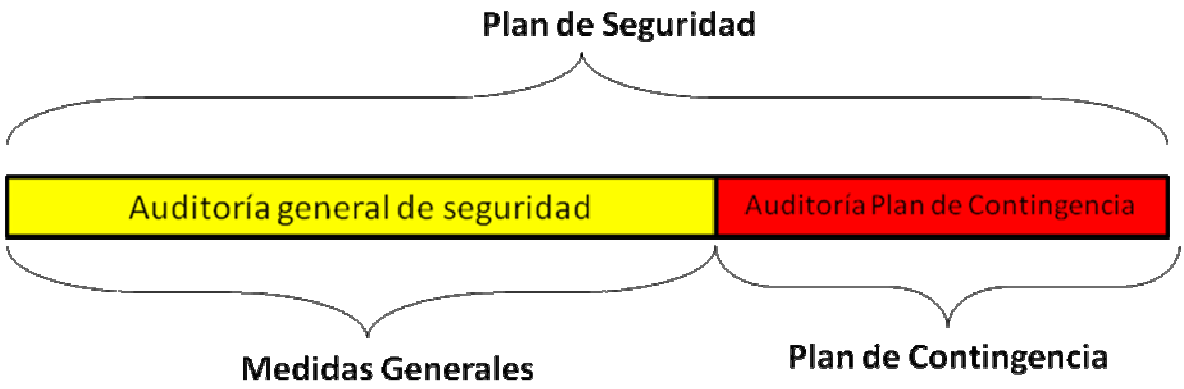
Las funciones del negocio no pueden continuar operando después de 4,8 días sin la recuperación de la infraestructura tecnológica. (Info Security News).

El 68% de los negocios reclaman planes de contingencia. (Disaster Recovery Journal).

El 60% de las empresas tienen información crítica de los usuarios en sus laptops o desktops. (Network World).

En muchas ocasiones vemos que la Dirección no conoce el alto riesgo que supone la no presencia de planes de contingencia en sus organizaciones o la debilidad de éstos. De ahí la importancia de las auditorías no solo generales del plan de seguridad sino de los planes de contingencia en particular, que dan una clara y seria advertencia de los riesgos de dejar los planes de contingencia como algo secundario y sin importancia.

Esquema:



Con esto vemos como en ocasiones se le concede poca importancia a esta fase imprescindible de todo proyecto que le resta versatilidad y robustez. De ahí que se haga imprescindible la realización de una auditoría de los planes de contingencia que nos permita evaluar la adecuación de los planes de contingencia al proyecto/s desarrollado/s por la organización.

La información en esta sociedad de la información es el activo más importante para una empresa y su protección a través de un plan de seguridad una de las máximas que debe tener cada entidad; dentro de la seguridad hay que proveer de una continuidad y operatividad a pesar de cualquier eventualidad que pueda acontecer, de ahí esa necesidad de un mayor control no solo ya del plan de seguridad de una entidad en general

sino de su plan de continuidad en particular, que nos permitirá no solo proteger nuestra información sino mantener una operatividad con nuestras funciones críticas y así poder seguir compitiendo y lo que es más importante: sobrevivir.

Los recursos o activos propios de una empresa son humanos, materiales (edificios, CPUs, etc.) e inmateriales (Software, etc). Todos estos recursos se encuentran en un entorno de incertidumbre que puede provocar interrupciones breves o prolongadas del funcionamiento normal de la empresa. De ahí la necesidad de un plan de contingencia que asegure de la mejor manera posible la continuidad.

Evidentemente dependiendo de la naturaleza y magnitud de la organización estos planes serán más o menos complejos, y tendrán más o menos procedimientos, pero lo que debe quedar claro es que el plan de contingencia no es algo que se deba atender a "ratos perdidos" y que supone algo primordial que debe ser atendido y revisado no solo dentro de los controles y auditorías internas sino también de las externas concediéndole la importancia que se merece en todo momento.

La Norma ISO17799-1 (EN 717799-1) nos dice las buenas prácticas de gestión de seguridad en su capítulo 11:

Gestión de continuidad del negocio (plan de contingencia):

Apartados:

- Proceso de gestión de la continuidad del negocio
- Continuidad del negocio y análisis de impactos
- Redacción e implantación de planes de continuidad
- Marco de planificación para continuidad del negocio
- Prueba, mantenimiento y reevaluación de planes de continuidad

Como vemos se incluye el plan de contingencia y su evaluación (auditoría).

Un plan de contingencia es un valor en alza y permite asegurar en parte el futuro de nuestra operatividad como empresa. Para un plan de contingencia que permita la continuidad del negocio es imprescindible abarcar (tener en cuenta) todo tipo de tecnologías y soportes tanto antiguos como nuevos, tanto en papel como en soporte electrónico, tanto manual como automatizado, tanto individual como integrado. También nos permitirá reducir las pérdidas económicas. Aunque cabe mencionar que requiere importantes recursos económicos, es de una gran complejidad y es muy sensible a cambios realizados, por lo tanto se necesita de una actualización permanente. El mantenimiento y pruebas del plan es una parte importante que forma parte del plan de contingencia, y eso implica que al menos una vez al año se hagan pruebas y se introduzcan modificaciones ya que la organización cambia cada día; el plan responde a las necesidades de un momento determinado y hay que ir actualizándolo para que no quede inservible y pueda responder a las nuevas situaciones. Lo peor que puede ocurrir no es que no se tenga un plan sino creer que se tiene uno y que este no sirva para nada.

Conviene tener presentes tres conceptos importantes a la hora de tratar de conformar primero y auditar después un plan de contingencia, son diferentes pero están relacionados:

Continuidad: se refiere al negocio (a sus funciones); requiere la disponibilidad de la información y por tanto de los sistemas que la tratan y su entorno (suministros, etc.)

Incidencia/Interrupción: evento que interrumpe la continuidad de los sistemas, con consecuencias limitadas para el negocio; puede reducirse por medios razonables y disponibles.

Contingencia: evento que interrumpe la continuidad de los sistemas, con consecuencias catastróficas para el negocio; sólo puede reducirse por medios extraordinarios y en general muy costosos, organizativa y técnicamente.

El plan de contingencia discierne estos elementos y actúa en función de cómo sean. Pretendemos una continuidad frente a incidencias y contingencias.

Otros conceptos de los que hemos hablado pero no hemos definido serían:

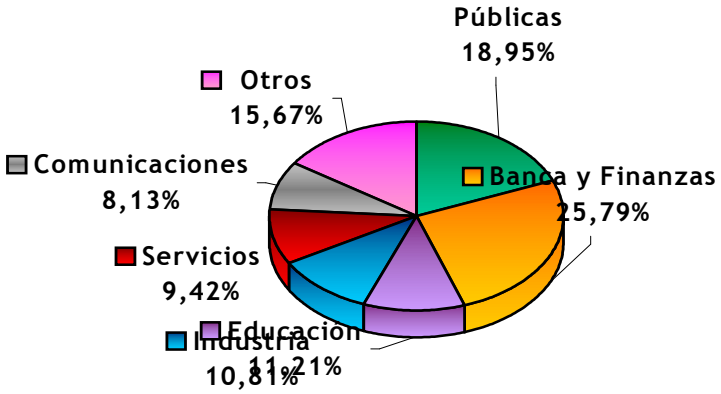
Amenazas: Que son los eventos que pueden provocar o desencadenar un incidente en la organización, que pueden provocar daños materiales o inmateriales en sus activos. Las causas son de diversos tipos: humanas, intencionadas o no; y no humanas: accidentes o desastres de origen natural o industrial, averías, interrupciones de servicios o de suministros esenciales.

Vulnerabilidad: Es la potencialidad o posibilidad de la materialización de una amenaza sobre un activo.

Impacto: Es la consecuencia de la materialización de una amenaza sobre un activo de la empresa. El impacto será cuantitativo si las pérdidas se pueden monetizar de alguna manera, será cualitativo cuando las pérdidas sean funcionales.

Riesgo: Es la probabilidad de que se produzca un impacto determinado en un activo. El análisis del riesgo permite, en conjunto con la vulnerabilidad y el impacto ambos derivados a su vez de las relación del activo y la amenaza, calcular si dicho riesgo es asumible o aceptable.

En el siguiente cuadro vemos en qué proporción afectan las interrupciones en los diferentes sectores, como vemos ninguno está a salvo de ellas y da fe de la importancia que tienen los planes de contingencia y su auditoría en una organización.



En definitiva el plan de contingencia es una parte más (quizá la más importante), de un plan de seguridad global que ha de tener la organización siempre acompañado de su respectiva auditoría, con ello buscamos minimizar el riesgo de colapso para que la organización siga siendo operativa a pesar de las posibles desastres, contratiempos, o fenómenos de cualquier otra índole que puedan ocurrir.

El plan de contingencia no es un requisito legal (en España) sino que es una obligación profesional ante las partes afectadas de una organización ya sean accionistas, empleados, clientes o proveedores. Sí es obligado para entidades financieras.

Un plan de contingencia es como tener un plan para un viaje en coche, es decir que tenemos todo lo necesario en caso de contingencia ya sea avería, revisión policial, etc (seguro, carnet, rueda de repuesto, herramientas, teléfono del seguro). La auditoría sería la revisión periódica de que todos estos elementos son funcionales y están a punto por si falla algo.

Ciertamente y en gran medida aún no somos conscientes completamente de la importancia de la información como activo, y nos siga faltando esa cultura de seguridad; seguridad que se centra en cubrir por ahora aspectos más tangibles.

La auditoría nos señalaría en definitiva la necesidad de un plan de contingencia y si éste cubre los requisitos mínimamente exigibles para que el plan sea adecuado a las necesidades de continuidad del negocio, la auditoría señalaría y determinaría las debilidades y propondría soluciones.

Auditoría/Control: Surge de la necesidad de ir optimizando la gestión de los recursos informáticos con presupuestos más ajustados y consiguiendo un equilibrio entre calidad y productividad.

Es la revisión, análisis y evaluación independiente y objetiva de la informática y su entorno (es decir los elementos propiamente informáticos como equipos, sistemas operativos, aplicaciones, comunicaciones, organización etc. por un lado y el entorno en forma de políticas, estándares y procedimientos en vigor en la entidad, su idoneidad así como el cumplimiento de estos por otro).

Comunican de forma objetiva e independiente las deficiencias, riesgos y posibles mejoras y pueden recomendar que se implanten o refuercen controles.

Los controles que realiza la auditoría han de ser razonables y adecuados sin ser excesivos ni insuficientes, en definitiva, que sean prácticos y se adecúen a las circunstancias del sistema con rentabilidad.

En el caso que nos compete en este trabajo aplicaremos la auditoría al plan de contingencia, lo que pretendemos con ello es:

- Asegurar que el plan de recuperación contribuye a la consecución de los objetivos del negocio y que, llegado el momento, funcionará como está previsto.

- Identificar las condiciones que facilitan la interrupción de los servicios como consecuencia de tener un plan inadecuado.

-En el caso de identificar debilidades en el plan, proponer soluciones.

-Procurar que el plan sea adecuado, ni sobreexceda ni sea exiguo.

Como iremos viendo a lo largo del desarrollo del plan iremos realizando una serie de ejemplos que nos permitirán ver los resultados de la evaluación de cada una de las fases del plan; esto nos ofrecerá un mejor conocimiento de la realidad propia de cada una de las fases y la calibración numérica que servirá como juicio para avisar de la facultad de cada una de las fases en su cometido.

El conjunto de las evaluaciones de cada una de las fases en los ejemplos prácticos que pondremos nos darán finalmente una evaluación global del plan y su comparación con lo que se considera una valoración objetivo, que sería el equivalente a la puntuación 3. No se persigue la puntuación máxima, que en este caso sería de 5, ya que nunca conseguiremos un nivel de seguridad absoluto, y el máximo de seguridad posible puede implicar un coste excesivo, no rentable, y a menudo, un freno para el trabajo diario.

La situación de una determinada fase, junto con su puntuación, reflejaría una situación concreta dentro de una actividad total de planificación, sin tener ninguna referencia respecto a la importancia de dicha fase dentro del

proceso total. Por ello, he optado por añadir un elemento de criterio propio basado en ejemplos prácticos visualizados por mí mismo, y cuya valoración, si bien subjetiva, nos ayudará de alguna manera a comprender la importancia de cada una de las fases dentro del conjunto total de fases de un plan de contingencia.

Cualquiera de las valoraciones que en los ejemplos iremos viendo tienen como objeto calibrar en qué medida esta fase está dentro de unos parámetros aceptables y si está en consonancia con el objetivo del plan o si por el contrario necesita de una mejora o actualización. Con objeto de visualizar esas valoraciones de una manera clara y concisa se aportarán una serie de tablas que nos permitirán conocer los cálculos relativos a estas valoraciones y por tanto saber con numeración y por tanto con exactitud en qué punto se encuentra nuestra fase respecto a nuestros objetivos y frente al resto del plan de contingencia.

La utilidad de estas tablas será primordial a la hora de evaluar y a lo largo del tiempo nos permitirán conocer los ajustes y desajustes sufridos por cada una de las fases y conoceremos por tanto la evolución de cada parte del plan. Ello nos permitiría, en función del sector de la entidad, y otros parámetros, conocer qué fases son más susceptibles de cambio, incluso predecir de alguna manera posibles comportamientos en un futuro.

Como veremos existen una serie de estándares que nos permiten también controlar y evaluar riesgos y aspectos del plan de contingencia, y qué implementaciones conseguirán reducir los riesgos, hablamos del estándar ISO/IEC 24762.

Éste estándar nos provee de una serie de guías para proceder correctamente dentro de la evaluación de los planes de contingencia. Cubre servicios y provee de la posibilidad de vuelta atrás y recuperación del soporte de la organización.

Asimismo en el mundo de los estándares disponemos de otro más para evaluación y auditoría de los planes de contingencia. Se trataría de COBIT, (Control objetives for information and related technology). Las empresas reconocen la importancia de las tecnologías de la información en el mundo actual y por tanto una guía como COBIT puede ser utilísima e imprescindible para reducir los riegos del uso de este tipo de tecnologías. Normalmente se utiliza el acrónimo IT para referirse a las tecnologías de la

información en inglés. Esto daría paso a lo que se llamaría IT Governance, que sería una estructura de relaciones y procesos para dirigir y controlar una empresa y conseguir una serie de éxitos ponderando los riesgos que pueda haber y considerando el retorno sobre las IT y sus procesos.

De esa manera las empresas han de decidir como otorgar responsabilidades a través de la comprensión de las IT que tengan y por tanto cual es la solución mejor para la continuidad y la reducción de riegos respecto a estas.

COBIT ayuda a encontrar numerosas necesidades de los planes de contingencia evaluando riesgos del negocio, necesidades de control y aspectos tecnológicos. Nos provee de un código de buenas prácticas y presenta actividades con una estructura lógica. Ello nos ayudará a optimizar la investigación de la información que conforma nuestro plan de contingencia y nos dará capacidad para evaluar de una manera fehaciente las cuestiones mal planteadas. Nos hemos de asegurar que existe una línea de trabajo de control interno que soporte nuestros procesos del plan de contingencia, hacerlo clarifica cuánto el control de las actividades satisface las necesidades de información y los impactos de los recursos de las IT.

El impacto de los recursos de las IT está bien determinado en las líneas de trabajo de COBIT junto con las necesidades del negocio para disponer de efectividad, confidencialidad, integridad, disponibilidad y realismo de toda aquella información que necesita de estos parámetros para satisfacer su proceso de vida dentro de una compañía. El control de la información de una empresa durante su actividad necesita de unas políticas, estructuras de organización interna, prácticas, procedimientos y responsabilidades. COBIT nos provee de ello de una manera estandarizada. El control de las IT es un objetivo claro y por tanto ha de realizarse con un propósito de implementar procesos de control y mejorar por tanto las IT presentes en los planes de contingencia.

La orientación del negocio es la temática fundamental sobre la que versa COBIT. Está diseñado para ser empleado no solo por usuarios o auditores, sino que es sin duda una guía fundamental para el desarrollo del negocio de los propietarios desde el punto de vista de las IT. Nos provee de los controles adecuados y por tanto es una herramienta imprescindible.

Las líneas de trabajo de COBIT son una herramienta para el proceso del negocio y por tanto para los propietarios del mismo representan una facilidad y una clarificación de los pasos a dar.

En definitiva COBIT constituye una guía que seguir, genérica y orientada al propósito de contestar algunas de las preguntas que se suelen realizar en el desarrollo de los planes de contingencia: ¿Hasta dónde podemos llegar?, ¿Está el coste justificado en función del beneficio que obtenemos?, ¿Cuáles son los indicadores de un buen plan?, ¿Cuáles son los factores críticos del éxito?, ¿Cuáles son los riesgos de no conseguir nuestros objetivos?, ¿Qué hacen los demás?, ¿Cómo podemos compararlos?

Asimismo COBIT tiene una serie de herramientas donde se presentan lecciones aprendidas de aquellas empresas que rápidamente y exitosamente aplicaron COBIT en sus entornos de trabajo, hay dos herramientas particularmente útiles, una es Diagnóstico consciente de la gestión y otro es Diagnóstico de control de las IT, que nos asiste para analizar la organización del entorno de control de las IT.

Como sabemos en esta época los gestores de las organizaciones necesitan demostrar que han aumentado los niveles de control y seguridad. COBIT es una herramienta que representa ese espacio necesario de control y seguridad, asuntos técnicos y riesgos del negocio y comunicar este nivel de control a los responsables correspondientes. COBIT permite una evolución clara de las políticas y buenas prácticas para el control de las IT en las organizaciones de todo el mundo. En definitiva COBIT está diseñado para la herramienta de las IT que ayude a entender y gestionar los riesgos y beneficios relacionados con la información y todo el mundo de las IT en las organizaciones.

Líneas de trabajo de COBIT:

Gestión/Administración/Dirección: En esta parte se ha de decidir cuánto razonablemente podemos dedicar a la seguridad y control de las IT y cómo ponderar la inversión en control, y riesgos que frecuentemente son

impredecibles en el entorno de las IT. Mientras los sistemas de seguridad y control de la información nos provean de ayuda para los riesgos, no los eliminaremos. Ciertamente el nivel de riesgo nunca puede ser conocido con exactitud, siempre existe un cierto grado de incertidumbre. La dirección ha de decidir el grado de riesgo que es aceptable. Juzgar qué nivel puede ser tolerado en contraposición con el coste que puede generar, puede ser una decisión de gestión particularmente difícil. No obstante, la dirección necesita claramente unas líneas de trabajo generalmente aceptadas por las prácticas de control y seguridad de las IT.

Hay un gran incremento de la necesidad de los usuarios de que los servicios de las IT estén asegurados, a través de auditar los servicios de las IT provistos tanto internamente por la organización así como por terceras partes, que aseguren la adecuación del control y seguridad existentes. Normalmente ha habido algo de confusión a la hora de auditar los planes de contingencia de las organizaciones, la presencia de múltiples estándares o métodos como COSO, ITSEC, ISO 9000 ha provocado mucha confusión en el mundo del control de los planes de las entidades. Como resultado se puede decir que los usuarios necesitan de un estándar generalizado y versátil que sea establecido como primer paso para un control efectivo de la auditoría de un plan de contingencia. Frecuentemente los auditores han tomado la delantera en este tipo de esfuerzo de estandarizaciones internacionales porque se han visto continuamente confrontados con la necesidad de reforzar su posición y opinión en el control interno frente a la dirección.

Sin unas líneas de trabajo este es un cometido excesivamente complicado. No obstante los auditores son frecuentemente llamados proactivamente por la Dirección para consultar y advertir sobre cuestiones de seguridad y control de las IT.

ANEXO I

5. Objetivos del plan de contingencia y su control

Tiene que ser un proyecto estratégico de toda la organización.

Los recursos se encuentran en un entorno de incertidumbre que puede provocar interrupciones inesperadas del funcionamiento normal de la actividad de la empresa. Algunas de estas interrupciones en ocasiones son prolongadas y pueden llegar a afectar a la capacidad de funcionamiento de los servicios de la empresa, impidiendo su desarrollo normalizado. Es **objetivo** del plan de continuidad o contingencia prever las consecuencias de estas situaciones y definir estrategias que aseguren la continuidad de la actividad con el menor tiempo y trastorno posible.

Este plan asegura que todos los recursos conocidos y disponibles se utilizan para recuperar las funciones de la actividad tras una emergencia o desastre y proporciona un conjunto de procedimientos que serán ejecutados para restablecer los procesos prioritarios lo antes posible y con el menor impacto posible sobre la actividad, empleados, proveedores y clientes de la entidad. Es absolutamente necesario y premisa indispensable sobre la que radica la mayor importancia del plan, priorizar las operaciones de negocio críticas, evitar la dependencia sobre una persona o grupo de personas, eliminar la necesidad de desarrollar nuevos procedimientos durante la recuperación y minimizar la pérdida de información que se considere crítica; buscamos un umbral de funcionamiento y/o de parada mínima temporal de esas operaciones que nos permitan resolver la situación cuando exista una contingencia o interrupción.

Para la consecución de esto, un plan reducirá el número y magnitud de decisiones que se toman durante un período de contingencia; el plan establecerá, organizará y documentará los riesgos, responsabilidades, políticas, procedimientos y acuerdos con entidades internas y externas. Esto reducirá los efectos negativos ocasionados por un posible caos.

En definitiva el objetivo del plan de contingencia es definir las pautas generales para asegurar una adecuada recuperación de información y

servicios a través de una metodología definida para restablecer el procesamiento de los recursos críticos. De esa manera obtendremos los beneficios (que a continuación mencionaremos) y por lo tanto la supervivencia de nuestro negocio ante cualquier eventualidad.

Beneficios y objetivos del plan de contingencia ante interrupciones:

Minimizar las potenciales pérdidas económicas

Reducir riesgos potenciales

Reducir las probabilidades de que ocurran interrupciones

De producirse, reducir interrupciones en las operaciones (e identificar las condiciones que facilitan la interrupción de los servicios y que impactan sobre la continuidad de las operaciones)

Asegurar la estabilidad de la organización

Proteger los activos de la organización

Clasificar los activos para priorizar su protección en caso de desastre

Facilitar una recuperación ordenada

Minimizar las primas de seguros

Reducir la dependencia de ciertos elementos clave

Ampliar la seguridad del personal y de los clientes

Minimizar la necesidad de toma de decisiones durante un incidente

Minimizar las responsabilidades legales

Aportar una ventaja competitiva frente a la competencia

Fomentar e implicar a los recursos humanos de la empresa en la actividad de continuidad

Control en la fase inicial del plan:

Antes de nada y antes de entrar en materia en las fases de un plan de contingencia, en la auditoría de un plan de contingencia deberíamos hacernos primero las siguientes preguntas generales: ¿Existe un plan de contingencia? Y si es así nos deberíamos preguntar ¿Cuándo fue la última vez que fue actualizado?, ¿Cuáles fueron sus resultados?

La primera pregunta nos dice claramente si la organización se ha preocupado de tener el plan de continuidad del negocio, y las dos siguientes preguntas nos dan idea de, si efectivamente existiendo un plan, cuando fue la última vez que fue actualizado, si éste ha entrado ya o no en obsolescencia, y en función del tiempo que ha pasado sin renovarlo, darnos una idea del grado de implicación y preocupación de la organización respecto a los planes de contingencia y si estos son efectivos.

Podemos establecer que el objetivo general del programa de auditoría de un plan de contingencia en su fase inicial consiste en verificar la existencia de éste, que contempla un conjunto de procedimientos de actuación y de recursos necesarios para la restauración progresiva de los servicios en el caso de paralización de las actividades; en los que están involucradas todas las áreas, departamentos y servicios de la organización y que se mantienen debidamente actualizados, realizándose pruebas periódicas para su eficacia.

Otras preguntas pertinentes en este momento serían: ¿Existe una política que sustente el plan?, ¿Es Parte de un plan de recuperación y seguridad global?

La primera pregunta nos permite conocer si existe una política específica de plan de contingencia verdaderamente efectiva, la segunda nos da idea de la ubicación del plan dentro de un plan de seguridad global.

Estas preguntas son importantes y pueden ser consideradas como una toma de temperatura para lo que después venga dentro de la auditoría del plan de contingencia. Los planes de contingencia variarán en función de la naturaleza de la empresa y de su idiosincrasia pero buscan siempre el mismo objetivo que es la continuidad del negocio frente a eventualidades.

Estas preguntas que propugnamos en el inicio de la auditoría son generalistas y nos permiten atisbar ya desde un primer momento el grado de compromiso de la organización.

Como sabemos dentro de la auditoría podemos disponer de hasta tres líneas de defensa. En función de la necesidad podremos establecer que dentro del plan de contingencia y en función de la naturaleza de la fase en la que estemos: (control interno, auditoría interna) y todo ello revisado por la auditoría externa.

Para la consecución de todos estos objetivos se necesitará una auditoría o control para el plan de contingencia en sus diferentes fases; el objetivo de la auditoría o control sobre el plan de contingencia buscará que este plan sea efectivo y que no concurra en deficiencias ni tampoco en sobreestimaciones, buscamos un plan de contingencia adecuado a nuestras necesidades; lo encuadramos como una parte más de la auditoría informática general que deben tener todas las empresas para sus sistemas de información. En definitiva con la auditoría se busca que el plan de recuperación contribuya a la consecución de los objetivos del negocio y que, llegado el momento, funcionará como está previsto. Por lo tanto buscamos que no sea un plan deficiente, que sea adecuado y no incurra en errores graves que producirían pérdidas igual o mayores que de no tener un plan, pues no hay peor situación que creerse salvaguardado por un plan que en realidad no funciona.

El auditor del plan de contingencia tiene como objetivo comprobar los aspectos estructurales y formales (que veremos más adelante), y también:

- Que se han ejecutado en su momento los programas de entrenamiento, mantenimiento y pruebas que son pertinentes dentro del plan.
- Que tras la ejecución se han tomado las medidas correctoras adecuadas.
- Que todo ha sido informado a la Dirección por cada responsable.

Aspectos estructurales y formales:

Las preguntas se realizarían por una auditoría externa ya que deberían ser los auditores internos los que deberían haber advertido acerca de este plan cuando realizaron sus auditorías, los auditores internos en caso de no haber plan no lo habrían desarrollado y por lo tanto se les debería explicar la importancia de su implantación, de todas formas estas preguntas serían básicas y siempre se tienen que realizar al comienzo de la auditoría de un plan, para ver si los objetivos están centrados y son acordes con lo que busca la entidad. Los auditores internos ya deberían de haberse hecho estas preguntas en las revisiones pertinentes, pero es cuestión formal que el auditor externo las haga porque siempre puede ocurrir cualquier cosa.

La misión de la auditoría interna debe consistir en comprobar que en la política de seguridad de la entidad se contempla la existencia de planes de contingencia; que dichos planes están formalizados por escrito y aprobados por la Dirección, que los empleados tienen asignadas responsabilidades para su ejecución, los conocen y están preparados para realizarlos; que abarcan todos los ámbitos críticos de la empresa y que en función de dicho aspecto se ha establecido el orden de prioridad en la recuperación; y que tengan garantizada su actualización mediante revisiones y pruebas periódicas, otorgando con todo ello a la institución la capacidad suficiente para dar continuidad a las operaciones ordinarias dentro de los plazos previamente establecidos.

Como consecuencia de la necesidad de auditorías sobre el plan de contingencia, evaluaremos las fórmulas adecuadas que los auditores tanto internos como externos deben realizar a lo largo del desarrollo de un plan, por tanto iremos viendo a grandes rasgos las posibilidades y fases del plan, como se desarrolla, y como deberíamos proceder para el caso de su control y auditoría.

En el caso de COBIT en la fase inicial del plan nos daría y consideraría una serie de cuestiones de vital importancia:

Para alcanzar el éxito la dirección o guía de la empresa y la guía de las IT no pueden ser consideradas separadas ni de distintas disciplinas. Tradicionalmente se consideró que la guía o dirección de una empresa se centrara en un conjunto experto que nos permitiera aumentar nuestra productividad y que nos asegurara el funcionamiento y resistencia en

asuntos críticos. Las IT fueron consideradas únicamente para permitir llevar a cabo las estrategias empresariales, pero realmente deben ser parte integral de la estrategia empresarial.

La guía o dirección de las IT provee de una estructura que une procesos de las IT, recursos de las IT e información sobre las estrategias empresariales y objetivos de las mismas. La guía de las IT integra e institucionaliza los caminos óptimos para planificar, adquirir e implementar, desarrollar y proveer en definitiva visualizar la realización de las IT. La guía de las IT es parte integral del éxito de la dirección de una empresa asegurando efectividad y llevando a cabo una efectiva mejora en relación con los procesos propiamente empresariales. La guía de las IT permite a las empresas tener una completa ventaja en su información, maximizando beneficios, captando y capitalizando oportunidades y ganando ventajas competitivas.

ANEXO I-1

Las actividades empresariales requieren información de las IT para poder encontrar los objetivos del negocio. Las entidades u organizaciones exitosas aseguran la interdependencia entre sus planes estratégicos y sus actividades relativas a las IT. Las IT deben ser alineadas de tal manera que permitan a la empresa u organización tener una completa ventaja sobre su información maximizando los beneficios.

ANEXO I-2

La empresas están guiadas y dirigidas por una serie de prácticas generalmente bien aceptadas, para asegurar que la empresa está consiguiendo que sus éxitos están garantizados por cierto tipo de controles. Estos objetivos que se quieren conseguir emanan de la dirección, que es la que dicta las actividades de la empresa, utilizando la propia experiencia empresarial. Los resultados de las actividades de la empresa son informados proveyendo una entrada constante de revisión y mantenimiento de los controles, comenzando el ciclo de nuevo.

ANEXO I-3

De la misma manera las IT también son guiadas por las mejores prácticas, para asegurar que la información empresarial y la tecnología relacionada con ella están encaminadas de manera adecuada y pertinente hacia los

objetivos del negocio, que sus recursos son utilizados responsablemente y que los riesgos están gestionados apropiadamente. Estas prácticas forman la base de la dirección de las actividades relacionadas con las IT. Los informes están cuestionados en las actividades propias de las IT que han sido medidas frente a varias prácticas y controles volviendo el ciclo a comenzar de nuevo.

ANEXO I -4

Para asegurar que la gestión consigue los objetivos prefijados en nuestro negocio, debemos dirigir y gestionar las actividades relacionadas con las IT de una manera efectiva basculando entre la gestión de riesgos y la consecución de beneficios. Para la realización de esto necesitamos que la gestión de la auditoría de los planes de contingencia identifiquen las más importantes actividades para que sean verificadas. Por lo tanto es necesario hacer una evaluación del grado o nivel de maduración de la organización y valorándolo respecto a las mejores prácticas industriales y estándares internacionales. Para conseguir este tipo de gestión, COBIT y sus guías de gestión han identificado factores específicos críticos de éxito, indicadores clave, claves de verificación de indicadores y un modelo de madurez de la guía de las IT tal y como se presenta en el ANEXO I.

Por último indicar en esta fase una serie de definiciones que hemos venido utilizando:

Control: Lo definimos como las políticas, procedimientos, prácticas y estructuras organizativas diseñadas para proveer a nuestro plan de un razonable aseguramiento de que los objetivos de nuestro negocio serán alcanzados y acontecimientos indeseados serán prevenidos o detectados y corregidos.

Los objetivos del control de las IT: Se definen como la declaración del resultado deseado o propósito para ser conseguido implementando procedimientos de control en una actividad de las IT en particular.

La dirección o guía de las IT: Se define como estructura de relaciones y procesos para dirigir y controlar la empresa para conseguir éxitos en ella, mediante un valor añadido que es la valoración de los riesgos frente a retornar sobre las IT y sus procesos.

Hay dos tipos distintos de clases o modelos de control actualmente disponibles: “El modelo de control del negocio” y el más enfocado “Modelo de control de las IT”. COBIT propone cubrir el hueco existente entre ambos. COBIT está más posicionado para ser comprensivo para la gestión o dirección y operar a un nivel más alto que la gestión de las tecnologías de los sistemas de información. COBIT es el modelo de gestión de las IT.

El propósito básico que las líneas de trabajo de COBIT proponen es que el control de las IT sean aproximadas mirando la información que es necesaria para mantener los objetivos del negocio o sus necesidades, y buscando información que es resultado de la aplicación combinada de los recursos de las IT que deben ser gestionados por los procesos de las IT.

ANEXO I-5

El dinero o el capital no fueron considerados en COBIT como recursos para la clasificación del control de objetivos.

Después de ver los criterios de un estándar consolidado como es el caso de COBIT, a lo largo del desarrollo teórico iremos desarrollando un par de ejemplos continuos a lo largo del proyecto que nos permitan clarificar y concretar con practicidad la aplicación concreta de cada una de las fases donde se desarrolla el plan y su control. Comenzando en la siguiente fase. Como sabemos esta primera fase y su control es una primera toma de contacto con el plan de contingencia de una entidad y por tanto se revisan asuntos generalistas que nos permiten ir encaminando no solo que tipo de plan deberemos desarrollar sino qué puntos debemos revisar.

Pasamos a ver las diferentes facetas del plan de contingencia y las aplicaciones en forma de auditoría en sus diferentes fases.

6. Iniciación y gestión del plan de contingencia y su control

(Ayudar a la dirección en la fijación de objetivos y políticas; análisis del negocio, evaluación de riesgos e impacto y su auditoría)

Ayudar a la dirección en la fijación de objetivos y políticas:

En esta fase del plan pretendemos fijar objetivos y alcance del plan, fijar los requisitos de seguridad, estudiar los condicionamientos legales y realizar estudios de caso. Para ello hay que delimitar y definir bien las necesidades y las limitaciones de recursos, en definitiva tenemos que ser pragmáticos y sensatos, de esa manera obtenemos un equilibrio en el cual salga rentable la aplicación del plan. Hay que saber claramente para qué estamos planificando y para que NO estamos planificando mediante supuestos de partida. Como se puede definir en una frase: el objetivo no es la seguridad absoluta pues esta tendría un coste infinito.

El proyecto, puesta en vigor y mantenimiento de un plan de contingencia debe estar enmarcado en la política del plan general de seguridad de la organización, emanada de la alta dirección.

Es una labor de significativa envergadura y complejidad que debe estar sujeta a los correspondientes requisitos de planificación previa y rigor en su desarrollo. La falta de estos requisitos puede dar lugar a elaborar un plan que no cumpla o no satisfaga los objetivos para él establecidos y resulte ineficaz en el caso de tener que ponerlo en práctica ante una interrupción de las actividades.

Tiene que haber un compromiso de la dirección para poder llevar a cabo la aplicación del plan, si no el plan no puede llevarse a cabo.

Compromiso de la Dirección:

- El Plan establece procedimientos que obligan a todos los afectados.
- Son necesarios además unos recursos que generan unos costes que deben ser asumidos y aprobados por la Dirección.
- La experiencia demuestra que sin este compromiso de la Dirección un Plan de Recuperación no puede llevarse a cabo.

- Es responsabilidad de los niveles altos de la Dirección asegurarse de que la continuidad de las operaciones y funciones que realiza la organización está garantizada después de que ocurra cualquier incidencia que las interrumpa.

Alcance del plan:

El alcance y complejidad del plan, en cuanto a acciones, funciones y recursos que se deben contemplar estará determinado por el grado en el que las actividades ordinarias de la organización dependan del funcionamiento del centro de proceso de datos, y por el carácter crítico de algunas de las operaciones informáticas para el funcionamiento normal de la empresa.

- A veces, el Plan no se corresponde con las necesidades del negocio, siendo más bien un conjunto de procedimientos de operación que una Estrategia de Recuperación.

- El auditor (como veremos en el apartado de control de esta fase) comprobará que los objetivos y las medidas de recuperación se establecen para las Aplicaciones o Servicios Críticos aprobados por la Dirección.

En definitiva por todo lo anterior se puede concluir que los planes de contingencia son una estrategia planificada, integrada por una organización, unos procedimientos operativos y unos recursos (humanos, técnicos y logísticos), que tienen como objetivo la restauración eficaz de los servicios paralizados o degradados por cualquier contingencia o interrupción.

Por lo tanto es imprescindible conocer las funciones críticas de la entidad y analizar y establecer su respaldo posible, una a una, para poder realizar la restauración progresiva de las mismas en orden a su importancia.

En el siguiente párrafo es donde comienza el análisis de los diferentes aspectos que competen al negocio y su plan de contingencia. Fase de primordial importancia pues es necesaria una visión objetiva y completa de todos los aspectos concernientes al negocio, su conocimiento profuso y de las amenazas potenciales que puedan suponer un revés para nuestra entidad.

Análisis del negocio, Evaluación/Análisis de riesgos y su impacto:

Análisis del negocio: Se trata de obtener un conocimiento de los objetivos del negocio y de los procesos que se consideran críticos para el funcionamiento de una compañía. Una vez identificados los procesos críticos, se analizarán cuales son los riesgos asociados a dichos procesos para identificar cuáles son las causas potenciales que pueden llegar a interrumpir un negocio. De esa manera podremos acometer las acciones que nos permitan reducir o eliminar los riesgos detectados y que la activación del plan de continuidad se produzca como consecuencia de incidentes que han ocurrido a pesar de las medidas de protección adoptadas, es decir, incidentes con una probabilidad de ocurrencia sensiblemente menor. Se ha de tener en cuenta la probabilidad de manifestación de cada uno de los problemas posibles, de esa forma se podrán priorizar los problemas y su coste potencial desarrollando un plan de acción que será más adecuado. Por tanto, es imprescindible conocer las funciones críticas de la entidad y analizar y establecer su respaldo posible una a una, para poder realizar la restauración progresiva de las mismas en orden de su importancia.

Para fijar los objetivos, los requisitos etc. y analizar los riesgos e impactos de la materialización de las amenazas, necesitamos preguntarnos a grandes rasgos las siguientes preguntas: ¿Cuáles son las actividades más importantes para la compañía?, ¿Cómo afectaría económicamente una interrupción de los servicios a medida que va pasando el tiempo sin reanudar el servicio?, ¿Cuál sería la capacidad operativa a medida que pasa el tiempo?, ¿Cuál es el plazo máximo para volver a la normalidad sin llegar a incurrir en graves pérdidas?; de esta manera tenemos una cosmovisión de la naturaleza de la empresa y cuáles son sus necesidades más imperiosas en el momento de la contingencia o interrupción, eso siempre a grandes rasgos ya que todavía no hemos entrado en materia específica.

Las actividades que se clasifican como esenciales dentro de una compañía suelen ser en su mayoría las operacionales. Estos procesos interactúan directamente con los clientes o con otras entidades externas a la compañía, también es posible que estos procesos dependan de otros internos, que también deben ser analizados. Para conocer cuáles son las necesidades de la compañía en cuanto a estrategias de continuidad, vamos a utilizar dos mecanismos de análisis, (riesgos e impacto):

Análisis de riesgos: El objetivo es identificar y analizar los diferentes factores de riesgo que potencialmente podrán afectar a las actividades que queremos proteger. Hay que evaluar cuan mal podría ir la actividad y estimar el impacto que tendría. Y ver qué problemas podrían ocurrir para así priorizar cuáles serían los más grandes en coste e importancia para atacarlos de manera adecuada llegado el caso y mantener la continuidad o por lo menos minimizar el tiempo de interrupción.

En esta fase se analizan las amenazas más probables para la organización y el riesgo o probabilidad de que estas amenazas se materialicen causando la interrupción de las operaciones. Es decir, es necesario realizar un análisis de riesgos y acometer acciones que se deriven del mismo con objeto de

reducir o eliminar los riesgos detectados y que la activación del plan de continuidad del negocio se produzca como consecuencia de incidentes que han ocurrido a pesar de las medidas de protección adoptadas, es decir, con una probabilidad de ocurrencia sensiblemente menor, pero no por ello menos desdeñables.

El análisis de riesgo permite calcular un indicador ligado al par de valores, también calculados, de la vulnerabilidad y el impacto, ambos derivados a su vez de la relación entre el activo y la amenaza, para decidir si dicho riesgo es asumible o aceptable. Existen diversas metodologías para evaluar o cuantificar un riesgo normalmente se suele adoptar una medida para ello denominada Expectativa de Pérdidas Anualizadas, que se obtiene multiplicando las pérdidas producidas por un determinado evento, por el número determinado de veces que un evento se produce a lo largo de un año. Fruto de esta decisión y con objeto de reducir el riesgo surge un conjunto de acciones que vendrían a constituir la "Función de salvaguarda", que se materializa en el correspondiente "Mecanismo de salvaguarda" o conjunto de procedimientos o dispositivos que reducen el riesgo y que opera de dos formas posibles:

- Neutralizando otra acción: la amenaza.
- Modificando el estado de seguridad del activo agredido o afectado con reducción posterior al evento productor de dicho impacto.

Estas funciones y mecanismos de salvaguarda se clasifican en función de su forma de actuación de dos maneras:

Preventivos: que actúan sobre la vulnerabilidad de los activos y reducen la potencialidad de materialización de la amenaza. Salvaguardas preventivas serían por ejemplo la detección preventiva o por ejemplo la información y formación del personal que permite una menor incidencia de errores y una mayor dotación de formación con la consecuente reducción de fallos y la mayor diligencia en las operaciones.

Restablecedores: Que actúan sobre el impacto y reducen su gravedad. En este caso el mecanismo de salvaguarda más importante es *el plan de contingencia y continuidad.*

Con más o menos variantes, todas las metodologías cuantitativas del riesgo que se han desarrollado a lo largo del tiempo están basadas en el mismo razonamiento, pero normalmente se tiene en cuenta que en un riesgo existen esta serie de elementos, que nos permitirán posteriormente evaluarlos en mejor medida:

Valor de los activos: Valor de cualquier propiedad de la entidad, cuantificado normalmente en términos económicos. Primeramente los tendremos que identificar y posteriormente cuantificar.

Frecuencia de la amenaza: Número de veces que es esperable la manifestación de un suceso, durante un año normalmente. Como en el caso de los activos, habrá que identificarlos y posteriormente evaluar su probabilidad de ocurrencia y el impacto de su materialización.

Impacto de la amenaza: La medida del daño o coste resultante como consecuencia de la materialización de una amenaza, expresado en porcentaje del valor del activo dañado. Se identificarán mediante las amenazas asociadas y determinaremos su valor para calcular junto con los demás parámetro el riesgo que conlleva cada amenaza.

Eficacia de las medidas de seguridad adoptadas y su coste: no solamente el de implantación, sino el de mantenimiento, reposición y adaptación a las necesidades cambiantes. Cuantificado en términos económicos.

Incertidumbre: Característica típica del riesgo, basada en el grado de confianza en las cantidades aplicadas a los ejemplos anteriores.

Con estos puntos se ve que la evaluación cuantitativa del riesgo depende en mayor o menor medida de un factor de incertidumbre. En algunos casos es fácilmente cuantificable, pero cuando se trata de evaluar o discernir la frecuencia de una amenaza no queda más remedio que tirar de estadísticas para evaluar de una manera más o menos fiable su probabilidad de aparición. Aunque en España, al existir una baja experiencia en este sector, hemos de decir que la aplicación de estadísticas no es del todo fiable, ya

que no existe una tradición de seguridad muy dilatada en el tiempo con respecto a los planes de contingencia.

Resulta imposible garantizar que no ocurran hechos imprevistos que provoquen desastres, por lo que una de las finalidades de estos planes consiste en minimizar la ocurrencia de éstos, así como tener definida y poner en marcha la organización necesaria para aplicar las acciones, procedimientos y recursos para la vuelta a la normalidad en el menor tiempo posible.

El análisis de riesgos pretende poner de relieve aquellas debilidades actuales que por su situación o importancia pueden poner en marcha un plan de contingencia antes de lo deseable. El análisis de riesgos debe centrarse en los procesos críticos aunque puede extenderse a los que no lo son, y de esa manera priorizarlos para actuar adecuadamente.

Las tareas inherentes a la realización del análisis de riesgos, y en general de cualquier trabajo de revisión del plan requieren el concurso de profesionales especializados con conocimientos actualizados y con una experiencia lo más variada posible para poder ajustar las soluciones y recomendaciones a cada caso particular concreto.

Existen diversas metodologías para llevar a cabo el análisis de riesgos, los objetivos de éstas serían estudiar los riesgos que soporta un sistema informático y su entorno asociable, y recomendar las mediadas apropiadas que deberían adoptarse para conocer, prevenir y reducir los riesgos investigados.

Los elementos metodológicos en este caso nos aportan una cierta estandarización que nos permite comparar con otras experiencias anteriores y también con las de otras entidades, entre estas metodologías estarían:

MARION: Es una metodología de análisis que permite evaluar el nivel de seguridad de una organización a través de cuestionarios ponderados con el objetivo de obtener una visión de la organización con relación a un nivel considerado óptimo, comparándolo con la situación estadística de otras organizaciones que ya hayan realizado el mismo análisis. A partir de este método se obtiene una radiografía objetiva y cuantitativa de la situación, que se representa de forma gráfica: diagrama polar (vulnerabilidades

relativas) y diagrama referencial (gravedades relativas). Según el autor Juan Gaspar Martínez, y a pesar de su dilatada presencia en el mundo de la evaluación de riesgos desde los años 80, ha mantenido su vigencia sin más que actualizar sus cuestionarios, de esta manera se revela como uno de los métodos más versátiles y estandarizados aparte de graficarlo de una manera que es fácilmente evaluable a simple vista, lo cual es bastante bueno y reseñable para el auditor que se acerque a evaluar el plan de contingencia a través de la metodología de evaluación de riesgos.

Otros métodos a reseñar serían:

MAGERIT: Maneja tres submodelos, el de elementos de seguridad (actividades, amenazas, vulnerabilidades, impactos, riesgos y salvaguardas), el de eventos de seguridad (estático, dinámico organizativo y dinámico físico) y el de procesos (planificación, análisis de riesgos, gestión de riesgos y gestión de salvaguardas). Como punto a su favor indicar que está muy extendido en la Administración Pública Española con lo cual podría ser favorable para auditorías de este tipo de organismos en cuanto a comprarlo con otras experiencias en las diferentes Administraciones del Estado.

Otros dos que existen (de los muchos que hay) pero de los que no hablaremos son: MEHARI y OCTAVE.

Es imprescindible en la fase de análisis de riesgos la identificación de los activos (como ya hemos indicado) que pueden ser vulnerados, más adelante en este trabajo veremos la identificación de las amenazas, su impacto y sus consecuencias sobre los activos a través de las vulnerabilidades.

Identificación de activos: Para cada uno de los procesos críticos de la compañía es necesario realizar un inventario de los activos involucrados en el proceso. Los activos son los recursos de la compañía para poder llevar a cabo la realización de sus tareas de explotación de la información y por lo tanto para cumplir sus objetivos como negocio. Activos para una entidad podrían ser: Equipamientos, información, conocimiento, sistemas.

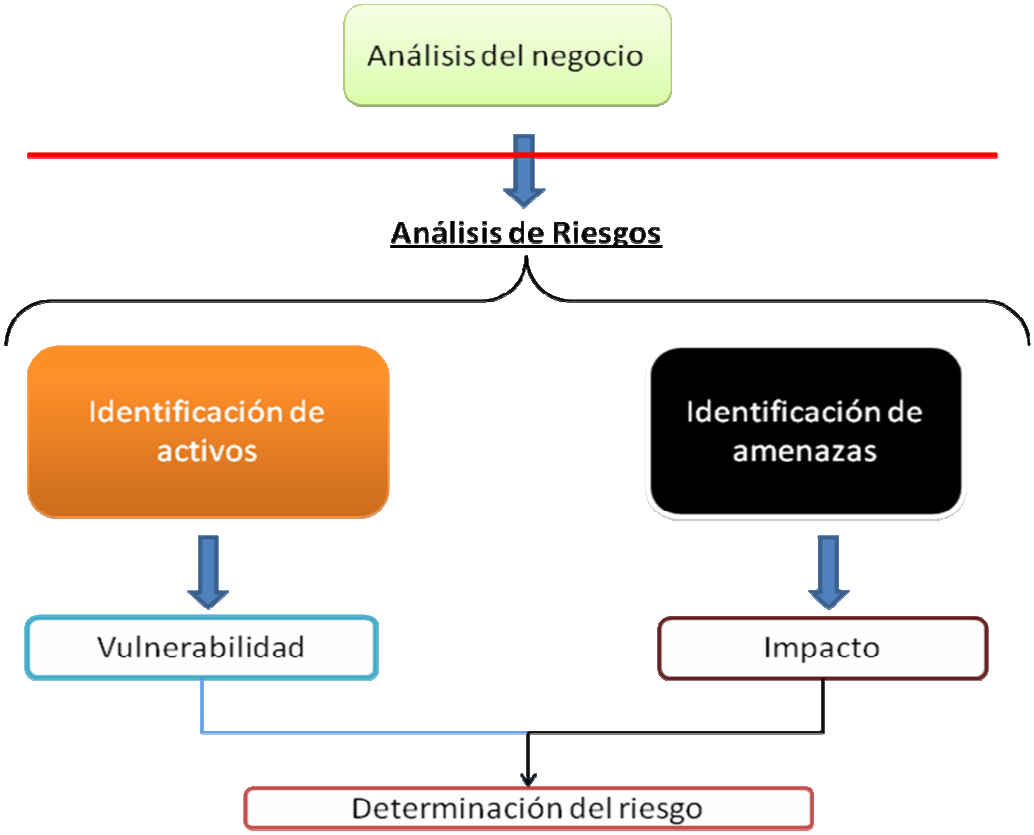
Como hemos indicado anteriormente cada activo tendrá unos costes asociados, en algunos casos cuantificables económicamente y en otros casos de una manera más sutil como por ejemplo la fiabilidad de los servicios que prestamos. El inventario de los activos es fundamental y en él

se reflejarán los responsables, valor, localización y factores alterantes e impacto sobre él (esto cuando se realice la identificación de amenazas y su impacto sobre el activo, se asociarán al inventario para conocer con claridad todo lo que afecta a dicho activo).

Identificación de amenazas: La identificación de tales sucesos debe ser realista. No sería práctico realizar una identificación de una amenaza que probablemente no ocurra nunca y que por tanto añadiría un sobrecoste; por lo tanto aportar recursos contra amenazas remotas no sería rentable así el plan de contingencia no debería adoptar medidas que serían innecesarias.

A la hora de evaluar la probabilidad de ocurrencia de una amenaza siempre es más complicado determinar las de origen humano que las naturales, no obstante el factor no es nada desdeñable ya que en ocasiones representan un porcentaje importante de los incidentes en una organización y deben ser tenidos en cuenta, sobre todo de la mano de empleados descontentos, ex-empleados etc.

Como hemos visto, una amenaza es un evento que puede desencadenar un incidente dentro de la organización produciendo tanto daños materiales como pérdidas inmateriales. Las amenazas pueden provenir de diversas fuentes como agresores malintencionados, amenazas no intencionadas, desastres naturales, errores etc.



Determinación de vulnerabilidades: Las vulnerabilidades son situaciones desfavorables que se producen en los activos como consecuencia de la naturaleza de éstos y la esencia cambiante de las amenazas del mundo circundante. Por lo tanto un elemento que hoy no tiene porqué ser vulnerable mañana podría serlo por la misma naturaleza evolutiva de los sistemas de información. La vulnerabilidad se crea en función del mundo que nos rodea y se modifica en función de las acciones que llevemos a cabo para anularla o reducirla lo máximo posible. Evidentemente las amenazas aprovecharán las vulnerabilidades de los activos para crear un impacto que puede ser más o menos grave, es nuestra función determinar el riesgo asociado a la conjunción de estos factores para adoptar, como ya hemos reseñado en más de una ocasión, las medidas más pertinentes y prioritarias para salvaguardar nuestros activos y por extensión nuestra organización.

Las vulnerabilidades son debilidades que pueden ser explotadas por las amenazas, en sí mismas no afectan negativamente pero sí pueden permitir la actuación perniciosa de las amenazas. Una forma efectiva de determinar la vulnerabilidad es preguntándose el tipo de amenaza que puede afectarnos y si existe alguna medida pertinente para proteger el activo o si por el

contrario no existe nada para evitarlo o ni siquiera se ha considerado. Las vulnerabilidades no han de ser consideradas ya de por sí solamente por el plan general de seguridad sino también porque son decisivas a la hora de la aplicación del plan de contingencia.

Toda afección susceptible de entorpecer o afectar negativamente las labores de la entidad en el día a día también les afectarán cuando se aplique un plan y con más intensidad pues la situación será de emergencia y las trabas en momentos de criticidad orgánica aumentan su poder "destructivo" en términos de eficiencia e integridad. Como hemos dicho las vulnerabilidades determinarán junto con las amenazas el impacto que se puede producir y el riesgo o probabilidad de que se materialice esa amenaza, por lo tanto la vulnerabilidad en este caso se manifiesta como piedra angular de nuestra visión del análisis de los riesgos y de la acometida de medidas efectivas dentro del plan de contingencia.

Ejemplo: Rotura de cableado eléctrico, pregunta pertinente en este caso sería ¿Existe un mantenimiento adecuado de la infraestructura del edificio en términos técnicos?

Evidentemente esta situación representa una vulnerabilidad ya de por sí para la entidad, pero en un momento de emergencia en el que se conjuntan varias amenazas que azotan a la entidad puede ser crítico, por tanto este tipo de preguntas en torno a las vulnerabilidades serían primordiales para la visión de las medidas pertinentes no solo ya en la elaboración del plan sino también en la realización del control en esta fase. De hecho en esta pregunta se plantea una cuestión que podría ser uno de los resortes que desencadenarían la puesta en marcha de un plan de contingencia ya que el corte de suministro eléctrico supondría la paralización total de nuestra operatividad y habría que llevar a cabo las medidas pertinentes (cables de reserva, generadores eléctricos, etc.), para restaurar la operatividad de la entidad.

Cuanto más detallado sea el análisis tanto más certero será el diagnóstico de las amenazas y vulnerabilidades posibles y por tanto más eficaces serán las medidas (no incurriremos en medidas innecesarias), adoptadas para la protección de la información. También sería muy necesario y claramente favorecedor que las amenazas estén clasificadas por orden de importancia en función del daño que puedan hacer y de esa manera priorizar la serie de

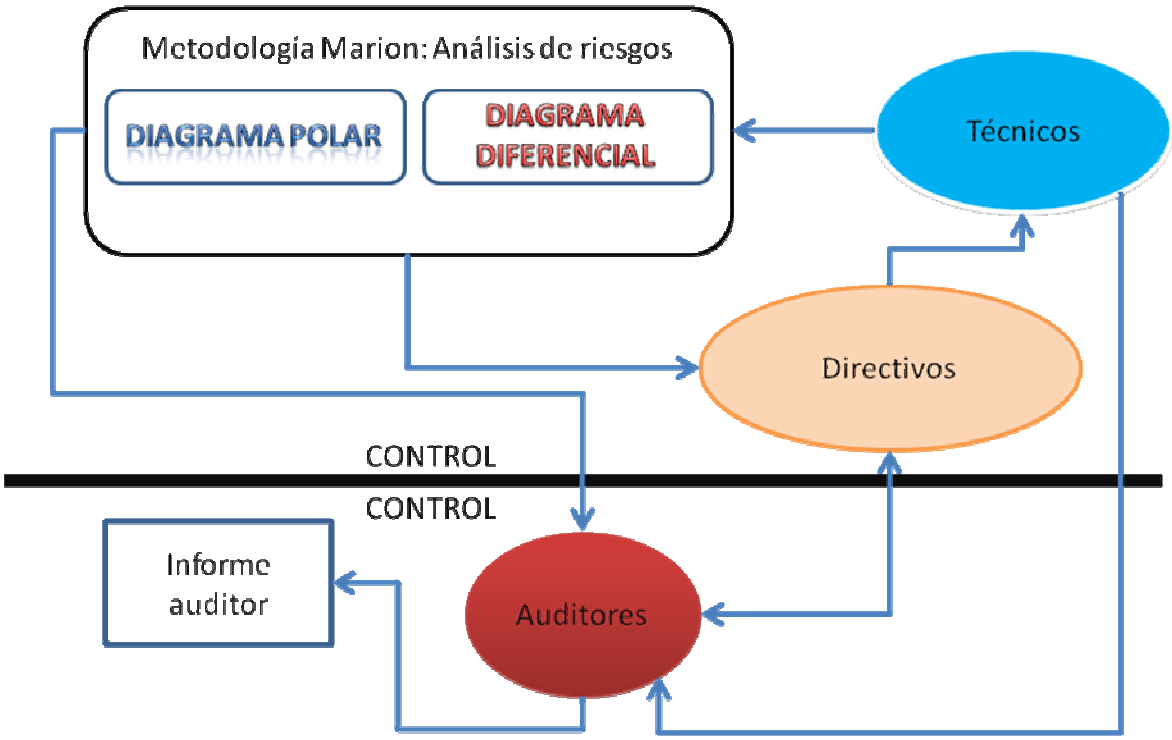
acciones a realizar por el plan de contingencia a la hora de implantar soluciones. Asimismo las vulnerabilidades deben ser priorizadas en cuanto a su supresión o disminución en función de la importancia de la debilidad que pueden representar en nuestra organización.

En este caso la metodología MARION se reveló como muy efectiva, y de la que haremos esta breve reseña; su metodología de análisis permite evaluar el nivel de seguridad de una organización a través de cuestionarios ponderados con el objetivo de obtener una visión de la organización con relación a un nivel considerado óptimo, comparándolo con la situación estadística de otras organizaciones que haya realizado el mismo análisis. De ahí se deduce una radiografía objetiva y cuantitativa de la situación, que se representa en la práctica de forma gráfica: diagrama polar (vulnerabilidades relativas), y diagrama diferencial (gravedades relativas). Estos gráficos nos darán una idea muy aproximada de cómo proceder en cuanto a vulnerabilidades y amenazas se refiere. El informe pertinente permitirá a la dirección de la organización tener la información suficiente para adoptar las medidas oportunas con el asesoramiento de los técnicos y auditores internos, a través de los diferentes niveles de riesgo que en función de los informes se procederá de alguna de las siguientes maneras:

- Transferir riesgo mediante la contratación de pólizas de seguros o proveedores de servicios.
- Eliminar riesgo mediante la adopción de las acciones recomendadas en el informe.
- Reducir el riesgo en los casos en los que su eliminación sea inviable.
- Aceptar el riesgo cuando la probabilidad de ocurrencia sea muy baja, o el coste de las medidas para eliminarlo o reducirlo sean inabordables.
- Una combinación de todas ellas.

Las amenazas tendrán una probabilidad de ocurrencia que dependerá de la existencia de una vulnerabilidad que pueda provocar su materialización en un incidente. Un ejemplo factible sería que una amenaza como una inundación tendría más probabilidad de ocurrencia en un edificio situado

en una vega que un páramo alto, por lo tanto el riesgo por daño de inundación es mayor en la vega (sería una vulnerabilidad), que en un páramo. Por lo tanto a la hora de determinar un riesgo siempre la conjunción de factores, vulnerabilidad e impacto asociadas al activo y la amenaza respectivamente nos mostrarán la realidad de la seguridad en la entidad y su forma de abordarla, incluso nos permitirán priorizar acciones en el plan de contingencia para ser más efectivos.



Dentro de un catálogo de amenazas posibles, podemos mostrarlas según el patrón utilizado por la metodología MAGERIT de este modo vemos las diferentes amenazas y el esquema que sigue esta metodología de análisis de riesgo en cuanto a identificación de amenazas y vulnerabilidades:

Grupo A, Accidentes:

A1. Accidente físico de origen industrial: incendio, explosión, inundación por roturas, daños por industrias cercanas o emisiones radioeléctricas.

A2.Avería: de origen físico o lógico, debida a un defecto de origen o sobrevenida durante el funcionamiento

A3.Accidente físico de origen natural: riada, fenómeno sísmico volcánico, meteoro, rayo, corrimiento de tierras, avalancha, derrumbe, etc.

A4. Interrupción de servicios o de suministros esenciales: energía, agua, telecomunicación, fluidos de suministros diversos.

A5. Accidentes mecánicos o electromagnéticos: choque, caída, cuerpo extraño, radiación, perturbación electrostática.

Grupo E, Errores:

E1. Errores de utilización ocurridos durante la recogida y transmisión de datos o en su explotación por el sistema.

E2. Errores de diseño existentes desde los procesos de desarrollo del software.

E3. Errores de ruta, secuencia o entrega de la información en tránsito.

E4. Inadecuación de monitorización, trazabilidad, registro del tráfico de información.

Grupo P, Amenazas intencionales presenciales:

P1.Acceso físico no autorizado con inutilización por destrucción o sustracción.

P2. Acceso lógico no autorizado con intercepción pasiva simple de la información (solo lectura).

P3. Acceso lógico no autorizado con alteración o sustracción de la información en tránsito o de configuración; lo que conlleva reducción de la confidencialidad del sistema para obtener bienes o servicios aprovechables (programas, datos).

P4.Acceso lógico no autorizado con corrupción o destrucción de información en tránsito o de configuración.

P5.Indisponibilidad de recursos, sean humanos (huelga, abandono, rotación) o técnicos (desvío del uso del sistema, bloqueo), sabotaje interno.

Grupo T, Amenazas intencionales de origen remoto:

T1. Acceso lógico no autorizado con intercepción pasiva.

T2. Acceso lógico no autorizado con corrupción o destrucción de información en tránsito o de configuración (requiere lectura y escritura) usando o no un reemisor o ”man in the middle”; es decir , reducción de integridad y disponibilidad del sistema sin provecho directo (sabotaje inmaterial, infección vírica).

T3. Acceso lógico no autorizado con modificación (intersección, repetición) de información en tránsito.

T4.Suplantación de origen (del emisor o reemisor) o de identidad.

T5.Repudio del origen o de la recepción de información en tránsito.

Evidentemente todo este tipo de amenazas podrían ser clasificadas de una manera más simple como naturales, accidentales e intencionadas. Y como es obvio cada amenaza puede llevar asociadas vulnerabilidades que le permitan manifestarse con mayor o menor intensidad. A estas, a grandes rasgos y como adición podríamos reseñar las siguientes.

Vulnerabilidades:

- Ausencia de un plan de Recuperación de incidentes, esta sería una de las vulnerabilidades más perniciosas de no contar con un plan adecuado.

- Personal sin formación adecuada

- Incumplimientos legales (LOPD, etc.)

- Definición de privilegios de acceso inadecuados. Sería una puerta para la materialización de un montón de amenazas.

- Protección física de equipos inadecuada.

- Ausencia de mecanismos de cifrado de datos para la transmisión de datos confidenciales.

- Descarga incontrolada y uso de software de internet.

- Carencia de software antivirus.

- Ubicación física en un área susceptible de desastres naturales.

- Ausencia de mecanismos de identificación y autentificación.

- Ausencia de control de cambios eficiente.

- Ausencia de backups, imprescindible realizarlos: representaría una gran vulnerabilidad su ausencia.

- Ausencia de un sistema de extinción de incendios automática.

- Ausencia de política de seguridad.

- Firewalls inadecuados.

- Ausencia de mantenimiento.

- Suministro eléctrico inapropiado, alternativas a la paralización eléctrica.

- Ancho de banda inadecuado.

- Cableado inapropiado.

- Existencia de materiales inflamables.

Por último determinaríamos el valor del impacto que un incidente tiene como consecuencia de la materialización de una amenaza. El impacto es imprescindible de tomar en cuenta a la hora de evaluar riesgos por tanto habrá que evaluarlo y para ello habrá primeramente que analizar qué posibles impactos pueden llegar a producir las amenazas y seguidamente cuantificarlos para determinar el posible riesgo. Para ello determinaríamos un análisis de impacto.

Análisis de impacto: La determinación del impacto en caso de interrupción en un activo o actividad nos dará el grado de repercusión de este impacto en la organización y eso nos permitirá determinar la urgencia de la recuperación de cada función del negocio; una interrupción no tendrá el mismo impacto si afecta a una u otra área de la entidad incluso la misma interrupción tendrá un impacto diferente en función del momento en que se manifieste.

El análisis de impacto nos permitirá obtener la información necesaria para que la dirección en función de los datos pueda adoptar una estrategia de recuperación adecuada a las necesidades de la entidad, que en principio dará continuidad a las actividades críticas y posteriormente al resto si es posible. Para la consecución de este objetivo el análisis de impacto debe determinar el grado de criticidad de las funciones o actividades y que estas sean la razón de ser de la organización en cuanto a plan de contingencia se refiere, de manera que se determine el tiempo máximo de admisibilidad de una interrupción, y cuál sería el umbral a partir del cual sería inadmisible el tiempo de interrupción.

Pasos a seguir en el análisis de impacto:

Definir tipos de impacto: Jurídico, comercial, de imagen, sistemas de información, etc.

Identificación de las funciones o relación de procesos de la organización y sus interdependencias. Ello nos permitirá saber qué funciones o procesos son los primordiales de mantener cuando se activa el plan de contingencia.

Identificación de la relación de aplicaciones que soportan los procesos de la compañía.

Identificación del impacto causado a la organización por la interrupción de cada una de ellas.

Identificación de los departamentos de la empresa y el nombre de las personas responsables que componen e intervienen en las funciones o procesos.

Identificación de entre los procesos, los que son críticos; dentro de estos se considerarían dos baremos, el cualitativo: los procesos que son críticos porque su ausencia supondría un impacto alto en la actividad de la compañía, y el cuantitativo: que supondrían las pérdidas económicas por la ausencia de los procesos.

Umbral máximo de interrupción: Es el límite en el tiempo en el cual las pérdidas sufren un aumento significativo y las funcionalidades o procesos que las implementan no podrían ser restablecidas a partir de ese momento.

Informar a la dirección de los resultados del análisis para que pueda fijar prioridades, definir cuáles son las funciones consideradas prioritarias y establecer los umbrales máximos de recuperación para cada una de dichas funciones.

Identificar los recursos mínimos necesarios para una recuperación satisfactoria de las funciones identificadas como críticas.

Tipos de impacto: El impacto es una consecuencia negativa de la interrupción de algún/os proceso/s de la organización durante un tiempo. Pueden ser de diversos tipos:

-Pérdida de ingresos: En organizaciones mercantiles cuya razón de ser es generar ingresos, el flujo de los mismos debe continuar si no se quiere poner en riesgo su existencia, por lo tanto es importante evaluar con exactitud los impactos. Su valoración será siempre cuantitativa.

-Incremento de costes: Las Interrupciones pueden generar un aumento de costes o gastos de la organización, como pérdida de productividad, multas, falta de control etc. Su valoración también debe ser cuantitativa.

-Peligro personal: Funciones que si no se desempeñan de forma adecuada pueden suponer un peligro para las personas. Hay que establecer criterios objetivos y su cualificación puede ser cuantitativa o cualitativa.

-Impacto operacional: Funciones que afectan al funcionamiento de la organización y su ausencia puede afectar al correcto funcionamiento de

otras funciones. Su criterio de valoración será cualitativo, aunque en muchas ocasiones podrá ser cuantitativo.

-Impacto Comercial: La interrupción de una función tiene repercusiones en las relaciones con los clientes, estos pueden entender la interrupción por incidentes graves, pero si la interrupción es prolongada puede ocurrir: que el cliente se vea forzado a cambiar de proveedor, que las ventas durante la interrupción no se recuperen nunca, que si se presta un servicio público tengamos responsabilidades jurídicas y generar desconfianza en los ciudadanos; el criterio de valoración será cuantitativo.

-Otros impactos reseñables que afectarían a la entidad serían: Funciones cuya interrupción afecta al control de calidad de los servicios o productos entregados (cuantitativo); Funciones cuyo impacto deteriora la imagen de la organización (cualitativo, y cuantitativo a medio plazo); Incumplimiento de obligaciones jurídicas como consecuencia de la interrupción de funciones, impacto ambiental etc...

Identificación de procesos: Existen procesos operativos (relación directa con el cliente: comercial, almacenaje, facturación etc.), y procesos de soporte (aquellos que facilitan los recursos para poder realizar los procesos operativos). Es esencial establecer un marco en el que se desarrollará el trabajo: debe enfocarse en el contexto de los servicios proporcionados por la organización, la evaluación de la contribución aportada por cada proceso y análisis de recursos mínimos que deben ser realizadas por responsables y personal de las áreas operativas pues estarán mejor preparados para identificar cuáles son los recursos más idóneos para conseguir una recuperación satisfactoria en los tiempos marcados como objetivo.

Para la identificación de las aplicaciones y sus consecuentes procesos se deberían utilizar una serie de cuestionarios normalizados, con instrucciones y unos criterios de valoración homogéneos.

Cada aplicación tendrá una serie de impactos en diferentes elementos de los sistemas de información de una compañía. Software de base que sustenta los sistemas operativos y sistemas de información de la empresa; software de gestión de aplicaciones empresariales; infraestructuras que permiten la

cumplimentación de estos sistemas y por último los recursos hardware que sustentan los sistemas de información.

Un ejemplo de quienes evalúan y como asignamos las tareas de evaluación lo encontramos en los siguientes cuadros, estos formularios nos servirán para conocer a fondo en identificar impactos, procesos, responsables, etc., de todas las áreas que incumben al análisis de impacto:

Nombre	**Puesto**	**Área de responsabilidad**
Fernando	Director	Área de seguridad
Luis	Empleado	Aplicaciones de gestión
María	Responsable	Departamento de marketing
…		

Los empleados reportarían información, los responsables y directores nos reportarían evaluación en función del estudio de los empleados de su área.

En el siguiente cuadro-formulario estableceríamos la identificación de procesos, las interdependencias, los responsables que cubren los procesos descritos y su frecuencia. Nos permitirá conocer mejor los procesos y sus interdependencias:

Función o Proceso:				
Procesos que dependen:				
Nombre de la Función:	*Departamento responsable:*	*Breve Descripción:*	*Frecuencia (diaria, semanal, mensual):*	*Persona responsable:*

Por cada proceso estableceremos una serie de datos identificativos que nos permitirán ver una serie de datos primordiales de cada proceso, su criticidad, su responsable, su presencia etc.; Que nos permitirán saber hasta qué grado su afección impactará en nuestra organización, o qué otros elementos de software o hardware les pueden afectar.

Cuadro del proceso:

Nombre del sistema	**Descripción**	**Criticidad**	**Tipo de sistema**	**Nº de equipos con la aplicación**	**Responsable**

Hardware del Proceso: Nos indica la interacción con el hardware de cada proceso, de esta manera sabremos si este es afectado y qué procesos pueden verse alterados o interrumpidos.

Tipo de hardware	Detalles del modelo	Distribuidor	Criticidad	Localización

Otros activos del proceso: Son activos que sin estar directamente relacionados sirven para el funcionamiento de uno o más procesos y por tanto pueden afectar al rendimiento de cada proceso. Lo describiríamos con el siguiente cuadro:

Descripción	Criticidad	Tipo de sistema	Localización

El cuadro que sigue sería el reflejo del tipo de impacto posible que cada uno de los procesos podría infringir si sufriese interrupción, por cada

proceso se establecería qué impactos produce y su magnitud que se evalúa por el tiempo de interrupción del mismo:

	Magnitud del Impacto					
Tipo de impacto	4 horas	1 día	1 sem.	1 mes	Peor día	Peor mes del año
Pérdida de ingresos						
Pérdida de beneficios						
Impacto en cash flow						
Incremento de costes o gastos						
Peligro para las personas						
Impacto operacional						
Impacto comercial						
Pérdida de calidad						
Impacto en la imagen						
Incumplimiento de obligaciones legales						
Impacto ambiental						
Desmoralización del personal						

Por último y en función del tiempo y naturaleza del impacto otorgamos una calificación del impacto a cada proceso en función de esos dos parámetros a cada proceso:

Un Día					
Proceso	Impacto	Leve	Medio	Grave	Catastrófico
A	Comercial	X			
B	Comercial y Operacional		X		
C	Económico		X		
D	Ambiental	X			

Una Semana					
Proceso	Impacto	Leve	Medio	Grave	Catastrófico
A	Comercial		X		
B	Operacional				X
C	Económico				X
D	Ambiental y	X			

	Comercial				

Un Mes					
Proceso	Impacto	Leve	Medio	Grave	Catastrófico
A	Comercial			X	
B	Operacional		X		
C	Económico			X	
D	Ambiental	X			

También realizaremos cuadros, con el tiempo máximo de interrupción tolerable por cada proceso, eso nos dará una idea no solo de su criticidad sino del orden que deberemos seguir estratégicamente en función del aguante operacional o funcional de cada proceso, y del orden de aparición de interrupción de cada unos de ellos.

Proceso	**Necesidades de recuperación**	**Criticidad**
Gestión pedidos	2-3 días	1
Gestión Stock	4 días	2
…	…	…

A partir de estos formularios y con toda la información recopilada de los procesos, podremos establecer una serie de prioridades para los procesos en función de su criticidad derivada del impacto que puedan tener y de las interdependencias con otros procesos a los que puedan afectar; Como hemos visto en el último formulario en función de una serie de parámetros podemos atisbar cuales serán los de mayor impacto y por tanto más críticos a la hora de tener en cuenta la recuperación de la funcionalidad de la entidad.

También hay que tener en cuenta aquellos procesos que en un inicio pueden tener un impacto leve pero la gravedad de su impacto puede crecer de manera exponencial con el tiempo. Determinar la valoración de pérdidas no es una cuestión sencilla, pero una vez determinados los procesos que deben ser objeto de recuperación preferente, podemos valorar en función de algunos criterios su valor. Como dijimos en la descripción de los tipos de impacto, en la valoración de los impactos estos podrán ser cuantitativos o cualitativos y en función de esta valoración el cuadro anterior nos dirá la gravedad o no del impacto de cada proceso.

Con todo esto se podrán tomar decisiones al respecto y se podrá escalar la recuperación de los procesos en función de su importancia. Mención aparte merece la repercusión de los recursos limitados para la recuperación, que obligará a asumir unas determinadas pérdidas en caso de incidente. Tendremos por tanto que ver la importancia del proceso por un lado, su impacto y las pérdidas por omisión de tratamiento de procesos también críticos pero que no son atendidos en el momento del proceso prioritario. Recuperar todo en un momento determinado no es posible y provocaría el colapso de la organización.

Una vez visto esto debemos establecer los tiempos de recuperación, tendremos que realizar una estimación del tiempo en que cada proceso

crítico tardará en recuperarse y a partir de qué tiempo puede suponer un daño grave para la empresa.

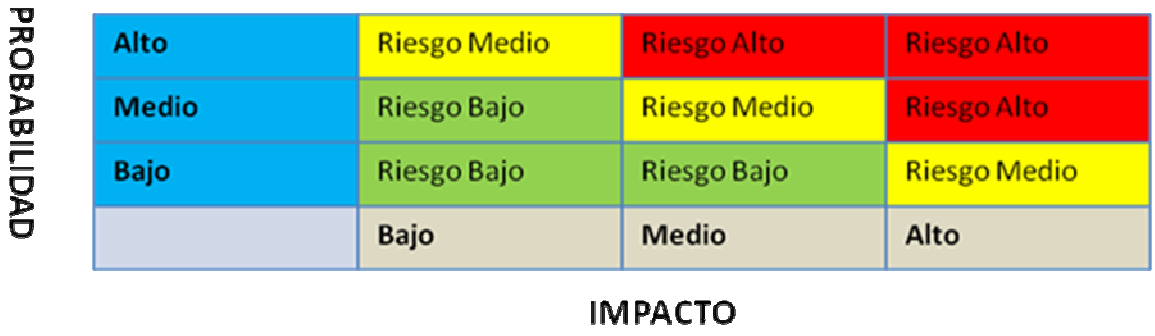
Con todo esto se aprobará un marco de actuación en el tiempo ante un posible incidente, las prioridades de los procesos, sus estimaciones de tiempo de recuperación, etc. que nos permitirán actuar de la manera acordada rápidamente ante un evento de interrupción.

Análisis de riesgos e impacto (síntesis):

Por último y después de ver los análisis de riesgos e impacto en sus diferentes facetas, podremos establecer la conjunción de ambos para establecer el verdadero riesgo de cada incidente en la organización. De esta manera después de ver en el análisis de riesgos las diferentes amenazas y las vulnerabilidades de los activos, podremos calcular con estos dos parámetros la probabilidad de incidentes en la organización.

Una vez determinada la probabilidad de manifestación de un evento debido a la facilidad o no en que una amenaza puede afectar a un activo, la probabilidad de manifestación de la interrupción junto con el impacto que causa dicha interrupción determinará el riesgo de dicha interrupción. De esa manera podremos determinar el riesgo que corre cada proceso, no solo en función de su impacto que tendrá por período de parada, sino por la probabilidad que tiene de que ocurra; el riesgo es la probabilidad de que ocurra un impacto.

El siguiente cuadro determina el riesgo en función de la probabilidad de manifestación de una amenaza y el impacto de la misma:



Matriz de riesgos.

Ejemplos:

1.- Acceso a la información remotamente durante una interrupción:

Probabilidad baja.

1.- Si afecta a la integridad, impacto alto, entonces riesgo medio.

2.- Si no afecta a la integridad, impacto medio, entonces riesgo bajo.

2.-Interrupción por inundación:

1.- Si el edificio se sitúa en una vaguada, probabilidad media.

2. -Si el edificio se sitúa lejos de las avenidas habituales de inundación, probabilidad baja.

Impacto de una inundación, alto. (Si no hubiera réplicas en otros edificios), si no este impacto sería bajo. Las circunstancias determinan la calificación de los impactos y las probabilidades.

En el caso 1, el riesgo es alto.

En el caso 2, el riesgo es medio.

Como vimos en el análisis de riesgos podríamos transferir riesgo, aceptarlo, reducirlo con controles o eliminarlo de alguna manera; En estos dos

últimos casos se puede evaluar algún tipo de contramedidas para hacerlo efectivo.

Algunas de esas medidas serían:

Controles preventivos: Identifican los posibles problemas que van a ocurrir y previenen los errores, omisiones o actos maliciosos que los pueden causar. Como por ejemplo: realizar copias de seguridad, establecer control de acceso físico o de acceso a la información de manera remota, etc.

Controles de detección: Identifican la ocurrencia de un error, omisión o acto malicioso, a veces este control puede complementarse con el preventivo si es posible, de todas formas es una buena forma de reducir riesgo pues el plan tendrá en cuenta la identificación de estos y su tratamiento si no fuese posible su minimización o eliminación. Algunos controles de detección serían: Monitorización de eventos, detección de virus, sensores de humo, revisiones periódicas de procesos.

En la parte de control de esta fase haremos referencia al control de detección más importante que sería la auditoría interna.

Controles correctivos: Minimizan el impacto de una amenaza, solucionan errores detectados por controles de detección, identifican las causas de los problemas con el objeto de corregir errores producidos y modifican los procedimientos para minimizar futuras ocurrencias del problema.

Las medidas seleccionadas para mitigar riesgos deben mantener un equilibrio entre esfuerzo y coste necesarios para su implantación y la importancia del riesgo que mitigan.

El plan de contingencia se activará cuando sea pertinente, pero otro de los objetivos del propio plan es evitar que se active si es posible. Por lo tanto también entre sus tareas está la de prevención, evidentemente esto entraría ya más de lleno en el área del plan general de seguridad, pero un apéndice como consecuencia de la detección de fallos a tratar por el plan de contingencia puede incorporarse a él como medida preventiva del propio plan y extender de esa manera su protección más allá de la simple intervención del plan en caso de contingencia, pero como decía es ya más cuestión del propio plan de seguridad que del plan de contingencia en sí.

La evaluación de riesgos será periódica y será controlada por la auditoría interna como veremos en la parte de control de esta fase del plan de contingencia, en función de la evolución del negocio, de cambios en la organización de la entidad o de nuevas obligaciones legales.

Control en esta fase:

La creación de una auditoría interna en esta fase es parte de los controles que lleva a cabo la dirección, es un control directivo y por lo tanto crean "marco".

El auditor buscará siempre lo más importante de la actividad empresarial, es decir, los elementos críticos y si el plan de contingencia responde a ellos adecuadamente manteniendo la operatividad en los momentos y procesos críticos; evidentemente el auditor externo buscará esto siempre y cuando compruebe que las operaciones críticas no funcionen adecuadamente, entonces se tornaría a un replanteamiento general del plan; normalmente los auditores externos se ceñirán al encargo realizado por la entidad que normalmente será concerniente a lo habitual y que como hemos indicado no será tan pormenorizado como la auditoría interna, si bien en función de las circunstancias los auditores externos podrían solicitar áreas complementarias de examen a la entidad; es tarea de los auditores internos que el plan se adecúe a la idiosincrasia de la empresa desde un inicio.

Se trata de verificar si los pasos seguidos en el desarrollo del plan, así como las actividades, recursos y funciones implicados, han sido objeto de planificación previa y en determinar si el proceso seguido en su elaboración ha sido idóneo para garantizar el resultado de un plan eficaz de cara a la restauración progresiva de los servicios y de los procesos que los sustentan.

Preguntas esenciales, que los auditores utilizarían para analizar la fase de análisis de riesgos e impactos y que sirven para poder conformarlos desde un principio, serían:

En el anterior control nos preguntábamos por la existencia del plan, ahora nos preguntamos ¿Está aprobado por la dirección? ¿El plan se elaboró con arreglo a un proyecto documentado y autorizado que se conserva adecuadamente?; Estas preguntas nos indican la autoridad e importancia que la entidad a través de los directivos conceden al plan, y si está debidamente tratado y guardado.

¿Qué se intenta proteger?, ¿Se corresponde con nuestros objetivos; preguntas esenciales para saber donde nos encontramos y qué es lo que queremos, el auditor ha de preguntarse esto como inicio en sus valoraciones, en las siguientes auditorías nos preguntaríamos ¿Es igual de importante que antes lo que se intenta proteger o esto ha cambiado?, esta pregunta sería de gran importancia y también sería realizada por un auditor externo, el auditor externo en esta fase pretendería ver que es lo que se quiere proteger y ver si las medidas adoptadas son pertinentes, ver si en realidad ha habido un cambio de objetivos y se han adaptado o si sigue todo igual, evidentemente desde un ángulo mucho más abstracto que el de un auditor interno; estas dos preguntas se refieren a los activos que la entidad intenta proteger con mayor fuerza durante el plan .

Estas dos preguntas serían precursoras de las siguientes que ya entran más en detalle sobre el control del análisis tanto de riesgos como de impacto.

¿Se han determinado correctamente las amenazas?, Como vemos es esencial una identificación de las posibles amenazas, ya que constituirá la piedra angular de nuestra estrategia de protección y reacción. Por tanto es esencial realizar una identificación lo más certera posible.

¿Se han determinado con corrección las vulnerabilidades presentes en nuestra organización?, es imprescindible que la valoración de las vulnerabilidades sea correcta, de esa manera podremos determinar de qué manera y en qué grado afectan a nuestros activos, y ver de qué manera las amenazas puede afectar a la organización a través de qué vulnerabilidades.

¿Cuál es el valor de los activos para la organización?; El auditor interno trataría de evaluar nuevamente estos valores en los activos con esta

pregunta y esto nos permitirá saber si las nuevas amenazas a través de las vulnerabilidades sobre los activos suponen un mayor riesgo y ver si las prioridades de los procesos sobre esos activos son las mismas o han cambiado. El auditor externo también revisaría esto.

¿Frente a qué se intenta proteger?; Los auditores internos tratarían de ver si las amenazas siguen siendo las mismas o han cambiado. Los auditores externos tratan de ver si las amenazas son las mismas que antes evidentemente de una manera más general y siempre haciendo preguntas también a los auditores internos.

¿Cuál es la probabilidad de ataque?; Se trataría de ver si la probabilidad es igual o ha cambiado. Se puede depender de los análisis de procesos que teníamos pero evidentemente si ha habido un cambio sustancial de vulnerabilidad de activos o cambios de amenazas por la propia naturaleza de los sistemas de información habría que mirar si estos siguen siendo los mismos con preguntas pertinentes a tal efecto.

¿En dicho proyecto se consideraron las posibles amenazas sobre los recursos adecuadamente? Nos permite comprobar si han sido valoradas adecuadamente. ¿Se definieron las actividades a realizar para la elaboración del análisis de riesgos e impacto y se designaron a las personas adecuadas para valorarlas?, nos permite conocer si fue un análisis adecuado con las personas indicadas.

¿Se han definido las criticidades de las funciones de manera adecuada?, Nos permite conocer de manera cercana si es adecuada la valoración de la criticidad.

¿Se han indicado contramedidas efectivas que se corresponden con el análisis de la situación realizada?, Nos permite conocer si son efectivas, y se corresponden las contramedidas con el análisis realizado para mejorar el plan de la organización.

Con estas preguntas desarrolladas y la presencia de puntuación de cada faceta de la fase pretendemos establecer una auditoría de la fase y una valoración objetiva de su buena o mala realización.

Con la auditoría en esta fase pretendemos que la efectividad del plan se haga realidad y cualquier desfase o incumplimiento de los propósitos sea corregido. Las auditorías competentes en materia de planes de contingencia de esta fase serán denominadas de “cumplimiento” ya que se centran y preocupan en el cumplimiento de políticas, estándares, requisitos legales etc. que es lo que concierne básicamente a un plan de contingencia; esta fase también podría ser considerada una auditoría de “seguridad” ya que se ocupa de una parte fundamental del plan de contingencia que nos permite salvaguardar la operatividad del negocio frente a eventualidades, (ya que se ocupa y preocupa de prefijar si en el plan están salvaguardados realmente los objetivos, es decir las prioridades).

Mención aparte es que haremos una valoración de cada fase para comprobar su grado de adecuación a nuestros objetivos como ya hemos reseñado.

Tipo de cuadro de valoración, válido para todas las fases:

Nombre de la fase		**Puntuación**
1	Tema a evaluar	..
2	..	..
3		
4	Puntuación de la sección	
5	Nota media	

6	Puntuación Objetivo	
7	Nota media objetivo	

7. Desarrollo de estrategias para el plan de contingencia y la continuidad del negocio:

Una vez desarrollados en la fase anterior, la identificación de todos los procesos que son críticos, su impacto y el umbral de recuperación, y el conocimiento de todas las amenazas, vulnerabilidades y en definitiva riesgos que corremos y asumimos podemos establecer con gran diligencia y cierta exactitud, una serie de estrategias para la recuperación de las funciones de los sistemas de información del negocio, en función de nuestros objetivos. En esta fase por tanto seleccionaremos métodos que se van a utilizar en caso de que ocurra una interrupción que active nuestro plan de contingencia. El método activado deberá restablecer los procesos afectados en el tiempo o umbral determinados en la fase anterior.

Objetivos básicos:

Estudiar alternativas disponibles, ventajas, inconvenientes, costo, incluyendo medidas de reducción del riesgo como estrategia de recuperación.

Contrastar con las áreas funcionales las estrategias viables de recuperación.

Identificar las necesidades de almacenamiento externo de las copias de seguridad y de centro alternativo.

Consolidar las estrategias elegidas y obtener la aprobación de las unidades de negocio.

Presentar las conclusiones a la dirección y obtener su aprobación.

Existen diferentes estrategias para mitigar el impacto de una interrupción; cada una de estas estrategias tiene unos parámetros de tiempo, disponibilidad y costes asociados que serán más o menos apropiados dependiendo de las funciones de negocio.

Diferentes estrategias de reubicación funcional, procesos alternativos desde el punto de vista del tiempo de respuesta y de su fórmula de contratación:

No hacer nada: Esta actuación podría utilizarse en aquellas funciones o actividades que se han clasificado como “no urgentes” en el análisis de impacto. En este tipo de estrategia se asume riesgo.

Reutilización de recursos: Reubicación de personal con funciones no urgentes en tareas que requieren una mayor prioridad. En este caso se debe poner cuidado en convertir la función no urgente en urgente por ser desatendida durante mucho tiempo.

Trabajo remoto: Posibilidad de trabajar desde ubicaciones exteriores a la compañía mediante conexión remota.

Centro frío: es una sala vacía preparada con las condiciones ambientales necesarias para albergar equipos informáticos. Tiene instalación de potencia, climatización, falso suelo y cierta estructura de comunicaciones. El centro frío está recomendado para empresas que por su estructura puedan estar un cierto período de tiempo sin servicios informáticos funcionando con procedimientos alternativos.

Centro caliente: en una instalación con un centro de proceso de datos totalmente configurado a las especificaciones del cliente y disponible en

pocas horas fundamentalmente para organizaciones cuyo tiempo de ruptura no supera las 24/48 horas.

Centro móvil: servicio que consiste en trasladar las facilidades informáticas de respaldo al lugar determinado previamente en el plan de contingencia. Consiste en una sala acondicionada, equipada en un contenedor y configurable en pocas horas. Dependiendo del centro de suministro, los umbrales de recuperación cubiertos pueden ir desde 6-8 horas en adelante. Esta solución está particularmente indicada cuando las instalaciones a respaldar están en una población en la que no existe oferta de servicios de respaldo. Una variante de este servicio, adecuada a los casos en que el incidente ha afectado solo a equipos y no a instalaciones, es el suministro de equipos de respaldo o servicio "off road".

Utilización de espacios propios: Espacios existentes en la compañía tales como salas de formación, cafeterías, etc. Este tipo de estrategia requiere de planificación minuciosa. Cuando una compañía tiene más de un centro de proceso de datos, una alternativa obvia es que un centro sirva de respaldo al otro. Hay que considerar si ambos centros están en la misma planta o mismo edificio, esta solución no ofrece garantías en el supuesto de que el incidente afecte al edificio. Incluso en la misma ciudad no estaría protegido frente a desastres naturales. Sin embargo si el centro de recuperación de proceso de datos alternativo está demasiado lejos, podría haber problemas de conseguir la recuperación dentro del tiempo marcado como objetivo en el Plan de Continuidad de negocio, además de los problemas logísticos de traslado de personas, materiales etc.

Se debe tener en cuenta si hay suficiente espacio para el personal, suministros, mobiliario, etc. para poder llevar a cabo el plan de recuperación desde allí, mención aparte de que puede haber largos períodos de interrupción. Se debe mantener el hardware compatible en ambos centros, ya que puede haber instalaciones hardware que evolucionen de distinta manera incluso estando en la misma organización y bajo un mismo director. Se debe hacer una revisión del hardware detalladamente al menos trimestralmente, también de las compatibilidades del software en lo referente al entorno de proceso. También se harán revisiones trimestrales para asegurar que existe soporte adecuado para todas las aplicaciones críticas. Asimismo se deben considerar los procedimientos específicos para

comunicar cualquier cambio o necesidades adicionales que puedan surgir o ser necesarias. Esto es aplicable para todo el hardware y el software.

Ventajas: Asegura a la compañía unas instalaciones. Disponibles durante todos los desastres. Se pueden hacer pruebas baratas. Está asegurado el backup de teleproceso. Personal con experiencias. Menor coste.

Desventajas: Si está en el mismo edificio o está cerca no está protegido ante desastres regionales. Puede no haber suficiente espacio para ambas operaciones.

Acuerdos recíprocos o de ayuda mutua: Acuerdo entre dos organizaciones (o unidades de la misma compañía), con características y equipamiento similares que permita a cada una de las partes recuperar funciones en otra localización. Hay que tener en cuenta que la capacidad de proceso sea adecuada, y de que se acepta la responsabilidad de comprobar si se hacen cambios en el hardware o software en ambas compañías, entidades o unidades. El acuerdo de ayuda mutua ha de estar especificado en un documento legal, los acuerdos verbales no funcionan.

Ventajas: Puede haber una solución de bajo coste ante una situación crítica.

Desventajas: No es fiable a menos que exista un acuerdo legal. Posibles problemas de seguridad. Puede no haber espacio para ambas operaciones. Puede ser difícil mantener la compatibilidad de hardware y software.

Sitio alternativo subcontratado a terceros o empresas de servicio: Contratación con compañías especializadas de espacios alternativos para la recuperación de la actividad. En este caso hay que asegurar que las compañías pueden proporcionar unos tiempos de recuperación acordes con las necesidades de la organización. Pueden proporcionar un "backup" temporal muy valioso. Hay que asegurarse de que la empresa que nos provee de este servicio tiene el suficiente hardware y software para cumplir con su cometido. Aquí se pueden provocar algunos problemas de

seguridad, ya que probablemente las aplicaciones se procesen junto a las de otros usuarios, en torno a datos confidenciales hay que asegurarse de que se toman las precauciones adecuadas y se establezcan responsabilidades legales en el contrato. También hay que revisar si existen espacios disponibles, hay que considerar los problemas de logística que pueden acontecer.

Normalmente el contrato establece que los servicios de la entidad o empresa pueden usarse por un tiempo limitado, lo suficientemente largo como para poder restaurar las instalaciones dañadas y los procesos críticos. De todas formas ha de tenerse en cuenta qué se debe hacer si superamos ese período máximo de permanencia en la empresa que nos ofrece el servicio de respaldo. También hay que considerar la localización de la empresa y si esto nos puede suponer un problema de logística. Y la problemática en caso de usar el servicio concurrentemente con otros clientes. Y por último la evaluación del coste que tendrá el uso de dicho servicio o la posibilidad de utilizarlo.

Ventajas: La solución más profesional junto con la de proveedores de equipos. Soporte técnico en software de operación, comunicación de datos y su planificación. Instalaciones bien equipadas. Posible espacio para usuarios. Disponible de inmediato por un período de tiempo limitado. Permite tiempo para pruebas. Solución a la medida y costes conocidos.

Desventajas: Necesidad de garantía de uso en caso de concurrencia. Necesidad de garantía de seguridad. Posible falta de espacio para usuarios. Necesidad de garantía en la infraestructura de comunicaciones. Tiempo de proceso limitado. No siempre es posible conseguir la configuración de hardware/software necesaria.

Acuerdo con proveedores de equipos: No todos los proveedores se comprometen a suministrar “backups” por lo tanto los proveedores nos darán la posibilidad de ofrecernos equipos y servicios de respaldo en caso de interrupción de servicios y que pueden ser útiles para nuestro plan de contingencia

Ventajas: Tanto más efectivo cuanto más fiable sea el proveedor y el acuerdo esté más claro en un contrato.

Desventajas: El hardware disponible puede cambiar con el tiempo, llegando a no ser compatible. Necesidad de garantía en la infraestructura de comunicaciones.

Localizaciones diversas: Se traslada la operación pero no el personal.

Centro replicado o Espacio dedicado: Solución que permite trasladar de forma inmediata la operación y continuar la actividad de forma inmediata. También puede denominarse "centro espejo". Son dos instalaciones idénticas y actualizadas permanentemente con objeto de que una de ellas se haga cargo automáticamente del trabajo si otra sufre una interrupción; esta solución es la más cara, pero también es la mejor en caso de que se necesite una recuperación muy rápida de la operación.

Los factores a tener en cuenta para la selección de estrategias dependen de la idiosincrasia de lo que queramos proteger y de las circunstancias que puedan impactar con más probabilidad en una contingencia en nuestra organización. Factores importantes a tener en cuenta serían: Capacidad de las instalaciones, prioridad con la que el suministrador da prioridad a los servicios que se le piden, (por ejemplo en desastres regionales y la concurrencia por instalaciones alternativas entre diversas empresas a las que se dediquen los servicios), tipo de vuelta al centro una vez superada la contingencia y restitución de la normalidad, la distancia que existe entre el centro de recuperación y nuestro centro de operaciones habitual, los gastos que eso conlleva, no solo la propia contingencia sino la reconstrucción, tipo de contratación de las instalaciones, precio por disponibilidad: mensual por suscripción, por activación en caso de desastre, por día de uso de los equipos, uso de consumibles, comunicaciones, etc. Se detallará con profusión la viabilidad económica de estas alternativas que nos permitan desarrollar estrategias viables y adecuadas para el plan de contingencia. Otro factor en cuenta es el prestigio o estabilidad de la empresa a otorgarle nuestra confianza en cuanto a servicios de contingencia se refiere. En ese caso deberíamos asegurarnos o proveernos de una alternativa si la empresa que ofrece el servicio no es muy consistente.

De todas las alternativas deberemos elegir la más adecuada en cada caso. Esto dependerá de nuestros recursos, necesidades, objetivos, costes, etc.

Factores importantes a reseñar cuando establezcamos un lugar donde desarrollar nuestro plan de contingencia tanto si es nuestro como contratado en sus diversas modalidades:

1) Ubicación y superficie requeridas: Espacio suficiente, Zonas acondicionadas para acoger al personal.

2) Recursos técnicos necesarios:

    1) Hardware:

    Debemos ver la compatibilidad para poder realizar un “backup”, en cuanto a los siguientes factores:

    Modelo de máquina, modelo de procesador y velocidad de proceso, número de procesadores, memoria RAM, capacidad de disco, dispositivo de” backup”, impresoras, HW de comunicaciones.

    Tipos de “backups” realizables:

    Los procedimientos de obtención de copias son primordiales a la hora de la recuperación de información, y su presencia en los planes de contingencia por tanto es totalmente necesaria e imprescindible. Por lo tanto debemos de contar a la hora de realizar estas copias con los diferentes tipos de “backups” que podemos contar:

    “Backups” del sistema operativo: Se realizará normalmente cuando existen varios sistemas operativos dentro de nuestra entidad, pero también si hubiera uno solo.

    “Backups” del software base: Paquetes o lenguajes de programación con los cuales han sido desarrollados o interactúan nuestros aplicativos institucionales.

    “Backups” del software aplicativo: Considerando tanto los programas fuentes, como los programas objetos correspondientes, y cualquier otro software o procedimiento

que también trabaje con los datos, para producir los resultados con los cuales trabaja el usuario final.

“Backups de los datos”: Bases de datos, Índices, tablas de validación, “passwords”, y todo archivo necesario para la correcta ejecución del software aplicativo de nuestra entidad.

“Backups del sitio web”: Software aplicativo y bases de datos asociados al sitio web de la entidad, asimismo como sus índices ficheros de descarga y contraseñas.

“Backups de hardware”: Como veremos serán la modalidad o solución externa y la modalidad o solución propia o interna.

Se deben establecer una serie procedimientos normas y determinación de responsabilidades en la obtención de “bakups”, debiéndose incluir:

- Periodicidad de cada tipo de “Backup”
- Respaldo de información de movimiento entre los períodos que no se sacan “backups”
- Uso obligatorio de un formulario estándar para el registro y control de los “backups”.
- Almacenamiento de los “Bacukps” en condiciones ambientales óptimas, dependiendo del medio magnético empleado.
- Reemplazo de los “Backups”, en forma periódica, antes que el medio magnético de soporte se pueda deteriorar.
- Almacenamiento de los “Backups” en locales diferentes donde reside la información primaria (evitando cierto destrozo de toda la información).
- Pruebas periódicas de los “Backups”, verificando su funcionalidad, a través de los sistemas, comparando contra resultados anteriores confiables (esta parte se realizaría durante la fase de pruebas).

2) Software: compatibilidad de SSOO y de otro software requerido para la manutención de nuestro sistema de información.

2) Datos de respaldo: documentación

3) Seguridad: seguridad lógica, seguridad de comunicaciones, control de accesos de personas y paquetes, detección y extinción de incendios, detectores de agua en falsos suelos.

4) Disponibilidad: espacio físico, mantenimiento de los equipos.

5) Recursos materiales, humanos y de infraestructura: instalaciones de voz y datos, mobiliario de oficina, equipo de oficina (fax, etc.), equipo de manipulación de formularios (clasificadoras, etc.), suministros de oficina y de proceso de datos, dispositivos de almacenamiento magnéticos adicionales, almacén, alimentación ininterrumpida de suministro eléctrico, área de descanso, facilidades de suministro de comidas, roperos, etc.

También tendremos en cuenta los posibles servicios auxiliares eventuales que puedan surgir así como los tiempos de activación y el coste.

Normalmente a menor tiempo de recuperación mayor coste, por eso es importante realizar un buen análisis y poder adaptar el plan de contingencia con tiempos adecuados a la realidad de la compañía.

Otro punto importante y reseñable es el tener copias de salvaguarda fuera del área de riesgo del centro de proceso de datos. En función de la necesidad se irá actualizando, existen dos soluciones estratégicas para la salvaguarda de datos:

Solución propia: Solución cara si se quiere mantener con un mínimo de garantía, debido a la ocupación de un espacio dedicado y acondicionado, por la logística de traslado y sobre todo por tener personal dedicado a la gestión de almacenamiento externo. Uno de los males más acuciantes de esta solución es la dejadez que hacen los mismos trabajadores, ya que al realizarlo nosotros mismos normalmente existe una relajación en los salvados, en los envíos y sobre todo en el control de la información. Su accesibilidad es de 24 horas al día, los 365 días del año. Luego existen una serie de parámetros a cumplir por la entidad para cumplir con los mínimos requisitos indispensables para la manutención adecuada de las copias de

salvaguarda, como por ejemplo: Resistencia al fuego, temperatura controlada, humedad controlada, resistencia al aplastamiento, hermeticidad ante gases, hermeticidad ante agua, sistemas de detección de humos, sistemas de extinción, cierre rápido en caso de desastre público protección contra el robo

Solución externa: Existen empresas que ofertan en exclusiva el almacenamiento de soportes informáticos, pero también existen empresas que ofertan estos servicios y que no se dedican en exclusiva a la oferta de ellos.

Los requisitos que se exigen a este tipo de instalaciones son los siguientes:

- Almacén vigilado y con sistemas de seguridad activa y pasiva.
- Sala de almacenamiento de soportes presurizada, con sistemas de extinción, control de parámetros como humedad, temperatura, etc.
- Sistemas de alimentación eléctrica redundantes.
- Transporte acondicionado para tal efecto, con comunicación.
- Disponibilidad de la información las 24 horas los 365 días del año
- Recogida y entrega planificada en las instalaciones del cliente.
- Posibilidad de acceso inmediato a la recogida de soportes de las personas autorizadas o posibilidad de peticiones de urgencia con un tiempo de respuesta aceptable (2/3 horas).
- Cobertura de seguro adecuada.
- Conceptos de facturación claros y cerrados, incluidas tarifas para servicios de emergencia en horario normal, nocturno, fines de semana, etc.
- Software de administración y logística integrados, que permitan la gestión de las unidades almacenadas y personalización de clientes.
- Confidencialidad de los datos almacenados, ya sea si están almacenados que no se pueda identificar a quien pertenezcan por etiquetado, etc.

Por último reseñar que no todas las áreas de una entidad necesitan de las mismas estrategias de recuperación, sus necesidades pueden ser diferentes, no solo en cuanto a equipos sino también a personal, umbrales de recuperación, suministros, etc. Por lo tanto se hace necesaria una solución estratégica que englobe a todas las áreas y que incida especialmente en las que sean comunes y de las que dependan las demás para poder seguir con la continuidad del negocio. Por ejemplo en algunas ocasiones será más rentable actuar con un solo departamento en vez de aplicar el plan de contingencia en su completitud, lo que supondría un trastorno grave para nuestra organización y un gasto innecesario, por lo tanto la solución estratégica variará dependiendo de las áreas afectadas y de la situación en que se den los problemas.

Por ejemplo: si existe un fallo en algún equipo del sistema de información que no es clave en la sustentación de dicho sistema y la adquisición de un equipo adecuado puede demorarse algunos días, se puede adoptar la solución de tener equipos antiguos con una funcionalidad limitada hasta que se consigue un equipo adecuado, en dicho caso una estrategia de traslado a un centro alternativo sería costosa e ineficaz. Por lo tanto en función de las circunstancias y de la manera en la que puedan ser salvadas se adoptará una u otra estrategia. De tal manera que en determinadas ocasiones podemos hablar de la activación parcial de un plan de contingencia, ya que no es necesaria una activación completa de todo el plan porque con una estrategia parcial de recuperación podemos recobrar la funcionalidad esencial de la entidad.

Control en esa fase:

Algunas de las cuestiones imprescindibles que un auditor o controlador ha de hacerse ante la fase de desarrollo de estrategias de un plan de contingencia son las siguientes:

Estratégicamente se pueden realizar las siguientes preguntas para poder comprobar la afección de la estrategia en función de la solución adoptada finalmente por la empresa:

¿Se han identificado correctamente las necesidades que debe cubrir la estrategia de continuidad de negocio seleccionada?

En esta pregunta se englobaría: Revisar umbrales de tiempo, comunicación, localización, personal, componentes tecnológicos de la recuperación para cada servicio de soporte, componentes no tecnológicos de la recuperación, comparar con soluciones externas y ver si pueden ayudarnos en algo. Analizar estrategias alternativas viables y ver si con el tiempo pueden ser mejores para nuestros planteamientos empresariales. Ver si el riesgo asociado a la estrategia elegida se ha evaluado correctamente.

¿Se han considerado las estrategias alternativas mencionadas en la anterior consideración de la pregunta y su idoneidad para nuestra entidad?

Para esta pregunta deberíamos analizar los criterios que definen las necesidades del negocio, los objetivos de la planificación de la recuperación, y el establecimiento de criterios base para definir las opciones que nos permitan comprobar su viabilidad. Conjuntamente se podría prestar atención a una relación coste/beneficio de cada una de las estrategias alternativas y su viabilidad futura en función de la reorientación estratégica de la compañía.

¿El centro elegido para la recuperación es propio o contratado?, ¿Es adecuado en función de nuestros objetivos?, Comprobaremos los criterios que rigen nuestra compañía en cuanto a objetivos se refiere, en función de lo que busquemos será propio o contratado, revisaremos las comunicaciones con dicho centro así como los contenidos de la contratación si es contratado a un tercero, también evaluaremos qué tipo de almacenamiento externo es el más adecuado en cada caso.

¿Se puede utilizar el centro para pruebas?, ¿Es utilizado para las necesidades de un tercero en caso de que sea contratado a una compañía externa?, ¿Si hay más de una compañía, hay suficiente tiempo de proceso disponible?

Nos permite evaluar en qué grado la compañía externa nos garantiza la posibilidad de respaldo en caso de necesidad, y si podemos usar dicho centro para poder probar nuestro propio plan.

¿Existe un documento legal que respalde y refleje lo que realmente se contrató?

Lo comprobamos para cerciorar que todo está acorde con la legalidad vigente sin que medien contratos verbales que no son formales.

En el caso de la contratación: ¿Hay suficiente tiempo de proceso para nuestras necesidades?, ¿Somos puntualmente informados de todos los cambios que se puedan producir dentro de los sistemas tanto de software como de hardware del centro alternativo?, ¿Se ha especificado el coste de contratación?

Nos permite conocer de primera mano si es adecuado el servicio que se oferta y de la prontitud de respuesta ante un cambio, asimismo es esencial el coste de contratación para determinar la rentabilidad de la utilización de dicho centro.

¿La distancia con el centro de desarrollo de nuestras actividades es lo suficientemente cercana como para permitir una fácil recuperación de las operaciones?

Esta pregunta es la disyuntiva, o solución de compromiso que se ha de adoptar como hemos reseñado en alguna ocasión, el centro ha de estar lo suficientemente cerca para permitir una pronta recuperación, pero lo suficientemente lejos como para no verse afectado por el mismo tipo de desastre natural por ejemplo. Esto lo podríamos ver en la siguiente pregunta:

¿Se encuentra dicho centro a una distancia que lo salve de desastres naturales que puedan afectar a nuestro centro donde nosotros desarrollamos nuestro trabajo habitualmente?

Otras preguntas que podrían determinar la calidad del servicio prestado y por tanto aumentan nuestra probabilidad de desarrollar con eficacia nuestro plan serían:

¿El proveedor dispone de un equipo de atención que nos permita acceder de una manera eficaz a los servicios propios que nos ofrecen?

¿Dan soporte alternativo de mantenimiento o ingeniería?

¿La disponibilidad de los servicios es absoluta?

¿Qué medidas de seguridad existen en el centro?

¿Qué espacio adicional de oficinas hay disponible?

¿Se proveerán técnicos de sistemas u operadores?

¿Qué comunicaciones hay disponibles?

¿Qué pruebas del plan pueden hacerse? ¿Se suministra espacio de almacenamiento? ¿Cuál es el procedimiento de petición del servicio, funciona correctamente? ¿Durante cuánto tiempo se pueden usar las instalaciones?, ¿Es suficiente?, ¿Qué procedimiento se seguirá para atender más de una petición simultánea?, ¿Se han determinado las responsabilidades en cada fase de traslación del plan de contingencia al lugar de recuperación?, ¿Se han determinado los precios específicos de los servicios?

Con estas preguntas podríamos cubrir con bastante certeza casi todas las facetas del control de la fase de estrategia de un plan de contingencia.

8. Desarrollo del plan de contingencia ante una emergencia:

Esta fase de refiere al desarrollo e implantación de los procedimientos en las diferentes áreas del plan dentro de la compañía y asimismo la organización de los equipos que intervienen en cada momento, de tal manera que nos permita la recuperación en el umbral de tiempo marcado como objetivo.

Hasta el momento y a estas alturas dentro del desarrollo de un plan tenemos los siguientes elementos:

Por un lado conocemos todos los procesos sabiendo cuáles son los críticos. Sabemos qué riesgos nos pueden afectar y que su materialización puede hacer activar el plan. Y conocemos cual es la estrategia que hemos adoptado en función de nuestros objetivos, estableciendo nuestro centro de operaciones de emergencia que será nuestro centro de control durante una contingencia.

Previamente a la manifestación del propio desastre en esta fase se debe determinar la formación de equipos operativos que atacarán la emergencia. En cada unidad operativa de la institución, que almacene información y sirva para la operatividad de la entidad, se deberá designar un responsable de seguridad de la información de su unidad, pudiendo ser el jefe de dicha área operativa; sus labores, previas al desastre, serán:

1. Ponerse en contacto con los propietarios de las aplicaciones y trabajar con ellos.
2. Proporcionar soporte técnico para las copias de respaldo de las aplicaciones.
3. Planificar y establecer los requerimientos de los sistemas operativos en cuanto a archivos, bibliotecas, utilitarios, etc., para los principales sistemas y subsistemas.
4. Supervisar procesos de respaldo y supervisión.
5. Supervisar la carga de archivos de datos de las aplicaciones, y la creación de respaldos incrementales.

6. Coordinar redes, líneas, terminales, módems y otras comunicaciones.
7. Establecer procedimientos de seguridad en los sitios de recuperación.
8. Organizar la prueba de hardware y software.
9. Ejecutar trabajos de recuperación.
10. Cargar y probar archivos del sistema operativo y otros sistemas almacenados en el lugar alternativo.
11. Realizar procedimientos de control de inventario y de seguridad del almacenamiento en el lugar alternativo.
12. Establecer y llevar a cabo procedimientos para restaurar el lugar de recuperación.
13. Participar en las pruebas de simulacros y desastres.

Desarrollaremos más en profundidad el tema de las pruebas en la fase de pruebas de este plan, pero esta parte previa al desastre siempre utilizará dicha fase de pruebas para realizar las comprobaciones pertinentes antes del desastre, y comprobar que estamos preparados para cualquier contingencia. Esto ocurre así ya que el plan en sí no es secuencial sino que va mejorando con la experiencia y es circular, siempre volvemos con nuestras pruebas a comprobar que hemos mejorado, o lo que hemos realizado es adecuado para el funcionamiento y efectividad de nuestro plan.

Para desarrollar nuestro plan y desarrollar e implementar procedimientos para responder a un incidente y estabilizar la situación debemos determinar qué objetivos buscamos:

Identificar emergencias potenciales y tipo de respuesta necesaria.

Averiguar si existen procedimientos adecuados de respuesta ante esas emergencias.

Recomendar el desarrollo de procedimientos en los casos que no existan (también en la fase de control).

Integrar los procedimientos de emergencia con los procedimientos de contingencia (recuperación ante desastres).

Identificar las necesidades de dirección y control para hacer frente a la emergencia.

Recomendar el desarrollo de procedimientos de dirección y control para definir responsabilidades, línea de mando y procedimientos de actuación durante la emergencia.

Asegurarse de que los procedimientos de respuesta ante la emergencia cumplen la normativa legal.

Y también necesitamos:

Definir los equipos necesarios para el desarrollo del plan, como dijimos anteriormente con la asignación de un responsable.

Definir las funciones y responsabilidades de cada uno de los equipos.

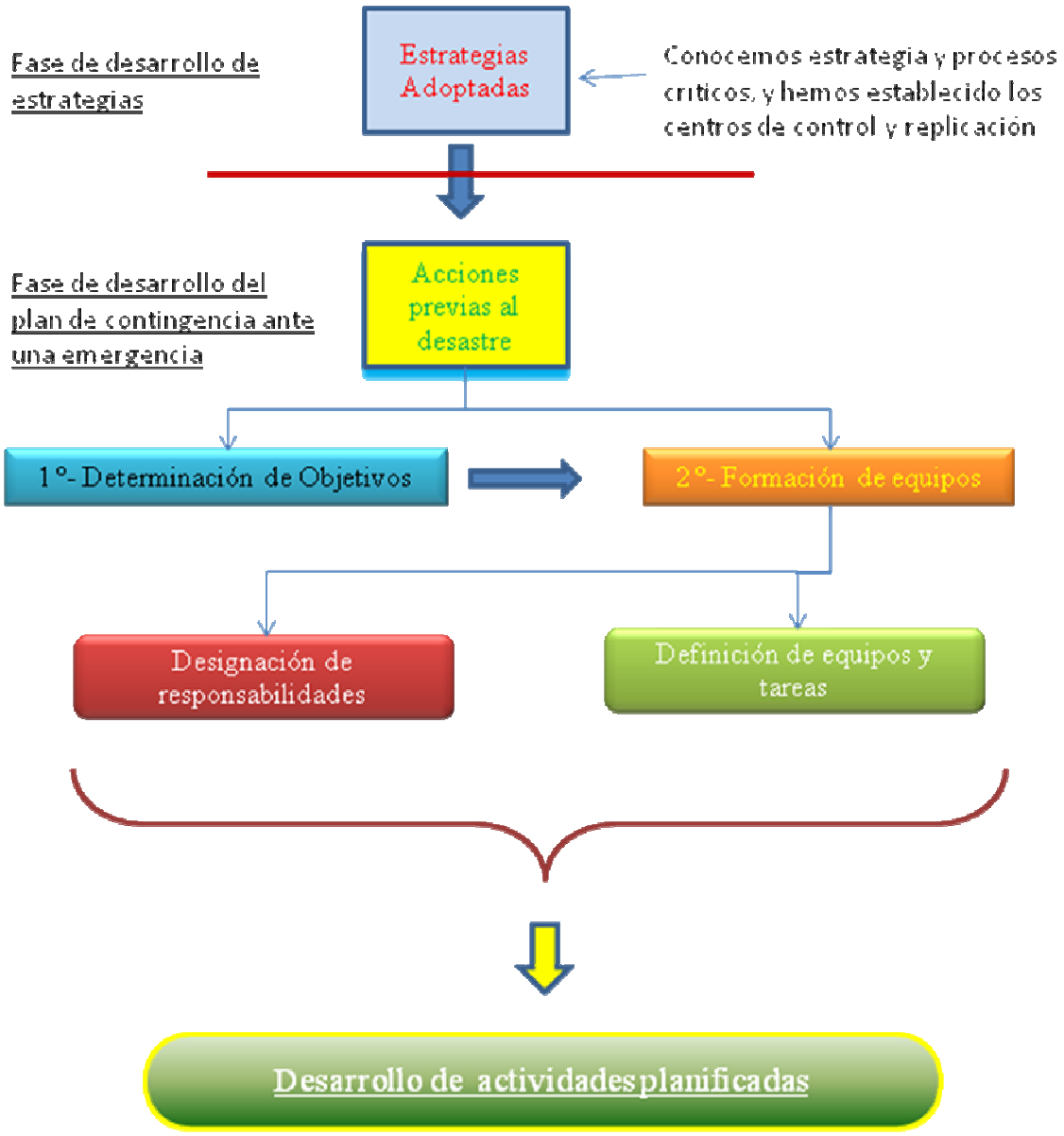
Definir las dependencias orgánicas entre los equipos.

Elaborar el desarrollo de procedimientos de alerta y actuación ante eventos que puedan activar el plan.

Definir los procedimientos de actuación ante incidentes.

Establecer la estrategia de vuelta a la normalidad.

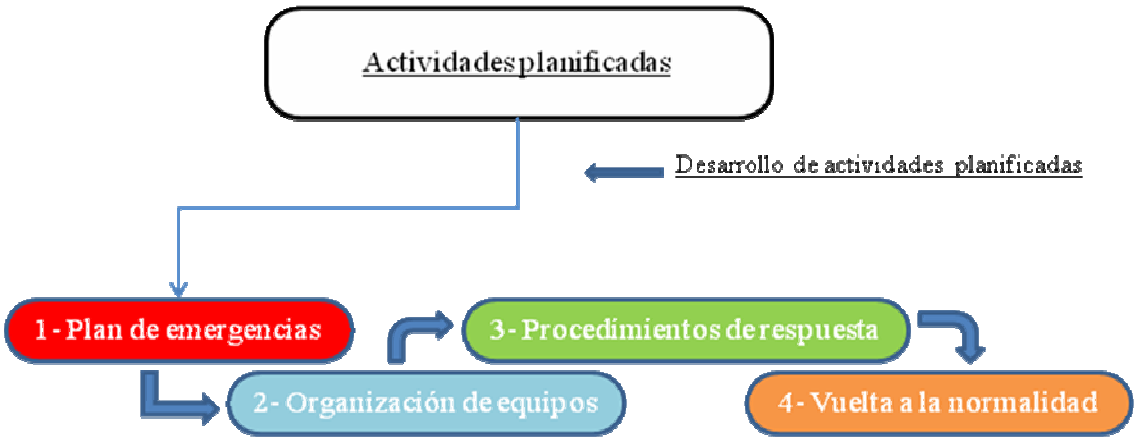
Cuadro de evolución previo a la declaración de la contingencia o siniestro:



Una vez presentada la contingencia o siniestro, se deberán ejecutar actividades planificadas previamente, y que perseguirán los objetivos enumerados anteriormente:

1. Plan de emergencias
2. Organización de equipos, (previamente formados antes del desastre como hemos visto).
3. Procedimiento de respuesta o desarrollo de procedimientos
4. Actividad después del desastre, vuelta a la normalidad.

Cuadro de actividades planificadas:



Las actividades se planificarán en ese orden, pero la aplicación y ejecución de las mismas se dan en paralelo y de manera coordinada ante una contingencia, con la salvedad de la vuelta a la normalidad que se ejecutará de manera posterior a la ejecución de las demás actividades, y siempre después del siniestro.

Veremos en los siguientes pasos la planificación de las actividades así como su comportamiento ante siniestros.

1. Plan de emergencias:

Como dijimos al inicio de esta fase existen una serie de objetivos que perseguimos y después formalizamos en una serie de pasos una vez manifestada la emergencia. Primeramente en el plan de emergencias

estableceremos una serie de emergencias potenciales que se pueden manifestar, de esa manera tendremos identificados previamente estos hechos, no obstante esta tarea de identificación de amenazas también se ha llevado a cabo en otras fases del propio plan y tiene como objetivo recordar y reforzar claramente la procedencia de ellas para estar bien preparado en el momento de la acción pertinente e indagar sobre la contingencia manifestada en cuestión.

Algunas de esas amenazas en el sentido general serían:

Algaradas callejeras, accidente nuclear, amenaza de bomba, derrumbamiento de edificio, epidemia, erupción volcánica, explosión, fallo de telecomunicaciones, fallo de los equipos, fallo de servicios esenciales, fallo de suministros de energía, fuga de sustancias tóxicas, huelga de servicios postales, otras huelgas, imposibilidad de acceso al edificio por casusas ajenas al mismo, incendio, inundación por casusas internas, inundación por riadas, maremoto, pánico colectivo, rayo, robo, rotura de presa, sabotaje físico, sabotaje lógico, terremoto, terrorismo, toma de rehenes, tornado, etc.

En este plan de emergencias se establecen las acciones que se deben realizar cuando se presente un siniestro, así como la difusión de las mismas.

Es necesario prever los posibles escenarios de ocurrencia del siniestro:

1. Durante el día
2. Durante la noche o madrugada

Y asignar los turnos correspondientes.

Este plan deberá incluir la participación y actividades a realizar por todas y cada una de las personas que se pueden encontrar presentes en el área donde ocurre el siniestro, debiendo detallar:

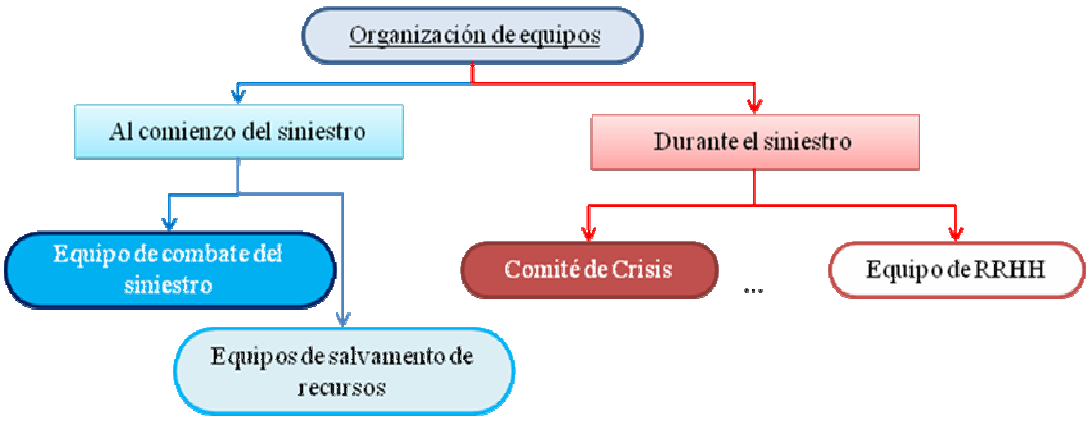
1. Vías de escape o de salida

2. Plan de evacuación del personal
3. Plan de puesta a buen recaudo de los activos (incluyendo los activos de información), de la entidad (si las circunstancias del siniestro lo posibilitan).
4. Ubicación y señalización de los elementos contra el siniestro (extintores, cobertores contra agua, etc.).
5. Secuencia de llamadas en caso de siniestro, tenerlos a mano: elementos de iluminación (linternas), lista de teléfonos (bomberos, ambulancia, policía, personal de seguridad de la entidad, etc.).

2. Organización de equipos

Establecer claramente cada equipo (nombre, puestos, ubicación etc.) con funciones claramente definidas a ejecutar durante el siniestro. Si bien la premisa básica es la protección de la integridad del personal, en caso de que el siniestro lo permita (por estar en un inicio o estar en un área cercana), deberán de existir dos equipos de personas que actúen directamente durante el siniestro, un equipo para combatir el siniestro y otro para el salvamento de recursos informáticos de acuerdo a la clasificación de prioridades reseñada en los planes de contingencia.

Cuadro de organización de equipos:



Los equipos están formados por personal clave necesario en la activación y desarrollo en el plan de continuidad. Cada equipo tiene unas funciones y procedimientos que tendrán que desarrollar en las distintas fases del plan. Los equipos normalmente se formarán en función de la estrategia de recuperación, algunos ejemplos de equipos que intervendrían serían:

Equipo director o comité de crisis: Encargado de dirigir las acciones durante la contingencia y recuperación. Su objetivo es reducir al máximo el riesgo y la incertidumbre en la dirección sobre la situación. Este comité debe tomar decisiones clave durante la crisis, además de hacer de enlace con la dirección de la compañía, manteniéndoles informados de la situación regularmente. Este equipo evalúa el incidente, activa el plan de recuperación y coordina el resto de equipos. Por lo tanto las actuaciones de respuesta ante la emergencia y posterior proceso de recuperación y vuelta a la normalidad se deberán dirigir y controlar desde el centro de control por parte del comité de crisis, por lo que tal centro debe estar, no solamente definido en cuanto a ubicación y recursos materiales y humanos con que debe contar, sino también dotado de procedimientos de actuación, definiendo las funciones de las personas que lo integran, sus niveles de responsabilidad y cadena de mando. Este equipo también es responsable de supervisar, documentar y coordinar el proceso de recuperación. Sus miembros son los responsables finales de la toma de decisiones y fijación de prioridades, políticas y procedimientos.

Las principales tareas y responsabilidades de este comité son:

- Análisis de la situación.
- Decisión de activar o no el plan de continuidad.
- Iniciar el proceso de notificación a los empleados a través de los responsables e informar a la dirección.
- Seguimiento del proceso de recuperación, con relación a los tiempos estimados de recuperación.

Equipo de recuperación:

Su función es restablecer todos los sistemas necesarios, ya sean infraestructuras, servidores, servicios de comunicaciones y cualquier otro servicio necesario para la recuperación de un servicio. Aquí estaría integrado el equipo de salvamento de recursos informáticos tal y como reseñamos anteriormente, y que es diferente del que ataca directamente el siniestro (aplicaciones críticas), el equipo de salvamento proveería al de recuperación de los recursos salvados y señalaría la operatividad de los mismos.

Equipo Logístico: Responsable de la logística en el esfuerzo de recuperación. Asume tareas como: Transporte de material y personas, suministros de oficina, comida, reservas de hotel (si fuesen necesarias), contacto con los proveedores. Este equipo debe trabajar coordinado con los demás, para asegurar que todas las necesidades logísticas son cubiertas.

Equipo de relaciones públicas y atención al cliente: Canaliza la información que se genera, al exterior en un solo punto para que los datos sean referidos desde una sola fuente. Sus funciones principales son:

Coordinar con los departamentos afectados y la alta dirección, la elaboración de una comunicación oficial de la organización para ser entregada a los medios de comunicación.

Desarrollar una estrategia de comunicación a los medios, con la celebración de ruedas de prensa periódicas, entrega de carpetas de información describiendo las causas del incidente, las medidas que estaban previstas y la evolución que se está produciendo, contacto directo con los directores de los medios principales etc.

Comunicados con los clientes: Uno de los valores más importantes de una entidad son los clientes, por lo que es prioritario

tener informados a los mismos, estableciendo canales de comunicación.

Equipo de unidades críticas: Son las personas que trabajan con las aplicaciones críticas y serán los encargados de realizar las pruebas de funcionamiento para verificar la operatividad de los sistemas y comenzar a funcionar. Cada equipo deberá configurar las diferentes pruebas qué deberán realizar para los sistemas.

Equipo financiero: Se encarga de las evaluaciones económicas para negociación con compañías de seguros y de la creación de cuentas especiales para controlar gastos extraordinarios resultantes del incidente, etc.

Equipo jurídico: Se encarga del estudio de los contratos con los clientes y proveedores para avisar de posibles incumplimientos y consecuencias derivadas de ellos. Asimismo establece comunicación oficial con organismos públicos, asociaciones empresariales, empresas participadas, accionistas, etc.

Equipo comercial: Realiza la comunicación y atención del cliente en función de niveles, transmitiendo información coordinada con el equipo jurídico y el equipo de relaciones públicas. Por otra parte se encarga también de las instrucciones a la red de vendedores y distribuidores propios de la entidad, etc.

Equipo de recursos humanos: Se encarga de atender todas las necesidades extraordinarias de índole laboral que puedan aparecer como consecuencia de las características especiales de los trabajos que hay que realizar, (contacto con el comité de empresa, establecimiento de turnos, horas extraordinarias, transporte de personal, etc.). También atienden el estado físico y sicológico de los afectados por el incidente, asimismo como atender e informar a familiares de posibles heridos, etc.

Equipo de servicios generales: Establece un sistema y centro alternativo de correo interno y externo. Organiza y atiende las posibles necesidades extraordinarias de material impreso y suministros de oficina. Organiza los servicios de cafetería para atender las necesidades especiales que puedan surgir como consecuencia de la incidencia, etc.

3. Procedimientos de respuesta

En primer lugar se deben diseñar los procedimientos de comunicación, tanto interior, definiendo los procedimientos de escalado de decisiones a tomar en función del alcance y gravedad de la emergencia, como al exterior, cubriendo no solamente la información a clientes y proveedores sino también a los medios de comunicación por los equipos señalados para tal efecto tal y como se designó en el apartado anterior. También se deberán diseñar los procedimientos de preparación ante posibles incidentes, según se trate de desastres naturales o de origen humano, fortuitas o errores. En ellos se deberán definir las funciones del personal designado para acometer determinadas acciones y niveles de decisión y autoridad.

Por otra parte se deberán tener en cuenta los procedimientos editados por el departamento de seguridad, solicitando que se desarrollen nuevos procedimientos donde no existan.

Debe prepararse un boceto de los contenidos del plan para guiar el desarrollo de procedimientos. El plan propuesto debe ser revisado y aprobado por la dirección. De esta forma:

- Se facilita la organización de procedimientos.
- Se identifican los principales pasos a dar antes de comenzar a escribir.
- Se identifican los solapes en procedimientos que producirían redundancias y pérdidas de tiempo.

- Se establece una pauta para el desarrollo de los procedimientos.

El plan de desarrollo de procedimientos debe tener un formato estándar y estructura homogénea que permitirá un más fácil mantenimiento del mismo. Es particularmente importante cuando este plan es elaborado a partir de distintos departamentos.

En el desarrollo es imprescindible la elaboración de unas pautas para el desarrollo de los procedimientos:

En cuanto al formato:

- Finalidad del procedimiento
- Alcance, (por ejemplo, lugar, equipos, personal y tiempo a los que afecta el procedimiento).
- Referencia a otros materiales, (manuales, documentación, etc.)
- Impresos aplicables que se deben utilizar cuando se ejecuten documentos.
- Autorizaciones pertinentes.
- Políticas particulares aplicables al procedimiento.
- Encabezamiento o pies de página tales como: código y descripción del asunto, número de página, número de versión, fecha de edición, etc.

En cuanto a métodos de redacción:

- Escribir los procedimientos de forma clara y fácil de entender, (quizá sean utilizados por personal poco familiarizado con el procedimiento y bajo presión emocional).
- Utilizar frases cortas, directas y sencillas.
- Párrafos cortos para facilitar la comprensión.
- Presentar las ideas de una en una.
- Utilizar los verbos en voz activa y en tiempo presente.

- Evitar argot, aunque sea común en el uso habitual de la profesión.
- Utilizar los títulos de los puestos en vez de nombres de personas, de esa manera habrá que actualizarlo menos veces.
- Identificar acciones que deben producirse simultáneamente y acciones que tienen que ocurrir de forma secuencial.
- Utilizar verbos descriptivos (adquirir, activar, almacenar, archivar, avisar, ayudar, comparar, contactar, contestar, crear, declarar, entregar, explicar, informar, listar, localizar, mover, pagar, registrar, revisar, sustituir), en vez de verbos más generalistas como (hacer o realizar).

Los procedimientos deben incluir los pasos a dar antes, durante, y después de la interrupción; sin embargo, no deben escribirse hasta no haber fijado la estrategia de recuperación, ya que serán totalmente dependientes de la misma.

Los procedimientos deben recoger también las pruebas que sea recomendable realizar, fijando una periodicidad de las mismas (periodicidad que puede ser también fijada en función de los resultados de las pruebas) y en función del alcance que se haya fijado para ellas, (comprobaciones con *checklist*, pruebas de simulación, pruebas en paralelo, o pruebas de interrupción total); estas pruebas serán desarrolladas durante la fase de mantenimiento y pruebas que todo plan de contingencia tiene previsto, asimismo estas pautas servirán para los auditores cuando tengan que llevar a cabo la realización de la auditoría pertinente de esta fase del plan de contingencia.

Asimismo los procedimientos deben incluir métodos para actualizar el planeamiento de la contingencia y que recoja en todo momento las modificaciones que hayan sufrido los componentes como consecuencia de la evolución de la organización.

Como dijimos anteriormente el plan ha de estructurarse mediante la definición de equipos cuyo cometido ya definimos en el punto anterior y a los cuales serán asignadas responsabilidades específicas en función de las áreas de trabajo de la organización.

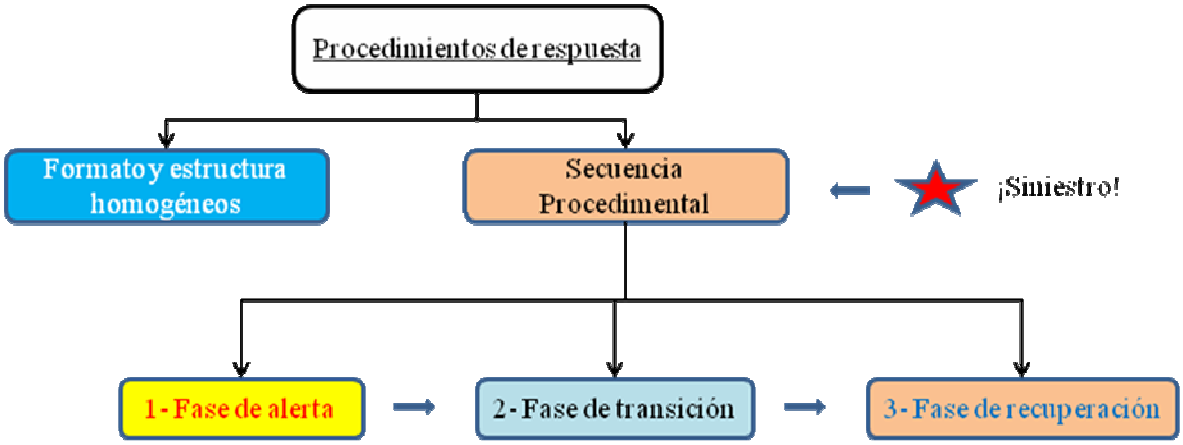
Las actividades para la implementación del Plan van encaminadas al establecimiento del centro de control, centro alternativo, centro de almacenamiento externo y a la identificación de las acciones y recursos específicos que necesitan los diferentes equipos de recuperación para poder poner en práctica las estrategias de respuesta y recuperación. Estas acciones son realizadas por los equipos de recuperación y deberán definir acciones de respuesta y recuperación, identificación de necesidades del personal, de registros vitales y soluciones disponibles, de contactos relacionados con la actividad, comprobación de disponibilidad de los recursos necesarios tanto de personal como de hardware o software y otro tipo de material como de oficina o suministro. Todo ello acompañado de una documentación incluida en los planes de recuperación de cada equipo.

Todas esas actuaciones de respuesta ante la emergencia y posterior proceso de recuperación y vuelta a la normalidad se deberán dirigir y controlar, como hemos indicado, desde el centro de control o gestión de la crisis, por lo que tal centro debe estar, no solamente definido en cuanto a ubicación y recursos materiales y humanos con que debe contar, sino también dotado de procedimientos de actuación, definiendo las funciones de las personas que lo integran, sus niveles de responsabilidad y cadena de mando.

También habrá que diseñar procedimientos tendentes a mitigar el daño producido por el incidente y a estabilizar el funcionamiento de la organización, aunque sea en situación provisional y precaria.

Los procedimientos seguirán una secuencia cronológica ante un evento de interrupción y en cada una de las fases de activación del plan desempeñarán un papel:

- Fase de alerta
- Fase de transición
- Fase de recuperación.



- Fase de Alerta:

  Implica procedimientos de actuación en los primeros momentos de un suceso que puede suponer la pérdida parcial o total de uno o varios procesos o funcionalidades críticas.

  Se puede dividir esta fase en las siguientes acciones:

  - Notificación: Se define quién y cómo debe ser informado en primera instancia de lo ocurrido. Evidentemente no se puede tener cubierta tal cantidad de casos, pero se establecerán unas pautas que permitirán concienciar al personal de cómo proceder en caso de contingencia.

    Situación de contingencia => Aviso inmediato al responsable de personal o de seguridad => Aviso a la persona responsable del comité de crisis y en su caso a los equipos de emergencia.

    Este sería el procedimiento de notificación del desastre.

  - Evaluación: Análisis de la situación y valoración inicial de los daños. Una vez que un miembro del comité de

crisis es contactado e informado del incidente, se procederá a la evaluación de la situación con la mayor recopilación de información posible.

El comité informará de lo ocurrido a los equipos y de la situación en ese momento para que permanezcan en situación de espera, hasta que se tome la decisión de activar el plan o iniciar otro tipo de estrategia.

Conocimiento por parte de algún miembro del comité => Reunión en un lugar acordado previamente y evaluación de la situación => Se informará a los siguientes responsables: De Seguridad, Comité de dirección de la empresa, Relaciones públicas, Equipo de recuperación, Responsable de los equipos.

Este sería el procedimiento de lanzamiento del plan.

- Ejecución: Una vez que el comité de crisis ha decidido poner en marcha el plan de recuperación, se comienza con el árbol de llamadas para comunicar a los responsables y componentes de cada equipo la situación de inicio de las actividades del plan para comenzar los procedimientos de actuación de cada uno de ellos. Deberá también informarse al comité de dirección.

  Consideración por parte del comité y ejecución en su caso del plan =>Iniciar árbol de llamadas e informar al comité de dirección => Paso a la fase de transición

  Este sería el procedimiento de notificación de la puesta en marcha del plan a los equipos implicados.

- Fase de transición: Es la fase previa a la recuperación de los sistemas. Es importante que en esta fase exista una coordinación entre los diferentes equipos y el equipo de logística ya que se encargan de que todo esté disponible para comenzar la recuperación en el menor tiempo posible.

  Se puede hablar de dos partes en esta fase:

  - Procedimientos de concentración y traslado de personas y equipo.
  - Procedimientos de puesta en marcha del centro de recuperación.

  Estos procedimientos son la base del proceso de recuperación de los sistemas, si falla, no será posible comenzar con la recuperación y el plan de continuidad habrá fracasado.

  Concentración y traslado de personas y equipos:

  La realización de estos procedimientos dependerá de la estrategia que se decida finalmente, pero de modo general seguiría de la siguiente manera: Una vez puesto en marcha el plan y avisados los equipos, se acude al centro de reunión. Si el incidente ocurre fuera del horario de trabajo, el lugar de reunión será el designado como centro de respaldo, o cualquier otro designado por el comité de dirección de crisis. Además del traslado de personas al centro de recuperación (si es necesario), hay que realizar una importante labor de coordinación para el traslado de todo el material necesario para poner en marcha el centro de recuperación, (backups, material de oficina, documentación,…).

  Puesta en marcha del centro de recuperación:

  Una vez concentrados los distintos equipos que van a intervenir en la recuperación, y con todos los elementos necesarios disponibles para comenzar la recuperación, hay que poner en marcha este centro, estableciendo la infraestructura necesaria, tanto de software como de comunicaciones, etc.

- Fase de recuperación: En esta fase, una vez establecidas las bases para comenzar la recuperación, se procederá a la carga de datos y a la restauración de los servicios críticos. Este proceso y el anterior suelen precisar los mayores esfuerzos e intervenciones para cumplir con los plazos prefijados. En esta fase se pueden distinguir dos elementos:

    - Procedimientos de restauración: Se refiere a los procedimientos de restauración de los sistemas críticos.

    - Procedimientos de soporte y gestión: Una vez restaurados los sistemas hay que comprobar su funcionamiento, realizar un mantenimiento sobre los mismos y protegerlos, de manera que se reanude el negocio con las máximas garantías de éxito. Los integrantes del equipo de unidades de negocio serán los encargados de comprobar y verificar el correcto funcionamiento de los procesos.

4. Fase de vuelta a la normalidad

Después de ocurrido el siniestro es necesario realizar las actividades que siguen:

- Celebración de reuniones: Por un lado se celebrará una reunión de planificación de vuelta a las instalaciones restauradas, dirigida por el equipo de gestión de incidentes (que forma parte del equipo de recuperación), y que abrirá una discusión sobre las estrategias generales de regreso.

  Y por otro lado se celebrará una sesión de planificación de cada equipo de recuperación, dirigida por su coordinador, para revisar y actualizar los procedimientos de recuperación del negocio (incluyendo procedimientos de respuesta) ante el retorno a las instalaciones permanentes desde el lugar alternativo.

- Evaluación de daños: Inmediatamente después de que el siniestro ha concluido, se deberá evaluar la magnitud del daño

que ha producido, qué sistemas han sido afectados, qué equipos han quedado no operativos, cuáles se pueden recuperar, cuánto tiempo será necesario, etc.

Adicionalmente se deberá lanzar un preaviso a la institución (si la hubiere) con la cual tenemos convenio de respaldo, para ir avanzando las labores de preparación de entrega de los equipos por dicha institución.

- Priorización de actividades del plan de acción: Toda vez que el plan de acción es general y contempla una pérdida total, la evaluación de daños reales y su comparación contra el plan, nos dará la lista de las actividades que debemos realizar, siempre priorizándola en vista de las actividades estratégicas y urgentes para nuestra entidad. Es importante evaluar la dedicación del personal a actividades que puedan no verse afectadas, para ver su asignación temporal a las actividades afectadas, en apoyo al personal de los sistemas afectados y soporte técnico.

- Ejecución de actividades: Implica la creación de equipos de trabajo para realizar las actividades previamente planificadas. Cada unos de estos equipos deberá contar con un coordinador que deberá reportar diariamente el avance de los trabajos de recuperación y en caso de producirse algún problema, reportarlo de inmediato a la jefatura a cargo del plan de contingencia. Los trabajos de recuperación tendrán dos etapas, la primera la restauración del servicio usando los recursos de la entidad o del local de respaldo, y la segunda etapa es la de volver a contar con los recursos en las cantidades y lugares propios del sistema de información, debiendo ser esta última etapa lo suficientemente rápida y eficiente para no perjudicar el buen servicio de nuestro sistema e imagen de nuestra entidad y para no perjudicar la operatividad de la entidad de respaldo.

- Evaluación de resultados: Una vez concluidas las labores de recuperación del sistema que fueron afectados por el siniestro, debemos evaluar objetivamente, todas las actividades

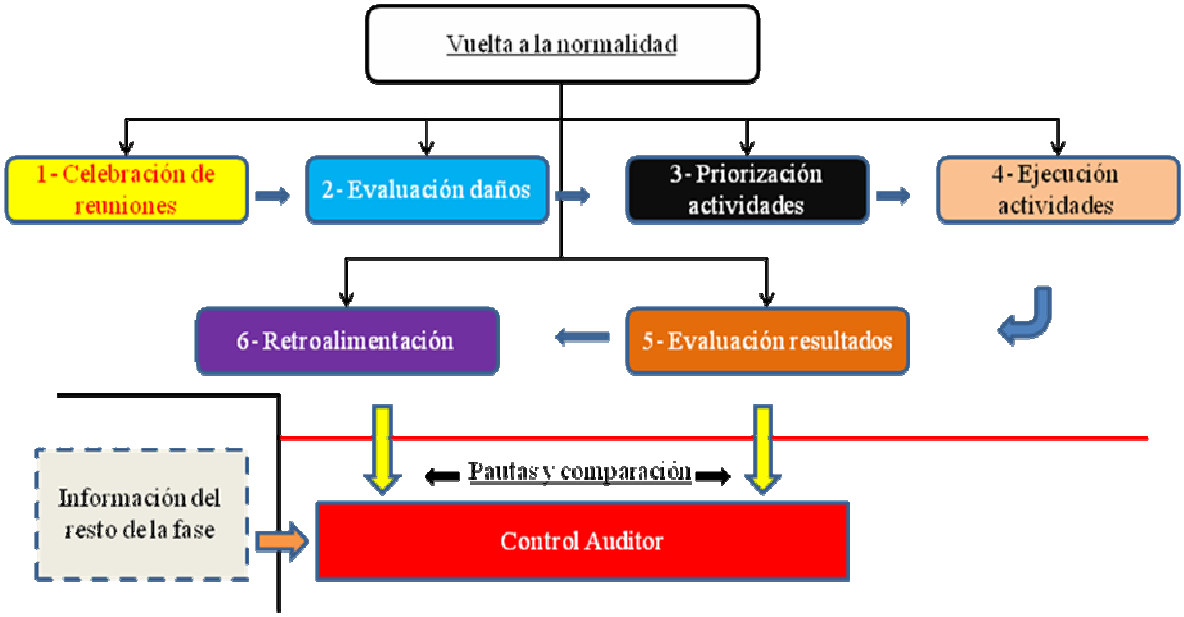
realizadas, si se hicieron bien, qué tiempo requirieron, qué circunstancias comportaron y modificaron (aceleraron, entorpecieron, interfirieron, etc.) las actividades del plan de acción, cómo se comportaron los equipos de trabajo, etc.

De la evaluación de resultados y del siniestro en sí, deberían salir dos tipos de recomendaciones, una retroalimentación del plan de contingencias (como veremos seguidamente), y una lista de recomendaciones para minimizar los riesgos y pérdidas que ocasionó el siniestro.

- Retroalimentación del plan de acción: Con la evaluación de resultados, debemos de optimizar el plan de acción original, mejorando las actividades que tuvieron algún tipo de dificultad y reforzando los elementos que funcionaron adecuadamente. El otro elemento es evaluar adecuadamente cual hubiera sido el costo de de no haber tenido en nuestra entidad un plan de contingencias realizado.

Finalmente desarrollaremos un programa aprobado y revisado con todo el personal participante de los equipos de recuperación. Y la puesta en marcha de los procedimientos modificados de recuperación del negocio, reanudando las operaciones en el lugar de trabajo permanente.

Cuadro de vuelta a la normalidad y su interacción con el control auditor:



Evaluación en esta fase:

El contenido del plan debe ser el resultado final de la ejecución del proyecto y el desarrollo del mismo. Ha de estar debidamente aprobado y formalizado por escrito de forma pormenorizada, con el fin de minimizar la toma de decisiones llegado el caso de tener que ponerlo en práctica.

La revisión del contenido del plan tiene por objeto comprobar que responde al proyecto autorizado y elaborado según los criterios expuestos; y que, siguiendo las instrucciones y procedimientos indicados y utilizando los medios y recursos definidos, el equipo de recuperación podrá dar respuesta a una situación de emergencia en las actividades, garantizando la continuidad de las mismas y la prestación de servicios a la organización con los niveles de calidad y puntualidad previstos en el plan en función del alcance o gravedad del siniestro. Las siguientes cuestiones nos permitirán,

como controladores o auditores, valorar si el plan cumple con los objetivos propuestos debido a la naturaleza de ejecución del plan propia de esta fase:

¿Están contemplados y definidos los posibles sucesos que pudieran ocurrir y las situaciones, diferentes de la normalidad, que se pudiesen dar?

¿Se determina con precisión el procedimiento a seguir antes de declarar la situación de emergencia, así como las personas que, en su caso, deben efectuar dicha declaración?

¿Están contempladas las actuaciones de respuesta para recuperar la actividad y definidas según un orden de prioridades?

¿Se asignan responsabilidades en su ejecución (actuaciones), que son conocidas por los empleados designados y éstos cuentan con la formación y entrenamiento necesarios para caso de siniestro?

¿Se han identificado claramente y tenido en cuenta los componentes de un procedimiento de respuesta ante una emergencia?. Tanto los de información (interna y externa), como los de preparación previa al desastre, las acciones de emergencia, estabilización de las instalaciones, atenuación del daño y procedimientos de prueba y asignación de responsabilidades.

¿Existe un equipo o comité de dirección de la reanudación y un responsable del mismo para dirigir y coordinar las distintas actividades durante la contingencia o desastre?

¿Del equipo de reanudación o recuperación y de cualquier otro previsto en el plan, se han definido sus componentes y funciones, así como los procedimientos y actividades que cada equipo ha de realizar para cada uno de los niveles de siniestro contemplados, incluida la reconstrucción del centro de proceso de datos si fuese necesario?

¿Para la reanudación del funcionamiento de las aplicaciones críticas, están definidas las necesidades de hardware, software y comunicaciones?

¿Están definidas unas normas sobre copias de seguridad de ficheros, que están aprobadas, actualizadas y se cumplen?

¿Están definidos unos procedimientos de obtención de copias de forma controlada y éstas se renuevan en los períodos establecidos?

¿Existe un inventario detallado de las copias de seguridad necesarias para la recuperación de los ficheros de las aplicaciones críticas y están definidas sus características?

¿La documentación correspondiente a las aplicaciones críticas existe y al igual que las copias de seguridad de los ficheros se conservan en otro edificio?

¿Están definidas las condiciones de custodia, acceso y uso de las copias de seguridad?

¿Está detallada la ubicación del centro alternativo de respaldo de proceso de datos, así como la configuración del mismo?

¿En relación con dicho centro, también se contemplan los requerimientos de hardware, software de explotación, ficheros, acuerdos con los proveedores, así como la inclusión del software de seguridad de dicha instalación?

¿Se ha tenido en cuenta el área de comunicaciones, las redes corporativas y las redes de área local?

¿De los ordenadores personales que tienen información crítica existen procedimientos de recuperación específicos?

¿Están definidos unos procedimientos manuales de respaldo?

¿Se han desarrollado procedimientos detallados de respuesta ante emergencias? Tanto de protección del personal, como para atenuar el impacto, evaluar los daños y decidir acciones a tomar.

¿Se han identificado todas las necesidades de dirección y control, así como sus procedimientos?

¿Se ha creado un equipo para el salvado y restauración y definido una estrategia para la actividad inicial in situ?

¿Se puede deducir de la experiencia de los siniestros acontecidos en el pasado alguna conclusión que no se corresponda con el estado actual del plan? ¿Han cambiado las estrategias y por tanto es necesario reorientar el plan y por eso no es posible unas el revisionismo de la fase de revisión de esta fase?

¿Se han desarrollado y probado los procedimientos para asignación de prioridades en la respuesta ante emergencias? (Esta entraría más en la siguiente fase de pruebas).

Asimismo después de hacerse todas estas preguntas, a las cuales incluso podríamos poner una puntuación para darnos una idea del grado de desarrollo de la fase, las respuestas nos ayudarán a comprobar el grado de efectividad y correspondencia de esta fase del plan y por otra parte y aprovechando que en esta fase se incluye, en el apartado de vuelta a la normalidad, una evaluación de resultados, para revisar este apartado y comprobar que esas mejoras se han hecho efectivas de haberse producido algún siniestro y han sido consideradas en caso de haber algún fallo aprovechando la experiencia adquirida o recomendar algún cambio si las circunstancias hubieren cambiado.

En esta fase se determina la calidad del plan y comprobamos su efectividad por tanto es primordial un análisis diligente por parte de auditores tanto internos como externos, por otra parte se puede concluir que las valoraciones en este apartado de la fase de auditoría garantizarán el nivel y la calidad de los servicios de la entidad, dentro de los plazos previamente determinados.

9. Mantenimiento y Pruebas

Si la finalidad del plan es dar una respuesta los más rápidamente posible a una interrupción de actividades, con motivo de un incidente o siniestro, es imprescindible que para satisfacer dicha finalidad esté totalmente actualizado.

Igualmente, para garantizar su eficacia, el plan debe ser probado periódicamente, además de cuando se produzcan modificaciones en el

entorno informático que de alguna manera afecten a su contenido y puesta en marcha (como veremos en la parte de control de esta fase).

En el desarrollo del mantenimiento de un plan se llevarán a cabo las pruebas del plan de contingencia, que en esta fase son absolutamente necesarias, y sobre todo se realizarán antes de su aplicación práctica, pero también después de una contingencia como consecuencia del amejoramiento progresivo y la reorientación estratégica de objetivos de la entidad a través del informe de resultados de dichas pruebas. El programa de mantenimiento, establecerá pruebas o entrenamientos que serán periódicos de todo el personal en la lucha contra todo tipo de siniestros, de acuerdo a los roles que se le hayan asignado en los planes de evacuación del personal o equipos; para minimizar costos se pueden aprovechar fechas de recarga de extintores, charlas de los proveedores etc.

Un aspecto importante es que el personal tome conciencia de que los siniestros pueden ocurrir realmente, y tomen con seriedad y responsabilidad estos entrenamientos, para estos efectos es conveniente que participen los elementos directivos, dando el ejemplo de la importancia que la alta dirección otorga a la seguridad institucional.

Por tanto se hace necesaria una campaña de sensibilización de los responsables de los departamentos y de la organización en su conjunto, para conseguir un procedimiento auténticamente efectivo del propio plan.

El proceso de concienciación tendrá un seguimiento para informar de los resultados obtenidos. Las pruebas nos permitirán evaluar de forma fehaciente que el plan corresponde a lo necesario y que en función de los resultados podremos adaptarlo en función de la evolución de la entidad.

Por tanto se puede afirmar que las pruebas son parte esencial de los cometidos en el mantenimiento de un plan de contingencia.

Por consiguiente, con el mantenimiento del plan buscamos una serie de objetivos:

- Buscamos que el personal esté preparado para utilizarlo.
- Buscamos mantener el plan actualizado y adaptado a las necesidades de la entidad.

Para llevar a cabo estos objetivos, el plan de mantenimiento debe estar constituido por los siguientes elementos:

- Revisiones periódicas
- Pruebas

Una vez llevados a cabo las revisiones o ejercicios debemos actualizar el plan si así nos lo indican los parámetros obtenidos durante estas revisiones. No obstante muchas de las actuaciones de dichas revisiones se solaparían con algunos trozos de las auditorías de otras fases, de todos modos como formalidad por parte del personal encargado del plan de contingencia es un complemento más para que el plan deba funcionar correctamente.

1) Revisiones: En este apartado comprobaríamos algunas facetas propias del plan, y si están debidamente actualizadas. Por ejemplo hablaríamos de comprobar si los recursos de recuperación están disponibles incluyendo las copias de seguridad de almacenamiento externo. Si los umbrales de recuperación son los adecuados, si ha habido algún cambio en la criticidad de algún proceso, y que por tanto ahora es imprescindible su inclusión en el inmediato proceso de recuperación, etc. Por consiguiente este apartado nos permite en cierta manera un revisionismo de algunas de las facetas propias del plan que, como dijimos, pueden solaparse con cometidos propios del auditor realizadas en alguna otra fase, pero que son imprescindibles como formalidad y permiten asentar y asegurar los cometidos que buscamos dentro de la recuperación en el plan de contingencia.

2) Pruebas: Este tipo de ejercicios servirá para tener bien definido el modus operandi del plan de contingencia y que los miembros del equipo asienten y se familiaricen con la forma de proceder y realizar la acción del plan de contingencia ante una emergencia. A estas sesiones asistirán todos los componentes del equipo. El plan de continuidad no se considerará válido hasta que no se hayan superado satisfactoriamente las pruebas que aseguren la viabilidad de las soluciones adoptadas.

La diferencia entre revisión y prueba vendría determinada más bien por el carácter de simulación de las pruebas ante un siniestro, mientras que la revisión se centraría más en la consulta de parámetros del plan sin

hacer referencia, ni provocar una simulación de un siniestro. Ambos conceptos quedarían englobados en el mantenimiento general de un plan y nos permiten evaluar con certeza su funcionamiento y adecuación a los objetivos estratégicos de nuestra entidad.

Los objetivos del mantenimiento y por extensión de las pruebas son:

Proporcionar una revisión y entrenamiento de la capacidad de recuperación.

Ensayo del plan en una situación de contingencia simulada.

Evaluar la capacidad de respuesta ante una situación de desastre que afecte a los recursos de la entidad.

Probar la efectividad y los tiempos de respuesta del plan para comprobar que están alineados con la definición realizada en el diseño.

Identificar las áreas de mejora en el diseño y ejecución del plan.

Revisar y actualizar la documentación del plan.

Identificar información perdida o incorrecta.

Comprobar si los procedimientos desarrollados son adecuados para soportar la recuperación de las operaciones de negocio.

Evaluar si los participantes del ejercicio están suficientemente familiarizados con la operatividad en situación de contingencia.

Concienciación y formación para los empleados a través de la realización de pruebas.

Evaluación de la exactitud de responsabilidades del equipo y de los procedimientos de recuperación.

Para que el funcionamiento del plan sea el adecuado, no queda más que realizar una serie de pruebas y comprobar de esa manera el buen funcionamiento de los métodos y las tecnologías. Algunos elementos requerirán de pruebas reales para asegurar que todo funciona según lo previsto. Las recomendaciones para realizar las pruebas se basarán en experiencias anteriores de pruebas, revisiones o contingencias

reales que nos guíen de la mejor manera posible en la elaboración y refinamiento de las pruebas. De tal manera que podremos basar nuestras pruebas en dos niveles:

Por un lado podemos optar por la solución del realismo para poder conferir un grado de autenticidad, que nos permita emular un escenario real con el cual con probabilidad nos enfrentemos y que nos permitirá ceñirnos con gran proximidad a lo que nos podamos enfrentar en un caso real. La desventaja de esto es que requiere de un gran esfuerzo por parte de la entidad y un consumo de gran cantidad de recursos, no obstante la evaluación de la adecuación de estas pruebas será dictada por el propio equipo que se encargue de llevar a cabo las pruebas.

Por otro lado y como alternativa al procedimiento anterior se podría adoptar la solución de la exposición mínima que trata de impactar mínimamente en el funcionamiento normal del negocio, es decir pretende que la prueba no suponga una parada de los sistemas de información o que esta sea de lo más mínima, sobre todo aprovechando momentos en los que impacte menos en el funcionamiento de la entidad.

En ocasiones puede resultar especialmente complicado desarrollar las pruebas de un plan de contingencia completo. Por ello es imprescindible desarrollar un plan de pruebas planeado para que se garantice que se han desarrollado todas las facetas del plan y que todo el personal requerido para su puesta en marcha ha practicado el mismo.

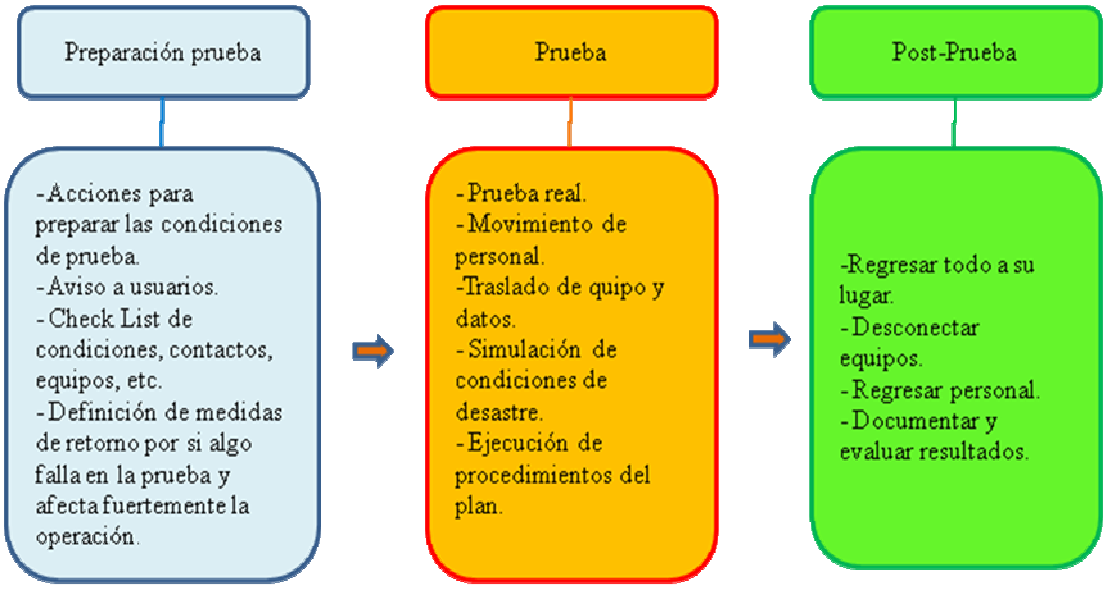
Gran parte del funcionamiento del plan se basa en el funcionamiento correcto de la tecnología, es fundamental por tanto la comprobación de estos elementos para cerciorarse del funcionamiento correcto de la misma. Las recomendaciones en torno a estas tecnologías serán fundamentadas en torno a la experiencia de muchos ejercicios de recuperación surgidos tanto por contingencias reales como por entrenamientos o pruebas.

La forma de secuencia en la ejecución de pruebas, sería:

1. Planificación previa de la prueba.

2. Coordinación de la misma con los departamentos competentes.
3. Ejecución de la prueba.
4. Evaluación de resultados.
5. Documentación de los resultados.
6. Actualización del plan.
7. Informar a la dirección de los resultados y la evaluación de la prueba.

Cuadro que refleja la evolución de la realización de las pruebas:



Elementos que se desarrollan/afectan durante las pruebas:

Especificaciones:

Medir la capacidad del lugar de respaldo.

Evaluar la capacidad de recuperación de registros vitales.

Evaluar estado y cantidad de equipos y suministros en el lugar de recuperación.

Medir el desempeño general de actividades operativas y de sistemas.

Verificar si el plan es completo y preciso.

Evaluar el desempeño del personal involucrado.

Evaluar el entrenamiento y conocimiento del personal que no pertenece a la entidad, y que intervenga en el plan.

Evaluar la coordinación entre el equipo de continuidad y proveedores externos.

Análisis de resultados: Tiempo, cantidad, conteo, exactitud.

Factores que impactan: Cambios en la organización, Nuevos recursos aplicaciones, cambios en la estrategia del negocio, cambios software o hardware.

Responsabilidades del plan, (implican):

Desarrollar un plan para revisión y mantenimiento periódico.

Exigir revisiones no programadas ante cambios significativos.

Examinar las revisiones y actualizarlas después de las revisiones.

Coordinar pruebas programadas y no programadas para evaluar suficiencia.

Participar en las pruebas anuales.

Actualizar lista de contactos.

Dentro del elenco de pasos que seguimos en la ejecución de pruebas se realizarán una serie de ejercicios técnicos que requerirán la ejecución de procedimientos de notificación, operativos, uso de hardware y software, y la utilización de métodos y centros alternativos para asegurar un rendimiento adecuado.

De la misma manera que se puede realizar una prueba o test del plan de contingencia entero que podríamos llamar prueba operativa completa, se pueden realizar pruebas parciales si así se requiriese en un determinado momento, que requerirán de una acción “real” o simulada.

Podemos resumir que el mantenimiento del plan es una parte esencial del plan, sin él no podremos evolucionar nuestro plan dentro de nuestra entidad y no se conseguirán los objetivos deseados de todo plan de contingencia. Por tanto es imprescindible desarrollar con total completitud las pruebas determinadas por el mantenimiento que nos permitirán tener un plan de contingencia que aportará estabilidad y vigor a nuestro plan y por extensión nos hará más competitivos en los sistemas de información dentro del mundo empresarial actual.

Control de la fase de mantenimiento y pruebas

Como hemos realizado en otras fases, el control de esta fase no es menos importante, y por tanto es necesario un control pertinente que nos permita asegurar el funcionamiento y adecuación de las pruebas y su mantenimiento a los objetivos primordiales del plan de contingencia. De esa manera aseguraremos quizá la parte que mejor nos guíe en la realización práctica efectiva de un plan de contingencia.

Dependiendo del alcance o magnitud de las modificaciones, las labores de adaptación del plan pueden realizarse directamente variando su contenido (por ejemplo, los cambios de personal o las direcciones de localización de proveedores), o requerir un proceso más laborioso incluyendo la repetición de fases de desarrollo del plan, (por ejemplo, con motivos de modificaciones significativas de aplicaciones o de implantación de otras nuevas).

Las principales causas para la actualización del plan son las siguientes: añadir, cambiar, o eliminar responsabilidades de la función; el cambio de personal; las mejoras tecnológicas que se incorporen (hardware y software); y la variación en el resultado del análisis de riesgos o del impacto de la actividad.

El objetivo de este apartado es verificar si se realizan puntualmente las labores de mantenimiento y pruebas del plan, en consonancia con las modificaciones e innovaciones del entorno informático, de forma que dicho plan se encuentre siempre a punto para ponerlo en marcha si fuera necesario.

Las respuestas a las siguientes cuestiones permitirán valorar si el mismo cumple los objetivos propuestos.

Para todo ello debe comprobarse si se han llevado a cabo una serie de actividades:

¿Están designadas las personas responsables del mantenimiento del plan?

¿Está definido un calendario de actualizaciones para las diferentes funciones?

¿Se cumplen los plazos establecidos para la revisión y actualización del plan?

¿Ante cambios significativos en los recursos de la empresa o en el entorno en el que se encuentra, se realiza una actualización del plan?

¿Las actualizaciones realizadas se registran?

¿Se han planificado las pruebas del plan y establecido plazos, motivos y responsable de las mismas?

¿Las pruebas se realizan puntualmente dejando constancia documental y se corrigen los fallos detectados?

¿Existe un desarrollo de programas de revisiones del plan? Si es así:

¿Siguen siendo críticas las funcionalidades revisadas?, ¿Se sigue revisando si cumplen con los umbrales de recuperación establecidos?, ¿Se han incluido en las revisiones nuevas funcionalidades que antes no eran críticas?

¿Se han llevado a cabo entrenamientos para la formación del personal y que puedan desarrollar las revisiones o pruebas?, ¿Están definidos los

objetivos de los entrenamientos?, si es así. ¿Se refleja su efectividad en las experiencias o siniestros del plan acontecidos anteriormente?

¿Se ha establecido un programa de pruebas?, si es así, ¿cubre los siguientes puntos?:

¿Tiene un enfoque lógico y estructurado?, ¿Pone en peligro la continuidad de las operaciones?, ¿Es práctica y apropiada a la organización?, ¿Es limitada y eficaz en el coste?, ¿Asegura un alto nivel de confianza en la capacidad de recuperación?, ¿Tiene un conjunto de directrices adecuado?, ¿Establece una periodicidad realista?, ¿Tiene una asignación adecuada de recursos?

¿Existe una definición adecuada de las necesidades de las pruebas?, si es así: ¿Existe una identificación de tipos de pruebas?, (simulaciones, pruebas modulares, pruebas funcionales, pruebas anunciadas, pruebas por sorpresa), ¿Cuál de ellas nos aporta éxitos o ventajas?

¿Se han creado escenarios realistas que se corresponden con incidentes probables?, si es así: ¿Se ha entrenado a los miembros del equipo de recuperación ante situaciones nuevas?, ¿Se han probado las comunicaciones, métodos de documentación y registros del centro de control?

¿Existe una serie de criterios de evaluación objetivos de los resultados de las pruebas?

¿Se ha seleccionado la metodología de pruebas más adecuada?

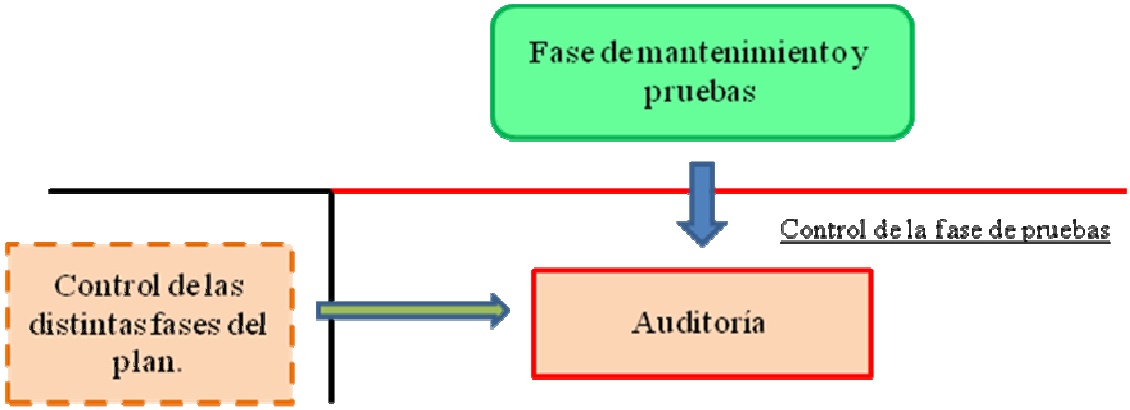
¿Se han definido con certeza los objetivos de las pruebas?

¿Se ha especificado un plan de controles de las pruebas y un método de información de los resultados a la dirección?

¿Qué acciones correctoras y de retroalimentación son resultado de las pruebas, y si son adecuadas?

¿Existen procedimientos adecuados para el control de cambios?

Cuadro de la parte de control de la fase de mantenimiento y pruebas:



Finalmente haríamos referencia en esta parte de control de la fase de mantenimiento a una serie de cuestiones que afectarían a la auditoría o fases de control propiamente dichas del plan, ya que esta permitirá mantener adecuadamente unos criterios objetivos y efectivos para el mantenimiento de cada una de las fases del plan, por tanto el cuestionamiento de las auditorías en esta fase nos dará una idea de la adecuación de los criterios auditores seleccionados y si por tanto estos han de continuar o han de ser cambiados:

¿Se han enunciado unos objetivos para la auditoría del plan? (conocimiento de los métodos y opciones de auditorías, estructuras viables para controlar las diferentes fases y recomendar unos objetivos consensuados y un alcance de la auditoría).

¿Qué metodología auditora se ha seleccionado? (Comprobar si es necesario realizar un estudio preliminar, qué tipo de desarrollo de actividades es necesario, evaluar los recursos para dichas actividades, establecer prioridades y ver cuál de las técnicas auditoras es más conveniente).

¿Se han auditado los aspectos administrativos del plan? (Entrenamientos, documentación, organización, registros vitales, instalaciones alternativas, contratos, ciclos de obtención de copias y logística).

¿Se ha auditado la estructura del plan? si es así: ¿Cubre aspectos de recuperación?, ¿con los procedimientos de emergencia adecuados?

¿Se han auditado los procedimientos de control de la documentación? (Determinación de si el personal clave dispone de una copia, revisión de los procedimientos de actualización y comprobar si son efectivos, examinar si existen copias de seguridad, qué personas disponen de una copia y asegurarse de que dichas copias estén actualizadas).

Finalmente este control de la auditoría nos permitiría en definitiva tener bien descrito y planificado el método de control de las fases, por tanto calibrando este aspecto último del plan se podría dar por concluido y completamente finalizado sin ningún tipo de descontrol el plan de contingencia referente a los sistemas de información de una entidad.

10. Desarrollo de ejemplos (Parte práctica):

Para ir viendo el desarrollo práctico de los ejemplos hablaremos del ejemplo como ejemplo 1.

Ejemplo 1:

Propondremos como ejemplo para nuestro plan de contingencia una fábrica de envases. En esta fase proponemos un conocimiento acabado de lo que concierne al negocio en sí, cada uno tendrá su propia naturaleza y de su conocimiento sacaremos las decisiones más adecuadas.

Un análisis de este negocio nos llevaría a determinar diferentes facetas como por ejemplo: Objetivos básicos de este negocio serían el de proveer de envases a todos los clientes que nos solicitasen pedidos, también habría que clarificar si los envases son únicamente para el mercado alimentario o si bien tenemos alguna sección de envases de uso industrial. Qué tipo de envases de cada uno de los sectores llevamos a cabo, si bien o son simplemente para contener líquidos o bien se

realizan para todo tipo de elementos. También los materiales, si determinados productos requieren condiciones especiales etc. y cuáles son los proveedores de los materiales. El conocimiento de esto nos permitirá determinar con exactitud cuáles serán los procesos críticos ya que por ejemplo si nuestra fortaleza como fábrica y como empresa radica en la entrega de envases industriales, y el de envases alimentarios fuese menor, los procesos relacionados con los primeros serían de primordial importancia. Por tanto es imprescindible un buen conocimiento del negocio y de los procesos relacionados con cada uno de los sectores del propio negocio.

En este caso que nos compete vamos a suponer que la fábrica está radicada en Madrid, constituida esta sede en sede central y donde existe otra parte de la fábrica en Valencia. Esta fábrica por lo pronto es solvente y tiene un gran número de clientes tanto nacionales como extranjeros.

Esta fábrica tiene un departamento de informática que está formado por diez personas que se encargan de la gestión de todo lo relacionado con los sistemas de información, es decir, software, hardware, comunicaciones, bases de datos, etc. Este departamento y su centro de proceso se encuentran en Madrid.

Esta fábrica se ha desarrollado rápidamente gracias al auge de su negocio y por tanto eso se ha traducido en un importante y rápido desarrollo de los procesos de soporte, tales como nóminas, facturación, atención al cliente, captación de proveedores, etc. Sin embargo las políticas de seguridad no han crecido al mismo ritmo que la compañía y por tanto han quedado en una situación de clara obsolescencia. Las políticas que antaño fueran llevadas a cabo por la que fue una pequeña compañía con solo dos empleados en el departamento de informática ha devenido en diez y estos han seguido como empleados que desempeñan las tareas que se venían haciendo pero sin un rediseño completo ni una redistribución competencial del trabajo, ni una revisión de los objetivos primordial, lo que ha llevado a la entidad a una indefensión desde el punto de vista computacional. La empresa consta de dos edificios uno en Madrid de dos plantas y otro en Valencia, que se constituyó más tarde, de una sola planta.

La política de seguridad actual por tanto es la que había anteriormente y consiste en:

No existe política de seguridad general diseñada de manera específica.

Sólo existen antivirus en algunos equipos básicamente los primeros de la compañía, en los demás no existen.

No se han realizado y no se realizan copias de seguridad ni salvados de información.

El control de acceso a los equipos es a través de contraseñas pero compartidas y no se renuevan cada cierto tiempo.

Los servidores se encuentran en una sala sin ningún tipo de protección física, y las medidas de control de acceso por parte de cualquier empleado de cualquier departamento no están siendo controladas.

No existen análisis de riesgos, ni un diseño prefijado, ni planes de contingencia. Sólo existe un protocolo de emergencia para el salvamento de personas de los edificios de la empresa.

Al necesitar de un análisis del negocio colocamos en esta parte el ejemplo, no obstante, debemos decir que de la fase anterior del comienzo de un plan de contingencia, (objetivos del plan de contingencia y su control) se englobarían las primeras preguntas y controles en torno a la seguridad de esta empresa respecto al plan de contingencia como veremos. No obstante la presentación del tipo y forma de la empresa sus empleados etc. es el análisis de la naturaleza de la empresa y por tanto hemos decidido comenzar aquí la presentación del ejemplo por una cuestión de practicidad, pero como distinguiremos cuando se lleve a cabo la labor de desarrollo del plan de contingencia veremos cómo se comienza en la anterior fase y los asuntos que le competen en aquella.

La dirección de informática de nuestra empresa se propone la realización de un plan de continuidad del negocio, para llevar a cabo una estrategia de

recuperación ante cualquier siniestro que haga peligrar el negocio en nuestra empresa.

Objetivos del plan de contingencia y su control

En esta fase surge pues la necesidad de llevar a cabo unos objetivos, básicamente la génesis de la proposición del director de informática se basa en una serie de carencias que son manifestadas como imprescindibles en cuanto al desarrollo de la actividad empresarial se refiere. Como vimos en esta fase desde minimizar las potenciales pérdidas económicas o reducir riesgos potenciales a aportar una ventaja competitiva frente a la competencia. Estas premisas básicas para acometer un plan de negocio son las que nos motivan para llevarlo a cabo y es en la parte de control de esa fase donde se manifestarían, tanto en controles internos como en auditorías externas, las carencias manifiestas de esta entidad; no obstante como digo esta empresa adolecía de controles, es por tanto en este caso que ha sido el director del departamento de informática, conocedor de las debilidades de nuestro sistema de información, quien ha propuesto que se lleven a cabo el diseño y realización los planes de contingencia.

El control pertinente en esta fase enseguida habría revelado las carencias, como por ejemplo:

¿Existe un plan de contingencia?, en este caso no existe. Las preguntas relativas a las consecuencias de haberlo tenido, por tanto, no tienen sentido. No obstante se podrían plantear otro tipo de cuestiones, que son de la misma parte de control y que nos permitan saber si existe otro tipo de control

¿Existe una política que sustente el plan?, ¿Es parte de un plan de recuperación y seguridad global?, La contestación es que no existe ningún tipo de política de seguridad, la única medida tomada al respecto es la presencia de antivirus, y solo en aquellos computadores presentes durante más tiempo en la entidad, es decir en las ampliaciones ni siquiera se tomó dicha medida. Es evidente que aquí no estableceremos ningún tipo de puntuación, por ser esta evaluación de índole esencial y no práctica propia del plan de contingencia.

Por lo tanto queda clara la revisión total de la política de seguridad de la entidad. En este caso el desarrollo en esta fase queda sentado para el diseño y acometimiento de un nuevo plan seguridad, donde estará presente el plan de continuidad del negocio. Por otra parte según vayamos desarrollando el plan de contingencia necesario para esta entidad, estableceremos el desarrollo de los controles pertinentes para cada una de las fases que se desarrollarán a lo largo de este ejemplo. Como se verá, el acometimiento del plan puede ser ajustado a la realidad o presentar deficiencias, es por tanto cometido de las partes de control de cada una de las fases determinar la adecuación del plan de contingencia para nuestra entidad. Evidentemente este tipo de revisiones se puede realizar inmediatamente después de haber de realizado el plan, o después de un tiempo o siniestro.

Como hemos hecho referencia en el desarrollo teórico, el plan de contingencia viene activado por una serie de acontecimientos que se han producido cuando todas las demás medidas de seguridad han fallado, por tanto mención aparte del plan de seguridad que desarrollaremos, tenemos que presuponer que una vez adquirida la conciencia por parte de la entidad, de la importancia de la seguridad en cuanto a sistemas de información se refiere, se habrá adoptado no sólo un plan de contingencia, sino unas medidas de seguridad propias de un plan general de seguridad, que como digo, estarán presupuestas o haremos referencias a ellas en determinados momentos, ya que es una ligazón imprescindible para la seguridad integral de una organización. No obstante nos centraremos, primordialmente, en el desarrollo del plan de contingencia y su revisión o control.

Iniciación y gestión del plan de contingencia y su control

Ayudar a la dirección en la fijación de objetivos y políticas:

Antes del análisis del negocio en esta fase pretendemos ayudar a la dirección en la fijación de objetivos y políticas. Por lo tanto el responsable del departamento de informática de esta empresa tendrá que presentar una serie de documentos, y la proposición correspondiente de plan de contingencias, qué recursos serán necesarios y otros requisitos para que la

dirección avale y confirme la puesta en marcha del plan de contingencia. Es imprescindible por tanto todo el apoyo de la entidad en este caso y en particular de la alta dirección como se indicó en el apartado teórico correspondiente. En este ejemplo se realizan las debidas reuniones y es autorizado por parte de la dirección el plan de contingencia.

Para su **revisión** haremos las preguntas pertinentes y comprobaremos si ha procedido a su control tal y como indicamos en el desarrollo teórico:

¿Está aprobado por la dirección? ¿El plan se elaboró con arreglo a un proyecto documentado y autorizado que se conserva adecuadamente?; Estas preguntas nos indican la autoridad e importancia que la entidad a través de los directivos conceden al plan, y si está debidamente tratado y guardado, por tanto nos permitirá discernir si es competente. En este caso concreto del de ejemplo 1, el responsable de informática de nuestra empresa ha presentado los documentos pertinentes no solo del plan de seguridad general sino de la plan de contingencias en particular, estando de acuerdo la alta dirección de la empresa aprobándolo, y por tanto avalando el proyecto de seguridad integral y el plan de contingencia que engloba. Por tanto en este caso en el control pertinente ante la instauración del plan de contingencia revelaría que esta todo correctamente documentado y aprobado, informando favorablemente.

Estableceremos un conjunto de puntuaciones en cada punto analizado de tal manera que nos puedan indicar a través de números cuán bien está desarrollada la fase y que puntuación se otorga. De esa manera podremos ponderar, como dijimos al inicio del desarrollo de los ejemplos, la situación de cada una de las fases en función de las puntuaciones obtenidas por la evaluación de éstas. Como vemos en el cuadro siguiente sobre puntuación en la parte de esta fase se han calibrado las puntuaciones en función de los puntos que ha cumplido nuestro equipo de informática en cuanto a resolución del plan de contingencia se refiere. Como vemos la puntuación objetivo, es decir, la puntuación equilibrada que buscamos es de 3, que es la que realmente proveerá de un plan justo a nuestra organización. Evidentemente las puntuaciones en algunos casos pueden ser algo subjetivas pero reflejan con cierta exactitud la realidad del plan, y por tanto nos sirven para limar o aumentar el grado de implicación en las fases en

función de ellas, en nuestro caso en concreto, mientras evaluamos, consideramos que los dos primeros puntos reflejan fielmente la realidad que buscamos mientras que el tercero se queda algo corto, no obstante la puntuación es buena y por tanto consideramos que en esta parte de esta fase se cumplen las expectativas de los puntos a tratar.

Puntuación:

Iniciación y gestión del plan de contingencia y su control		**Puntuación**
1	Se ha involucrado a la alta dirección en el proyecto de los planes de contingencia	3
2	Se ha involucrado a la alta dirección y se ha obtenido su aprobación y compromiso	3
3	Se han definido las necesidades de documentación y gestión del proyecto	2
4	Puntuación en la sección	8
5	Nota media	8/3=2,66
6	Puntuación objetivo	9
7	Nota media objetivo	3

El alcance del negocio se determinará en función de las funciones críticas que vayamos viendo a lo largo del proceso del desarrollo del plan de

contingencia, por tanto estableceremos la criticidad de las operaciones después de los análisis pertinentes.

El director o coordinador del departamento de informática conoce perfectamente los entresijos de la organización y por tanto sabe cuál será el alcance del plan. La empresa ha adoptado la solución estratégica de fabricar los envases en Madrid como consecuencia de su proyección nacional inicial, ya que administrativamente, se situarían en la capital, donde existen más oportunidades de mercado y de personal cualificado no solo en la propia producción, sino también el nivel administrativo y cualificado en entornos informáticos. Mención aparte que la situación central en la península nos aporta una ventaja de reducción de costes de transporte al ser el lugar más cercano a todos los puntos. Por otra parte ante la expansión internacional se eligió Valencia por ser el puerto más cercano a Madrid, y desde ahí distribuir las mercancía a Europa y otros países. Por tanto nuestro centro de producción y también de distribución nacional es Madrid, y nuestro centro de distribución internacional es Valencia. Como consecuencia nuestro sistema de información principal estará en Madrid, y seguidamente en importancia será el de Valencia. Donde el departamento de informática en este caso tiene muy claro qué es lo que hay que proteger. En este caso protegeremos dichos sistemas y la información tratada en torno a ellos. Información tanto de nuestros clientes, como de nuestros proveedores, como de los empleados de cada uno de los departamentos de la empresa, ya sea informática, RRHH, unidades de producción, directiva, etc.

¿Qué se intenta proteger?; pregunta esencial para saber donde nos encontramos, en este caso el jefe del departamento de informática sabe fielmente qué es lo que se intenta proteger y qué estructura sigue la información en nuestra empresa, por lo tanto la puntuación en este caso reflejará un buen conocimiento y por tanto un exacto, incluso acabado conocimiento de la naturaleza de los sistemas de información de la empresa; en las auditorías siguientes nos preguntaríamos ¿Es igual de importante que antes lo que se intenta proteger o esto ha cambiado?, En nuestro caso lo que buscamos es un incremento de la protección, y en la

temática particular del plan de contingencia buscamos una recuperación efectiva de la información y restauración ante siniestros, como vemos, más que cambios de objetivos sería una reorientación estratégica de nuestra organización para eliminar vulnerabilidades y riesgos, ya que antes no existía ningún tipo de plan y una escasa protección de la información, y permitir una mayor versatilidad y recuperación dentro de un umbral de tiempo, que permita la pervivencia de nuestra organización. Estas dos preguntas se refieren a los activos que la entidad intenta proteger con mayor fuerza durante el plan, tal y como hemos visto durante el desarrollo teórico.

En la puntuación vemos como sobrepasamos ciertamente el valor objetivo, pero en este caso el motivo es un gran conocimiento por parte del jefe de proyecto del sistema de información debido a su experiencia en la empresa, por tanto no supondrá un sobrecoste adicional, y será una baza importante para la conformación del plan de contingencia.

Alcance del negocio		**Puntuación**
1	Conocimiento de lo que se pretende proteger	5
2	Ha habido cambios, se han detectado de manera adecuada y se ha tomado conciencia de un cambio	3
3	Puntuación en la sección	8

4	Nota media	8/2=4
5	Puntuación objetivo	6
6	Nota media objetivo	3

Análisis del negocio:

Hemos visto y explicado a grandes rasgos las actividades primordiales de la compañía por tanto ahora nos centraremos en aspectos más específicos que nos permitirán conocer más de cerca, cuáles son los procesos concretos sobre los que deberemos centrar nuestra atención para conseguir una valoración lo más certera, que nos permita por tanto obtener la mayor concreción a la hora de establecer cuáles han de ser los procesos que tienen que ser ayudados en primera instancia por el plan de contingencia.

Para fijar los objetivos etc. y comenzar a establecer la estrategia computacional a adoptar por la organización debemos realizar las siguientes preguntas esenciales, que no están encuadradas en la revisión auditora de esta fase, pero que nos permiten conocer más de cerca la naturaleza de la empresa, y por tanto conocerla más de cerca serían:

¿Cuáles son las actividades más importantes para la compañía?, Como hemos visto el éxito de nuestra empresa radica en la provisión de envases y por tanto es este proceso de peticiones el que ha de ser satisfecho de una manera efectiva. Por tanto en cuanto a actividades importantes podríamos tener el servicio de alta de clientes, y el mantenimiento de la información y la renovación de contrato con proveedores.

¿Cómo afectaría económicamente una interrupción de los servicios a medida que va pasando el tiempo sin reanudar el servicio?, en este caso nuestra entidad se vería afectada si paralizamos la actividad que llevamos a cabo, evidentemente esta afección no sería igual que en otras empresas donde los sistemas de información tienen más peso en la actividad empresarial, pero efectivamente en nuestro caso una interrupción a determinadas horas sobre todo puede determinar la pérdida de oportunidades de negocio ya que las actividades esenciales de nuestra actividad son las operacionales. Como es evidente la pérdida de negocio con motivo de una interrupción tendrá un umbral a partir del cual será imposible restablecernos de manera adecuada, pero a grandes rasgos y en el inicio de la elaboración de un plan de contingencia se puede atisbar que la pérdida sería importante de estar dos o más días inactivos en jornadas laborables.

¿Cuál sería la capacidad operativa a medida que pasa el tiempo?, Es pronto para emitir un juicio para nuestra empresa, y sus sistemas de información pero el restablecimiento de la capacidad operativa dependerá en primer lugar de las estrategias que adoptemos en plan de contingencia, en segundo lugar de la cantidad de gente que está implicada, y en tercer lugar de la eficiencia en la aplicación de los protocolos, es evidente que hasta ahora sin plan alguno, no había ninguna posibilidad ni capacidad de restablecimiento.

¿Cuál es el plazo máximo para volver a la normalidad sin llegar a incurrir en graves pérdidas?

Evidentemente en este caso sería muy pronto para poder decidir cuánto tiempo es el máximo, pero siempre este tipo de preguntas a priori nos pueden dar una idea de la dimensión que puede alcanzar el plan de contingencia en nuestra empresa. En nuestro caso parece claro que una parada de más de un día comenzaría a plantear problemas, ya que al ser una fábrica con proyección internacional, el ritmo de número de pedidos de nuestros clientes, y el nuestro respecto a los proveedores de materias primas será alto y por tanto si no queremos perder en exceso una cuota de clientes, la recuperación de los sistemas en un tiempo reducido no es una cuestión baladí.

A grandes rasgos ya hemos visto la naturaleza de la empresa y en su evaluación pertinente de cada fase de qué punto puede adolecer el plan que está fraguando nuestro equipo informático. Hasta el momento va cumpliendo con las expectativas. No obstante hasta que no lleguemos al desarrollo completo y a la completitud de las fases auditoras de cada parte del plan no podremos valorar la adecuación del plan de contingencia.

Análisis de riesgos:

Una parte importante dentro del desarrollo del plan de continuidad es el análisis de riesgos. Éste permitirá a la compañía conocer sus riesgos y gestionarlos de manera adecuada.

Existen diferentes metodologías, como vimos, para analizar el riesgo (MARION, MAGERIT, OCTAVE, MEHARI, etc.), que pueden aplicarse para realizar el análisis de riesgos. No entraremos en metodologías específicas para el ejemplo que proponemos, solo lo enfocaremos de manera general.

Como sabemos necesitamos para el análisis de riesgos, una identificación de los activos, que como sabemos del análisis del negocio, el propio departamento informático elaborará. Evidentemente para cada uno de los procesos críticos habrá asociados unos activos que serán los que haya que considerar.

Activo/ Descripción	**Tipo**	**Propietario**	**Localización**	**Valor**
Redes de comunicaciones	Comunicaciones	Ejemplo 1 S.A.	Centros de Madrid y Valencia	Bajo

Información clientes	Información	Ejemplo 1 S.A.	Centros de Madrid y Valencia	Alto
Información proveedores	Información	Ejemplo 1 S.A.	Centro de Madrid	Alto
Aplicaciones de gestión de clientes, pedidos, Stock y proveedores	Aplicación	Ejemplo 1 S.A.	Centros de Madrid y Valencia	Alto
Servidor de aplicaciones	Hardware	Ejemplo 1 S.A.	Centros de Madrid y Valencia	Medio
Impresoras	Hardware	Ejemplo 1 S.A.	Centros de Madrid y Valencia	Bajo
Aplicaciones de seguridad	Aplicación	Ejemplo 1 S.A	Centros de Madrid y Valencia	Alto

Éstos son los activos propios de la empresa implicados en la mayoría de los procesos críticos. Cuanto mayor valor para la empresa tenga el activo tanto más será crítico el proceso que la incumbe.

Por otra parte y como es natural en esta fase procedemos a la identificación de amenazas, existe el método MAGERIT que hemos expuesto durante el desarrollo teórico y que a grandes rasgos nos hace comprobar los diversos puntos amenazantes para nuestra organización, aquí lo exponemos de una manera más simple por la procedencia de las amenazas, lo que nos dará una visión de por donde podrán venir posibles siniestros para adoptar estrategias adecuadas para combatirlas:

AMENAZAS	POSIBLE
DESASTRES NATURALES	
Inundaciones	No en Madrid, pero sí en Valencia
Incendios	Sí
Huracanes	No
DAÑOS ACCIDENTALES	
Fuego fortuito	Sí
Inundaciones	Sí
Fallo del aire acondicionado	No
Exceso de humedad	No en Madrid, pero sí en Valencia
Humo, Gases tóxicos	Sí en Madrid, no en Valencia
Subida de tensión	No
Fallo de suministro eléctrico	Sí
Accidentes del personal	Sí

AMENAZAS	POSIBLE
DAÑOS ACCIDENTALES	
Capacidad inadecuada de las comunicaciones	No
Fallo/degradación del hardware	No
Fallo/degradación de las comunicaciones	Sí
Errores de operación	Sí
Fallos en las copias de seguridad	Sí
Fallos en los sistemas de autenticación/autorización	Sí
Pérdida de confidencialidad	Sí
Incumplimientos legales	No

AMENAZAS	POSIBLE
ATAQUES INTENCIONADOS	
Explosivos	No
Fuego intencionado	No
Accesos no autorizados al edificio	Sí
Actos de vandalismo	No
Radiaciones electromagnéticas	No
Robos intencionados	Sí
Manipulación de datos/software	Sí
Manipulación de hardware	Sí

AMENAZAS	POSIBLE
ATAQUES INTENCIONADOS	
Uso de software por personal no autorizado	Sí
Acceso no autorizado a datos de la compañía	Sí
Software malicioso	Sí
Robo de equipos	Sí
Robo de documentos	Sí
Robo de software	Sí
Descarga de software no controlada	No
Interceptación de las líneas de comunicación	Sí

AMENAZAS	POSIBLE
ATAQUES INTENCIONADOS	
Manipulación de las líneas de comunicación	Sí
Abuso de privilegios de acceso	Sí
Introducción de virus en los sistemas	Sí
Troyanos	Sí
Ataques por ingeniería social	Sí
Bombas lógicas	Sí
Ataques de denegación de servicio	Sí
Errores intencionados	Sí

AMENAZAS	POSIBLE
ATAQUES INTENCIONADOS	
Copias incontroladas de documentos/software/datos	Sí
Errores en el mantenimiento	Sí
Corrupción de datos	Sí
Incumplimientos legales intencionados	No

Como comprobamos existen una serie de amenazas que pueden darse y otras que no, incluso en función de la ubicación de los centros pueden darse unas en uno y otras en otro, por tanto es misión del departamento de informática el saber discernir qué amenazas y en qué lugares pueden darse.

Por otra parte comenzamos con la identificación de vulnerabilidades, que como sabemos determinarán si las amenazas se pueden cumplir con mayor o menor facilidad:

ESCENARIOS	NIVEL DE PROTECCIÓN	RESPUESTA
Inundación de los centros de proceso de datos	¿Los centros están situados en terrenos altos?	En Madrid sí, en Valencia están en un valle fluvial.
Ausencia de plan de recuperación	¿Existe plan de contingencia?	En el momento de evaluar no, pero se está realizando en este momento.
Fallos de suministro eléctrico	¿Existen unidades de suministro eléctrico alternativo?	Ahora no, pero como consecuencia del plan se instalarán.
Personal sin formación adecuada	¿Existe personal sin experiencia?	No, tenemos un buen equipo y un responsable conocedor de la realidad de los sistemas de información.
Pérdida de información clave de la compañía	¿Se realizan copias de seguridad periódicamente?	En este momento no, pero se deberán hacer cuando realicemos el plan de contingencia.

ESCENARIOS	NIVEL DE PROTECCIÓN	RESPUESTA
Incumplimientos legales (LOPD, etc.)	¿Se cumple con la legalidad vigente?	Sí.
Accesos no autorizados a los edificios	¿Existen controles pertinentes de acceso?	No, en el plan general de seguridad y en el plan de contingencia se revisará.
Definición de privilegios de acceso inadecuados	¿Existen controles específicos de control de privilegios?	No, se considerarán en el plan de seguridad
Robo de datos	¿Existe una clasificación de la información adecuada al nivel de confidencialidad de los datos?	No, tendrá que revisarse.
Pérdida de servicios por infección de virus	¿Están los equipos protegidos por un antivirus?	Solo alguno, así que habrá que revisar la política de antivirus.
Descarga incontrolada y uso de software de internet	¿Se revisa el software instalado?	No
Mecanismos de autenticación e identificación	¿Existen métodos de identificación?	No

ESCENARIOS	NIVEL DE PROTECCIÓN	RESPUESTA
Incumplimientos legales (LOPD, etc.)	¿Se cumple con la legalidad vigente?	Sí.
Accesos no autorizados a los edificios	¿Existen controles pertinentes de acceso?	No, en el plan general de seguridad y en el plan de contingencia se revisará.
Definición de privilegios de acceso inadecuados	¿Existen controles específicos de control de privilegios?	No, se considerarán en el plan de seguridad
Robo de datos	¿Existe una clasificación de la información adecuada al nivel de confidencialidad de los datos?	No, tendrá que revisarse.
Pérdida de servicios por infección de virus	¿Están los equipos protegidos por un antivirus?	Solo alguno, así que habrá que revisar la política de antivirus.
Descarga incontrolada y uso de software de internet	¿Se revisa el software instalado?	No
Mecanismos de autenticación e identificación	¿Existen métodos de identificación?	No

Evidentemente, cualquier NO, presente dentro de las vulnerabilidades de nuestra organización deberá ser tratado en el plan general de seguridad, asimismo específicamente en el plan de contingencia si así le afectara, de

tal manera que las amenazas puedan aprovechar lo más mínimo cualquier vulnerabilidad de nuestro sistema.

Análisis de impacto:

Después de la determinación de amenazas y las posibles vulnerabilidades que pueden permitir a esas amenazas manifestarse, debemos definir el impacto que pueden producir esas amenazas a través de las vulnerabilidades en la organización. Para ello deberemos identificar y analizar los procesos que pueden ser susceptibles de una amenaza y entonces determinar a través de la importancia de estos para la organización los impactos que pueden causar.

Estableceremos una serie de formularios que nos ayudarán a identificar estos procesos, las interdependencias de estos, los responsables que cubren los procesos y su frecuencia. De esta manera tendremos una clara idea de qué procesos afectan a nuestra organización, qué afecciones pueden desencadenar en otros procesos relacionados, quienes se encargan de ellos y con qué frecuencia pueden realizarse. Esto nos permitirá evaluar en consecuencia y de manera más pertinente, el valor de estos procesos para la organización.

Algo que nos ayudará en ese proceso es el siguiente cuadro:

Funciones o procesos					
Nombre de la Función ó Proceso:	Departamento responsable:	Breve Descripción:	Frecuencia (diaria, semanal, mensual):	Persona responsable:	Procesos que dependen de éste proceso:
Pedidos Clientes	Departamento de gestión	Se encarga de recibir todos los pedidos de los distintos clientes y gestionar su envío en los plazos y condiciones establecidos.	Diario	Ana González	Stock
Alta clientes	Departamento de gestión	Se encarga de dar de alta en el sistema de los clientes que han solicitado pedidos a nuestra organización, pro primera vez.	Una vez	Pedro Castro	Baja clientes
Baja	Departamento	Se encarga de dar de	Una vez	Pedro	Alta cliente

clientes	de gestión	baja en el sistema de aquellos que han dejado de ser nuestros clientes.		Castro	s

Como vemos en este cuadro los procesos, en este caso de gestión de aplicaciones, acometen una serie de importantes funciones para la organización y su importancia es capital. Como vemos, de cada proceso existe un responsable, estos responsables pueden ser meros empleados o ser responsables del departamento en el que trabajan. Por tanto como veremos más adelante serán importantes para la evaluación de la importancia de cada proceso. No obstante también existirán empleados o responsables del departamento que quizá no estén involucrados directamente en los procesos pero conozcan de cerca, por pertenecer al área estudiada en cuestión, el funcionamiento de dicho departamento y puedan comunicarse de manera eficaz con las personas implicadas. Esta gente también podrá servirnos para la evaluación de la importancia de los procesos, en función de su valía o experiencia en el área en cuestión. No obstante tanto en el cuadro anterior como en los que le siguen, queda reflejada fielmente la distribución de competencias y por tanto el cuadro de responsabilidades que en caso de contingencia será muy útil.

Funciones o procesos					
Nombre de la Función ó Proceso:	Departamento responsable:	Breve Descripción:	Frecuencia (diaria, semanal, mensual):	Persona responsable:	Procesos que dependen de éste proceso:
Stock	Departamento de gestión de Stocks	Se encarga de la gestión del Stock	Diaria	Fernando Fueyo	Pedido clientes
Alta proveedores	Departamento de gestión	Se encarga de dar de alta a los proveedores que por primera vez nos ofrecen un servicio	Una vez	Ana Huidobro	Baja proveedores
Baja proveedores	Departamento de gestión	Se encarga de dar de baja a los proveedores.	Una vez	Ana Huidobro	Alta proveedores
Nóminas	Departamento de RRHH	Genera y paga las nóminas de los empleados	Mensual	Paco Fernández	

Funciones o procesos					
Nombre de la Función ó Proceso:	Departamento responsable:	Breve Descripción:	Frecuencia (diaria, semanal, mensual):	Persona responsable:	Procesos que dependen de éste proceso:
Revisión de sistemas	Departamento de informática	Se encarga de revisar los fallos de los sistemas de información	Mensual	Antonio Pérez	
Reclamación clientes	Departamento atención al cliente	Se encarga de atender las reclamaciones de los clientes	Diario/Semanal	Ana de Gustín	Alta clientes
Recursos Humanos	Departamento de RRHH	Se encarga de gestionar los recursos humanos	Diario	Natalia de Francesca	

Una vez vistas las responsabilidades de cada persona en el día a día de cada proceso, nos preocuparemos de quién se encargará de la evaluación en importancia de los procesos. En este caso como comentamos, o bien será gente responsable del proceso en cuestión, pero también en algunos casos los responsables propios del departamento o simples empleados que por su dilatada experiencia o conocimiento puedan ser mucho más eficaces en

estas tareas; en este caso reportarían finalmente a los responsables del área de su departamento las medidas a acometer en cuanto a evaluación de los proceso y su impacto frente a amenazas se refiere.

Como vemos en el siguiente cuadro, la repartición de responsabilidades para evaluar posible impactos de los procesos amenazados:

Nombre	**Puesto**	**Área de responsabilidad**
Antonio Pérez	Director	Área de seguridad
Ana González	Empleado	Aplicaciones de gestión general
María Hierro	Responsable	Departamento de marketing/atención al cliente
Ana Fernández	Empleada	RRHH
Fernando Fueyo	Responsable	Aplicaciones de gestión de Stocks

Como vemos existen procesos que en función de sus consecuencias al ser azotados por una amenaza serán más o menos críticos. Función de los responsables de la evaluación de amenazas, que no de la evaluación correcta del análisis de impacto, nos permitirán evaluar la criticidad de estos procesos, y por tanto determinar con mayor exactitud cómo actuar en función de la situación. No obstante se podrían realizar test de evaluación de conocimientos en cada departamento para saber cuál es la persona más apta para este cometido.

Comenzamos por ver el proceso de Pedidos Clientes:

- Sistemas del proceso de pedidos

Nombre del sistema	Descripción	Criticidad	Tipo de sistema	Nº de equipos con la aplicación	Responsable
Gestión pedidos	Aplicación para gestión de pedidos	1		10	Ana González
Correo electrónico		2	Servidor de correo	10	Antonio Pérez

- Hardware del proceso de pedidos

En el caso del servidor no nos harán falta grandes servidores para el correo como GRAN servidor (CPU Intel Xeon o AMD Opteron), ya que el número de personas en informática en nuestra empresa es pequeño. Por tanto podemos optar por una solución más pequeña como DELL PowerEdge 1950, si en un futuro fuésemos a ampliar podemos tener como opción DELL PowerEdge 2950 con más almacenamiento. Esta última solución nos podría servir para el

servidor de aplicaciones que requiere algo más de proceso, y con más peso.

Tipo de hardware	Detalles del modelo	Distribuidor	Criticidad	Localización
Servidor de correo	PowerEdge 1950	Dell	3	Centro de proceso de datos de Madrid
PC´s	Procesador Intel core 2 duo. Solución LAN gigabit Ethernet de Intel	Dell	2	Madrid y Valencia
Servidor de aplicaciones	PowerEdgeTM 2900	Dell	1	Centro de procesos de Madrid

- Otros activos del proceso:

Descripción	Criticidad	Tipo de sistema	Localización

Línea ADSL de comunicaciones	1	Comunicaciones	Madrid y Valencia
Centralita de comunicaciones	2	Comunicaciones	Madrid y Valencia
Impresoras	2	Hardware	Madrid y Valencia

En este proceso tenemos la utilización tanto de servidores, porque es necesario para la comunicación de la información de nuestras aplicaciones, la centralita de comunicaciones que es necesaria para la recepción efectiva de pedidos, y las impresoras para los albaranes correspondientes.

- Proceso Nóminas: Seguidamente pasamos a ver los componentes del proceso de Nóminas.

Nombre del sistema	Descripción	Criticidad	Tipo de sistema	Nº de equipos con la aplicación	Responsable
Aplicación Nóminas	Aplicación para el cálculo de nóminas	3	Servidor/PC´s	3	Ana González
Windows XP	Sistema operativo	2	PC´s	10	Antonio Pérez

- Hardware del proceso nóminas:

Tipo de hardware	Detalles del modelo	Distribuidor	Criticidad	Localización
PC´s	Procesador Intel core 2 duo. Solución LAN gigabit Ethernet de Intel	Dell	2	Madrid y Valencia
Servidor de aplicaciones	PowerEdgeTM 2900	Dell	1	Centro de procesos de Madrid

- Otros activos del proceso:

Descripción	Criticidad	Tipo de sistema	Localización
Impresoras	2	Hardware	Madrid y Valencia

El proceso de nóminas llevará a cabo todo lo relacionado con las nóminas de los empleados de la empresa, en este caso utiliza los PC´s habituales bajo S.O. Windows asimismo como hardware se utilizan las impresoras, para la impresión de las hojas de nóminas en papel.

- Proceso Alta Clientes:

Nombre del sistema	Descripción	Criticidad	Tipo de sistema	Nº de equipos con la aplicación	Responsable
Aplicación Gestión Clientes	Aplicación para el registro de clientes nuevos en nuestro sistema	1	Servidor/PC´s	10	Pedro Castro

Windows XP	Sistema operativo	2	PC´s	10	Antonio Pérez
Correo electrónico		2	Servidor de correo	10	Antonio Pérez

- Hardware proceso Alta clientes:

Tipo de hardware	Detalles del modelo	Distribuidor	Criticidad	Localización
PC´s	Procesador Intel core 2 duo. Solución LAN gigabit Ethernet de Intel	Dell	2	Madrid y Valencia
Servidor de aplicaciones	PowerEdgeTM 2900	Dell	1	Centro de procesos de Madrid
Servidor de correo	PowerEdge 1950	Dell	3	Centro de proceso de datos de Madrid

- Otros activos del proceso:

Descripción	Criticidad	Tipo de sistema	Localización
Línea ADSL de comunicaciones	1	Comunicaciones	Madrid y Valencia

Serían los mismos cuadros para la baja de clientes, la misma aplicación de gestión se dirigirá tanto a la baja como alta de clientes. Se obvian las impresoras ya que el proceso de registro es electrónico vía mail.

- Proceso Stock:

Nombre del sistema	Descripción	Criticidad	Tipo de sistema	Nº de equipos con la aplicación	Responsable
Aplicación Gestión Stock	Aplicación para la gestión de stocks de nuestros productos	1	Servidor/PC´s	10	Pedro Castro
Windows XP	Sistema operativo	2	PC´s	10	Antonio Pérez

Correo electrónico		2	Servidor de correo	10	Antonio Pérez
Aplicación de aviso de reposición de género	Aplicación de apoyo a la gestión de stock que avisa vía mail, de la necesidad de reponer género.	1	Servidor/PC´s	10	Pedro Castro

- Hardware del proceso:

Tipo de hardware	**Detalles del modelo**	**Distribuidor**	**Criticidad**	**Localización**
PC´s	Procesador Intel core 2 duo. Solución LAN gigabit Ethernet de Intel	Dell	2	Madrid y Valencia
Servidor de aplicaciones	PowerEdgeTM 2900	Dell	1	Centro de procesos de Madrid

Servidor de correo	PowerEdge 1950	Dell	3	Centro de proceso de datos de Madrid

- Otros activos del proceso:

Descripción	Criticidad	Tipo de sistema	Localización
Línea ADSL de comunicaciones	1	Comunicaciones	Madrid y Valencia

- Proceso Alta proveedores:

Nombre del sistema	Descripción	Criticidad	Tipo de sistema	Nº de equipos con la aplicación	Responsable
Aplicación Gestión Proveedores	Aplicación para el registro de Proveedores	1	Servidor/PC´s	10	Pedro Castro
Windows XP	Sistema operativo	2	PC´s	10	Antonio Pérez

Correo electrónico		2	Servidor de correo	10	Antonio Pérez

- Hardware del proceso:

Tipo de hardware	Detalles del modelo	Distribuidor	Criticidad	Localización
PC´s	Procesador Intel core 2 duo. Solución LAN gigabit Ethernet de Intel	Dell	2	Madrid y Valencia
Servidor de aplicaciones	PowerEdgeTM 2900	Dell	1	Centro de procesos de Madrid
Servidor de correo	PowerEdge 1950	Dell	3	Centro de proceso de datos de Madrid

- Otros activos del proceso:

Descripción	Criticidad	Tipo de sistema	Localización
Línea ADSL de comunicaciones	1	Comunicaciones	Madrid y Valencia

En cuanto a esta aplicación se encarga no solo del alta de proveedores sino también de la baja de proveedores.

- Proceso Revisión de sistemas:

Nombre del sistema	Descripción	Criticidad	Tipo de sistema	Nº de equipos con la aplicación	Responsable
Aplicación revisión sistema.	Aplicaciones para la revisión de los sistemas	1	Servidor/PC´s	10	Antonio Pérez

	proveyendo de seguridad a nuestro sistema de información.				
Windows XP	Sistema operativo	2	PC´s	10	Antonio Pérez

- Hardware del proceso

Tipo de hardware	Detalles del modelo	Distribuidor	Criticidad	Localización
PC´s	Procesador Intel core 2 duo. Solución LAN gigabit Ethernet de Intel	Dell	2	Madrid y Valencia

- Proceso Reclamación clientes:

Nombre del sistema	Descripción	Criticidad	Tipo de sistema	Nº de equipos con la aplicación	Responsable

Reclamación clientes	Aplicación para gestión de las reclamaciones de los clientes	2		2	Ana de Agustín
Correo electrónico		2	Servidor de correo	10	Antonio Pérez

- Hardware proceso:

Tipo de hardware	Detalles del modelo	Distribuidor	Criticidad	Localización
PC´s	Procesador Intel core 2 duo. Solución LAN gigabit Ethernet de Intel	Dell	2	Madrid y Valencia

- Proceso de RRHH:

Nombre del sistema	Descripción	Criticidad	Tipo de sistema	Nº de equipos con la aplicación	Responsable

Reclamación clientes	Aplicación para gestión de los RRHH de la empresa	2		1	Natalia de Francesca
Correo electrónico		2	Servidor de correo	10	Antonio Pérez

- Hardware del proceso:

Tipo de hardware	Detalles del modelo	Distribuidor	Criticidad	Localización
PC´s	Procesador Intel core 2 duo. Solución LAN gigabit Ethernet de Intel	Dell	2	Madrid y Valencia

Después de ver la idiosincrasia de cada uno de los procesos y todos los elementos que les pueden afectar en una interrupción, tendremos que evaluar el impacto producido por cada uno de ellos, en función del tiempo que estén inoperativos; asimismo el tipo de impacto y magnitud que puede provocar su interrupción.

La evaluación final del apartado la haremos respecto a los errores detectados por el plan y su conciencia para cambiarlos y ver si son efectivos. En el caso de los dos escenarios nos permitirá evaluar cuanto de bien está planteado nuestro plan de contingencia y si realmente es efectivo.

Tomaremos como referencia los dos procesos más representativos y con dos tipos de impacto diferente. Sería este proceso extensible a los demás procesos y con diferentes tipos de impacto. De esta manera comprobamos la efectividad del plan de contingencia y su evaluación.

Veremos dos de los procesos más importantes en cuestión:

Gestión de pedidos:

Este proceso de gestión de pedidos sufrirá una serie de interrupciones específicas que veremos, cuyo impacto cómo afecta a cada área de nuestra organización (económica, jurídica, operacional, comercial, de imagen, etc.) y cuya magnitud vendrá determinada por una valoración cuantitativa y cualitativa en el tiempo.

En nuestro ejemplo vamos a presuponer que la gestión de pedidos ha sufrido una interrupción por un corte de suministro eléctrico. Esto nos dará una idea del impacto ante este tipo de eventos de interrupción.

Habíamos visto que no teníamos equipos de apoyo eléctrico ni generadores. En nuestro plan se había contemplado que había que poner generadores. En este caso habrá cinco horas de corte de suministro.

Vamos a presuponer dos escenarios:

El escenario antes de la aplicación del plan. No tenemos generadores y por tanto la única opción que nos queda es que vuelva el suministro eléctrico. La única comprobación que podemos hacer es que el problema eléctrico no es solo nuestro, sino general. Si fuese nuestro la única opción sería llamar a la compañía eléctrica y mirar las razones que nos han llevado a la falta de suministro o bien en su caso llamar urgentemente a un electricista.

En este caso causaría un impacto de diversos tipos y de distinta magnitud. Recordemos el corte de luz es de aproximadamente seis horas en horario de trabajo.

Tipo de Impacto	**Magnitud del Impacto**					
	4 horas	1 día	1 sem.	1 mes	Peor día	Peor mes del año
Pérdida de ingresos		x				
Pérdida de beneficios		x				
Impacto en cash flow		x				
Incremento de costes o gastos			x			
Peligro para las personas	--					
Impacto operacional			x			
Impacto comercial			x			

Pérdida de calidad			x			
Impacto en la imagen			x			
Incumplimiento de obligaciones legales		x				
Impacto ambiental	--					
Desmoralización del personal			x			

Vemos que se producen impactos como pérdidas de ingresos, cuya magnitud se califica en un día, ya que la restitución de todos los pedidos de ese día conllevará una carga de trabajo importante el resto de la semana y muchos de hecho se habrán perdido ya que no habrán podido ser atendidos. También pérdidas de beneficios y de cash flow por una cuestión análoga. Se produce un incremento de costes de una semana ya que en ocasiones los pedidos necesitan un proceso de peticiones a fábrica y la ralentización del proceso de petición vía telefónica (en el caso de que se produzca), produce en ocasiones colapsos por pedidos diarios amontonados de un día para otro. Asimismo un impacto semanal tendría en el ámbito operacional, comercial, de calidad, de impacto en la imagen y de desmoralización del personal.

En este caso ponemos el grado de impacto en la organización y su tipo de naturaleza para saber que afecciones tuvo:

Un Día					
Proceso	Impacto	Leve	Medio	Grave	Catastrófico
Gestión pedidos	Comercial			x	

Gestión pedidos	Operacional			x	
Gestión pedidos	Económico			x	
Gestión pedidos	Ambiental	x			

El impacto semanal en cada tipo de impacto de suaviza y ya no es tan profundo como el diario en determinados tipos de impacto.

Una Semana					
Proceso	Impacto	Leve	Medio	Grave	Catastrófico
Gestión pedidos	Comercial		x		
Gestión pedidos	Operacional		x		
Gestión pedidos	Económico		x		
Gestión pedidos	Ambiental	x			

De haber tenido una magnitud en el tiempo mayor el impacto de un tipo en un día sería mayor.

El otro escenario sería: como consecuencia del plan existe un generador y un responsable de mantenimiento encargado del mantenimiento y puesta en marcha. Como es lógico en cuanto se produce el fallo la cadena de comunicación se pone en marcha y en poco tiempo se lleva a cabo el

funcionamiento del generador (así es como se estipulará en la fase de desarrollo del plan cuando lleguemos a ella). Esta inclusión es a título comparativo para comprobar la eficiencia y por tanto tomar nota de la evaluación de la situación de nuestra empresa para adoptar un plan adecuado.

Tipo de Impacto	**Magnitud del Impacto**					
	4 horas	1 día	1 sem.	1 mes	Peor día	Peor mes del año
Pérdida de ingresos	--					
Pérdida de beneficios	--					
Impacto en cash flow	--					
Incremento de costes o gastos	--					
Peligro para las personas	--					
Impacto operacional	--					
Impacto comercial	--					
Pérdida de calidad	--					
Impacto en la imagen	--					

Incumplimiento de obligaciones legales	--					
Impacto ambiental	--					
Desmoralización del personal	--					

Como comprobamos no existe ningún tipo de menoscabo de nuestra actividad, gracias a las medidas de contingencias adoptadas frente a esa amenaza. La vulnerabilidad se subsanó correctamente.

Proceso revisión de sistemas:

En este caso sufriríamos un ataque a nuestros sistemas de información con una bomba lógica. A cierta fecha y ciertas condiciones de estado de algunos programas se activa. Provoca colapso de los sistemas, y borrados de disco duro, lo cual hace que nuestra operación se pare y perdamos información relativa a nuestras operaciones comerciales.

Consideramos dos escenarios que nos permitirán conocer cuán mala o perniciosa es la acción de esta bomba lógica en nuestra organización, y como paliarla a través del plan de contingencia que tenemos diseñado.

Para ello nos centraremos en el proceso de revisión de sistemas que es un conjunto de aplicaciones controladas por el responsable de informática de nuestra empresa.

Escenario antes de la aplicación del plan: Como vimos solo tenemos antivirus en algunos ordenadores, no en todos, y tampoco se producen salvados de información. Por lo tanto en este caso el impacto de esta amenaza a través de esta grave vulnerabilidad es total.

Tipo de Impacto	**Magnitud del Impacto**					
	4 horas	1 día	1 sem.	1 mes	Peor día	Peor mes del año
Pérdida de ingresos						x
Pérdida de beneficios						x
Impacto en cash flow						x
Incremento de costes o gastos						x
Peligro para las personas	--					
Impacto operacional						x
Impacto comercial						x
Pérdida de calidad						x
Impacto en la imagen						x
Incumplimiento de obligaciones legales	--					

Impacto ambiental	--					
Desmoralización del personal						x

El impacto es ingente y supone la quiebra de nuestra empresa, como vemos la magnitud del impacto sería la máxima según el gráfico. El tiempo máximo de recuperación de los procesos se sobrepasa y se llega al colapso de la organización. Por tanto el plan de contingencia debe subsanar esto.

A continuación vemos que impacto en un día, semana y mes tiene el proceso impactado.

Un Día					
Proceso	Impacto	Leve	Medio	Grave	Catastrófico
Revisión de sistemas	Comercial				x
Revisión de sistemas	Operacional				x
Revisión de sistemas	Económico				x
Revisión de sistemas	Ambiental				x

Una Semana					
Proceso	Impacto	Leve	Medio	Grave	Catastrófico
Revisión de sistemas	Comercial				x
Revisión de sistemas	Operacional				x
Revisión de sistemas	Económico				x
Revisión de sistemas	Ambiental				x

Un Mes					
Proceso	Impacto	Leve	Medio	Grave	Catastrófico
Revisión de sistemas	Comercial				x
Revisión de sistemas	Operacional				x
Revisión de sistemas	Económico				x

Revisión de sistemas	Ambiental				x

Tanto en un día, como en una semana, como en un mes el impacto es catastrófico, por lo tanto el cambio es necesario como veremos en la fase pertinente seguidamente veremos las consecuencias del amejoramiento en el siguiente escenario que será realizado cuando desarrollemos el plan en sí.

El segundo de los escenarios se refiere a una vez implantado el plan de contingencia. Como vimos la seguridad constituía una vulnerabilidad completa en nuestra empresa y por lo tanto se decidió (lo veremos cuando desarrollemos la fase de desarrollo del plan), adoptar las medidas oportunas. En este caso en concreto contemplamos el impacto de tener instaurado el sistema de seguridad, pensado para nuestra empresa, y de esa manera comparar de una manera efectiva la utilidad de la implantación del mismo.

En este caso la explosión de la bomba es detectada, y afecta a un solo equipo impidiendo, con motivo de cómo veremos, las nuevas medidas de seguridad, que se extienda. De esa manera cortamos el impacto en los demás equipos y en el que se manifestó fue limitado. No hemos perdido gran cantidad de información de ese equipo porque se realiza un backup periódico. Por tanto cuando desarrollemos el plan veremos qué medidas permiten este éxito rotundo en nuestro plan. Seguidamente vemos el impacto, que como veremos será muy reducido.

Tipo de Impacto	**Magnitud del Impacto**					
	4 horas	1 día	1 sem.	1 mes	Peor día	Peor mes del año
Pérdida de ingresos	x					

Pérdida de beneficios	--					
Impacto en cash flow	--					
Incremento de costes o gastos	x					
Peligro para las personas	--					
Impacto operacional	x					
Impacto comercial	--					
Pérdida de calidad	--					
Impacto en la imagen	--					
Incumplimiento de obligaciones legales	--					
Impacto ambiental	--					
Desmoralización del personal	--					

Prácticamente insignificante en comparación con antes del plan, vemos por lo tanto que es muy efectivo y que por tanto desarrollarlo en la fase de desarrollo del plan nos traerá grande beneficios. Se produciría el mismo análisis de impacto para los demás proceso o funciones del proyecto, pero aquí no los hemos desarrollado todos, solo hemos desarrollado aquellos más representativos.

Como hemos visto el impacto de un proceso es medible en función del alcance en días de daño, para nuestra organización. Por otra parte el tiempo máximo de interrupción de un proceso será el tiempo o umbral máximo en que puede aguantar éste sin funcionar, a partir del cual es ya inaceptable su permanencia en ese estado. No coincidirá por tanto con la magnitud de impacto para la organización, sino que será un parámetro crítico para la pervivencia de la organización en torno a ese proceso.

Proceso	**Necesidades de recuperación**	**Criticidad**
Pedidos Clientes	2-3 días	1
Alta Clientes	5 días	2
Baja Clientes	5 días	3
Stock	2-3días	1
Alta Proveedores	4 días	1
Baja Proveedores	4 días	3
Nóminas	15 días	3
Revisión de sistemas	2 días	1
Reclamación Clientes	6 días	3
Recursos Humanos	6 días	3

El proceso de Pedidos es clave para la organización, ya que si no se pueden gestionar los pedidos de los clientes de la empresa no puede dar servicio y por lo tanto incurrirá rápidamente en pérdidas. Por ello es importante que este proceso se recupere rápido. En contraposición al proceso de nóminas, en el que la compañía puede esperar semanas a que se restablezca y crear procedimientos alternativos como por ejemplo, repetir el último pago de nómina de los trabajadores y realizar las compensaciones correspondientes, cuando estén disponibles de nuevo los sistemas.

Como consecuencia de todos estos análisis seguidamente pasamos a ver el riesgo derivado de cada amenaza y su impacto. Todo dependerá de la probabilidad de manifestación de esa amenaza y el impacto que cause su manifestación. Como hemos reseñado no hemos desarrollado toda la magnitud y tipos de impacto causados por todas las amenazas y por todos los procesos, solo los más representativos que nos den una idea del funcionamiento del análisis de amenazas e impactos.

Aquí reflejamos los riesgos de las amenazas anteriores que hemos visto para esos dos procesos, la matriz de riesgos que hemos visto en el desarrollo teórico nos dará la magnitud del riesgo:

Descripción Amenaza	**Probabilidad manifestación**	**Impacto**	**Riesgo**
Fallo de suministro eléctrico	Baja	Alto	Medio
Software malicioso	Media	Alto	Alto

Inundaciones	En Madrid Bajo, en Valencia Alto	Alto	En Madrid Medio, en Valencia Alto
Accesos no autorizados	..	..	..
Actos de vandalismo	..	..	..
Etc.			

Para las demás amenazas se desarrollaría de igual manera, ver que probabilidad y el impacto. Pasamos a desarrollar contramedidas para el desarrollo de nuestro plan de contingencia, derivadas de todo lo que hemos percibido en esta fase.

Recomendaciones Contramedidas:

- Realizar copias de seguridad periódicamente
- Controlar el acceso físico al lugar donde se encuentran los equipos con información clave para la compañía
- Establecer medidas anti-inundaciones en la delegación de la empresa de Valencia por el alto riesgo que allí supone.
- Establecer detectores de humo y alarmas de fuego.
- Instalar antivirus y firewalls en todos los equipos de la compañía

Control y valoración de la fase:

Análisis de riesgos e impactos		Puntuación
1	Se ha aprobado el proyecto por la dirección sobre base firme, definiendo objetivos que se corresponden con la realidad.	3
2	Se han realizado variaciones (o se ha establecido de no existir), respecto del último plan elaborado que mejoren lo anteriormente establecido.	3
3	Evaluar los efectos de interrupciones, exposición a pérdidas e impacto en la organización.	2
4	Se han determinado e identificado de manera correcta las amenazas.	3
5	Se han determinado e identificado de manera correcta las vulnerabilidades.	3
6	Se han definido las criticidades de las funciones y datos, asignando prioridades.	3
7	Se han identificado los activos y determinado de manera correcta el valor de los activos.	3
8	Se han asignado las personas adecuadas para los análisis y las medidas a tomar.	1

9	Las contramedidas son adecuadas a nuestras valoraciones	3
10	Puntuación de la sección	24
11	Nota media	2,6
12	Puntuación objetivo	27
13	Nota media Objetivo	3

La valoración es cercana a la media-objetivo, por tanto es una fase que se ha realizado de manera correcta su realización y nos proveerá de un plan correcto y sin sobreestimaciones.

Estrategia de recuperación:

Una vez que se ha realizado la gestión de riesgos detectados, se debe seleccionar una estrategia de recuperación de negocio que asegure la continuidad de los procesos que hemos considerado críticos en el análisis de impacto.

Como vimos en el desarrollo teórico existen varias alternativas para adoptar estrategias, debemos adquirir la que mejor se adecúe a nuestros objetivos y a la idiosincrasia de la organización.

Así que en función de las áreas funcionales, las necesidades de almacenamiento externo de copias de seguridad y las necesidades de un centro de proceso, se determinará la estrategia a adoptar.

De las alternativas existentes y dado que sería muy caro subcontratar a terceros para que salvaguardasen nuestros datos y nos ofreciesen un centro de proceso de datos, optamos por la solución propia, ya que no somos una gran empresa con un proyecto de sistemas de información ingente.

Ante consideraciones de centro propio debemos establecer una serie de razones. Como tenemos dos centros la idea es que un centro sirva de respaldo al otro. Estos están en ciudades diferentes, lo que nos permite salvar los desastres regionales, lo único que el de Valencia está más amenazado por desastres naturales que el de Madrid. De esa manera será en Madrid donde deberemos instalar nuestro centro de respaldo. Otras consideraciones serían si en el centro de Madrid existe el suficiente espacio, personal, suministros, etc. En este caso es así porque el Centro de Madrid aglutina la mayor parte de la actividad de los sistemas de información. Tendremos la ventaja de compatibilidad con software, y haremos una revisión trimestral para asegurar que existe soporte adecuado para todas las aplicaciones críticas. También tendremos la solución propia, la ventaja es la de tener disponibles, como es nuestro centro, las instalaciones todo el tiempo durante cualquier tipo de desastre. Se pueden hacer pruebas baratas, de menor coste y tendremos el personal experimentado y cercano. Consideraremos que en nuestro centro de Madrid tendremos un centro de proceso habitual y en otro edificio anejo tendremos un centro de proceso, donde llevaremos a cabo todo el proceso alternativo de datos y su almacenamiento. De tal manera que no resulte afectado por siniestros dentro de un mismo edificio. Ante la proximidad de nuestro edificio perteneciente a la empresa, cercano al centro de Madrid, se puede

optar por la solución de centro replicado, ya que no nos costará sobremanera mantener un centro idéntico con las actualizaciones al día, estando tan próximo el material y el personal. Esto nos permitirá el mantenimiento adecuado de nuestro plan. No obstante se pueden llevar actualizaciones con una periodicidad mayor que dentro del periodo habitual de la empresa, para ahorrar algunos costes, ya que los cambios dentro de la gestión de sistemas de información no será muy profusa.

Por tanto todas las facetas de capacidad, prioridad, tipo de vuelta al centro y restitución de la normalidad son cubiertas de manera adecuada y menos costosa que mediante otras soluciones. Evidentemente la actualización no será como la de un centro espejo muy costoso, pero si será periódica, por tanto esta solución propia podría acercarse a la de centro espejo pero sin llegar a serlo por lo costoso de su mantenimiento.

Por otra parte dispondremos de ubicación y espacio suficiente, recursos técnicos necesarios tanto hardware como dentro de la esfera de los backups, asimismo software compatible de aplicaciones requeridas y SSOO. También dispondremos de documentación replicada y adecuada, una serie de medidas de seguridad para el centro de recuperación, tanto en comunicaciones, como en acceso de personas, detección de incendios, etc.

Subcontratar espacios y soporte a terceros resultaría muy caro, nos ahorramos también cualquier tipo de incompatibilidad, de no actualización, de no disponibilidad, comunicaciones etc. Por tanto la solución propuesta en caso de incidencia sería la adecuada.

La traslación de la información del centro de Valencia a Madrid será en parte algo menor que la de Madrid ya que existen algunos equipos menos, y por tanto menos información y personal que trasladar, no obstante es importante reseñar que la llegada de estos datos tendrá algo de retardo con respecto a los de Madrid. Para mayor seguridad se puede hacer un salvado de datos desde el centro de proceso de datos de Madrid al de Valencia, en una pequeña instalación, que permita por otra parte salvar cualquier incidencia grave de pérdida de datos, no obstante esta salvaguarda tendrá una periodicidad mayor.

Control y Evaluación de esta fase:

Estrategia de recuperación		Puntuación
1	Identificación de las necesidades de la estrategia de continuidad del negocio	3
2	Consideración de idoneidad de otras alternativas estratégicas, en función del análisis de impacto realizado	2
3	Selección de centros alternativos de proceso y almacenamiento externo	3
4	Documento contractual que respalde y refleje lo contratado realmente	2
5	Alcance a toda la organización, distancia, presteza, mantenimiento, protocolos, etc.	4
6	Comunicaciones adecuadas	3
7	Medidas de seguridad	2
8	Puntuación de la sección	19
9	Nota media	2,71
10	Puntuación Objetivo	24

11	Nota media objetivo	3

Desarrollo del plan:

Empezaremos a construir el plan de continuidad definiendo la estructura y composición de equipos y acciones de cada uno de ellos. En cada unidad operativa de la institución, que almacene información y sirva para la operatividad de la entidad, se designará un responsable de seguridad de la información de su unidad, pudiendo ser el jefe de dicha unidad operativa. Nuestra empresa es de tamaño medio y por tanto reducimos el número y equipos y su composición, ya que no somos una gran empresa, y éstos serán necesarios en caso de activación de nuestro plan de contingencia. Acometerán asimismo las actividades previas al desastre estipuladas en los 13 puntos que se mostraron en el desarrollo teórico de esta fase.

También y con el objetivo de refinar y hace más efectiva la respuesta del plan, determinaremos los objetivos que buscamos tal como dijimos en el desarrollo teórico, el cumplimiento de esos objetivos nos permitirá ser más eficientes y cumplir la función del plan de contingencia.

De la determinación de objetivos y posteriormente la formación de equipos, designando responsabilidades y definiendo equipos y tareas, deviene el desarrollo de actividades planificadas.

Actividades planificadas:

Plan de emergencias*:* Visionamos una serie de emergencias potenciales que pueden acontecer. Así tenemos previamente establecidos y preparados estos hechos.

En sentido general hablamos de amenazas, que ya hemos comentado pero que tratamos de manera específica: Hablamos de incendios, ataques intencionados mediante software, ataques físicos dentro de la propia entidad, fallos de equipos, fallos de suministro, derrumbamientos, rayos, robos, etc. Y sobre todo zonas inundables en el centro de Valencia que es

más expuesta a estos fenómenos, por lo demás el catálogo de amenazas como vimos al principio suele ser el habitual salvo alguna condición específica como es el tema de las inundaciones en Valencia.

Estableceremos escenarios de contingencia en turno de mañana o laboral, y resto del día, es decir tarde-noche y madrugada, donde los equipos serán activados remotamente.

Para cada persona perteneciente a cada uno de los grupos de actuación durante la contingencia establecemos:

Detallamos vías de escape o emergencia correspondientes en cada uno de los edificios, tanto habituales como de respaldo.

Establecemos plan de evacuación ordenado por departamentos.

Establecemos comprobación por parte del personal, si existe posibilidad de poner a buen recaudo activos de la empresa, dada una contingencia.

Señalizamos elementos contra siniestros, extintores, cobertores de agua, etc.

Establecemos secuencia de llamadas. Y elementos de iluminación y teléfonos de bomberos, policía, ambulancia y personal de seguridad.

Todo ello vendrá en una memoria entregada a los empleados y cargos de la empresa, acompañados por los mapas pertinentes y sus protocolos.

Organización de equipos*:* Son equipos cuyos ejecutores determinan la manera en que se distribuirán las acciones y competencias durante el siniestro.

Ahora veamos los equipos y sus responsables de funcionamiento:

Al comienzo del siniestro, y como hemos reseñado, tendremos un equipo de combate de siniestro que permitirá afrontar activamente algunos acontecimientos en su comienzo, estarán conformados por los propios empleados del departamento/s afectado/s en cuestión, para afrontar algún ataque específico; asimismo dispondremos de un equipo de salvamento de recursos que implique salvar en los primeros momentos algunos datos o material de la organización si se pudiera, estos estarán conformados por los

responsables de los departamentos en su caso. Esta es la manera en que se comenzaría a luchar contra una incidencia en sus primeros estadios.

Implantada ya la incidencia y habiéndose activado los equipos de combate y recuperación comienza la fase propia durante el siniestro.

Comité de crisis:

Integrantes del comité

Responsable del Comité	**Nombre: Antonio Ochoa** **Posición: Director General** **Teléfonos de contacto: XXXXXXXX**
Miembros del Comité	Nombre: Paco Fernández Posición: Director Fábrica Teléfonos: XXXXXXXXX
	Nombre: Ana Fernández Posición: Empleada Departamento de RRHH Teléfonos: XXXXXXXXX
	Nombre: Antonio Pérez Posición: Director Área de seguridad Teléfonos: XXXXXXXXX

Lugar de reunión: Casa del director del área de seguridad C/Jabonería nº 10 Madrid.

El comité de crisis debe reunirse una vez dada la voz de alarma, ante una incidencia, y tomar las decisiones a adoptar. Debe haber una información continua de lo que está aconteciendo, y si es necesario poner en marcha la aplicación del plan. Se comunicará a los responsables de los equipos, el comienzo de las actividades que llevarán a restablecer los servicios de la empresa en cualquiera de los dos centros afectados.

Equipo de recuperación:

Se encarga de poner en marcha todo el proceso de recuperación para restaurar los servicios en el centro afectado.

Se acometen las siguientes actividades:

Traslado de personal a Valencia en caso de que el siniestro sea allí, si se produce en el de Madrid tenemos suficiente gente aquí para acometer la recuperación.

Puesta en marcha de los sistemas por orden de criticidad: Pedidos, facturación, correo, nóminas, etc.

Para poner en funcionamiento los sistemas, se tomará la última copia de seguridad de los sistemas que tiene una periodicidad de actualización semanal replicada en nuestro centro de almacenamiento de Madrid.

Los equipos utilizados para cualquier contingencia serán los del centro de proceso específico de Madrid.

Una vez restablecidos los servicios, comprobamos su operatividad.

El punto de referencia o reunión principal será el centro de recuperación de Madrid.

Integrantes del equipo de recuperación	Nombre: Antonio Pérez Posición: Director Área de seguridad Teléfonos de contacto: XXXXXXXX
	Nombre: Juan Fernández Posición: Técnico informático Teléfonos: XXXXXXXXX
	Nombre: Ana González Posición: Técnico informático Teléfonos: XXXXXXXXX
	Nombre: Antonio Suárez Posición: Técnico informático Teléfonos: XXXXXXXXX

Equipo de coordinación logística:

Se encargará de todo lo relacionado con el esfuerzo logístico de recuperación.

En función del tipo de incidente se encarga de:

- Atender las necesidades logísticas de primera instancia tras la contingencia. (Transporte de personas, transporte de materiales, etc.)
- Contactar con los proveedores para solicitar el material necesario que indiquen los responsables en recuperación.
- Reservar habitaciones de hotel (en su caso), para cuando haya que desplazarse a alguno de los dos centros.

- Gestionar suministro de comida y materiales.

Integrantes equipo coordinación Logística:

Integrantes del equipo de Coordinación logística	Nombre: Ana Fernández Posición: Empleada RRHH Teléfonos de contacto: XXXXXXXX
	Nombre: Juan Gómez Posición: Administrativo Teléfonos: XXXXXXXXX

Proveedores de nuestra organización, (relacionados con logística):

Proveedores	Contacto
DELL	Persona de contacto: Julio Rodríguez Teléfono: XXXXXXXXXX
LG	Persona de contacto: Pepe Suárez Teléfono: XXXXXXXXXX
SAMSUNG	Persona de contacto: Julia Navarro Teléfono: XXXXXXXXXX

Equipo de relaciones públicas:

Se responsabilizará de canalizar la información que generamos para los medios de comunicación y ser la voz de la empresa en contextos de contingencia.

Las tareas que se realizarán serán:

- Si el tipo de incidente lo requiere, emitir un comunicado oficial a clientes y proveedores en el que se identifiquen las causas y consecuencias así como el restablecimiento de los servicios lo antes posible.
- Atender a los clientes para proporcionarles información sobre el incidente y tranquilizarles lo máximo posible.

Integrantes del equipo de relaciones públicas:

Integrantes del equipo Relaciones Públicas	Nombre: Ana Duarte Posición: Atención al cliente Teléfonos de contacto: XXXXXXXX
	Nombre: Ángela Gámez Posición: Comercial Teléfonos: XXXXXXXXX

Equipo de las unidades de negocio:

Estas personas trabajarán con las aplicaciones críticas de la organización y también harán las pruebas de funcionamiento para verificar la operatividad de los sistemas.

Integrantes del equipo Unidades de Negocio	Nombre: Ana González Posición: Responsable de pedidos Teléfonos de contacto: XXXXXXXX
	Nombre: Ana Duarte Posición: Atención al cliente Teléfonos: XXXXXXXXX
	Nombre: Ana Fernández Posición: RRHH Teléfonos de contacto: XXXXXXXX

Generalmente para proyectos más amplios se incluirían los equipos de finanzas, jurídicos, comerciales, recursos humanos específicos y equipo de servicios generales.

Procedimientos de respuesta:

Fase de alerta:

Notificación de la incidencia: En este caso cualquier empleado que vea un incidente grave que afecte a la empresa, debe comunicarlo al jefe de seguridad de planta, proporcionando el mayor detalle posible en la descripción de los hechos.

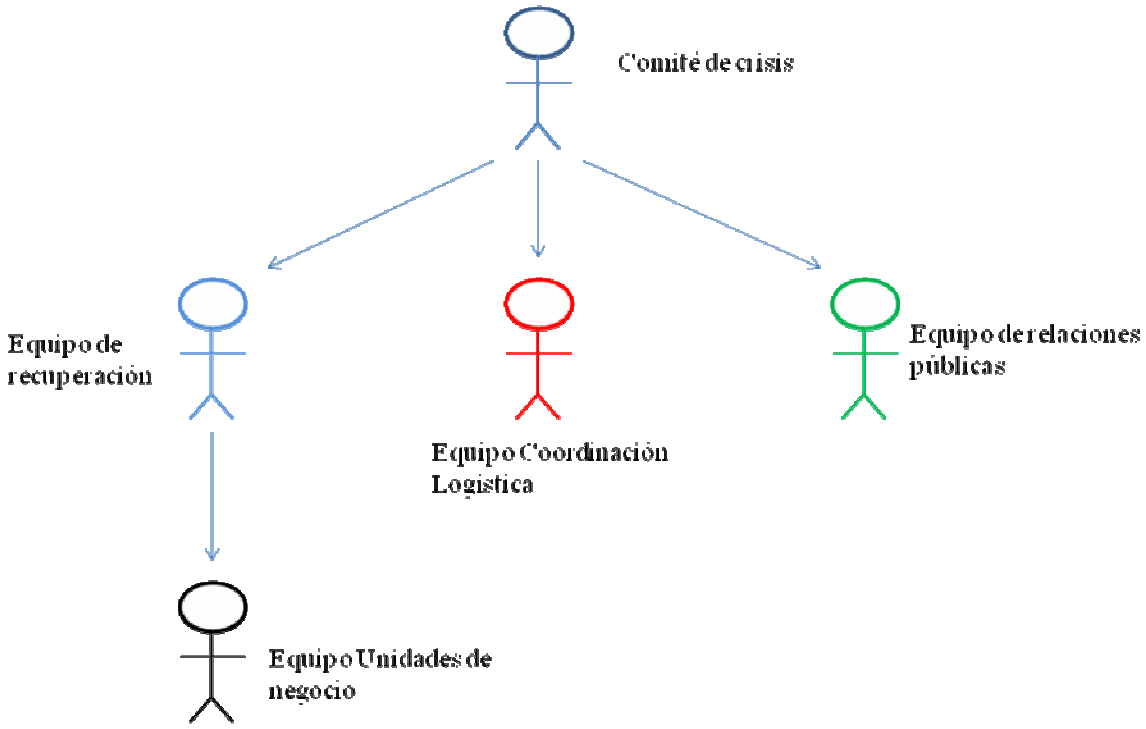
El jefe de seguridad debe analizar los hechos, evaluar la situación y transmitir al responsable del comité de crisis. En este caso concreto, hemos decidido que sea la figura del director general.

Evaluación del daño: Una vez notificada la incidencia, se procede a su evaluación en función de la gravedad del incidente. Los miembros del

comité serán informados por una comisión evaluadora, integrada por algunos miembros de nuestro comité, y el resto del comité estará a la espera hasta que se tome una decisión. Seguidamente se informará a los responsables de seguridad, comité de dirección de empresa, relaciones públicas, equipo de recuperación y responsables de equipos, la decisión adoptada.

Ejecución del plan: Se comienza con el árbol de llamadas para avisar a los integrantes de los equipos, en caso de que después de la evaluación, se haya decidido poner en marcha el plan de contingencias frente a la incidencia. Mientras se va informando al comité de dirección.

Árbol de llamadas:



Una vez terminada la fase de alerta, pasamos a la fase de transición.

Fase de transición: Previa a la recuperación de los sistemas. Existe una coordinación y comunicación profusa entre los diferentes grupos y el grupo de logística.

Parte de concentración y traslado de personas: Una vez que han sido avisados los equipos y puesto en marcha el plan, los equipos acuden al centro de reunión indicado. Además del traslado de personas al centro correspondiente, hay que trasladar todo el material necesario para poner en marcha el centro de recuperación, no obstante al haber optado como solución estratégica un centro propio cercano a la solución espejo, no será necesario un gran despliegue de materiales ya que nosotros mismos hemos provisto al centro de todo el material necesario, no obstante todo lo necesario será comunicado y trasladado si hiciera falta, por parte del equipo logístico.

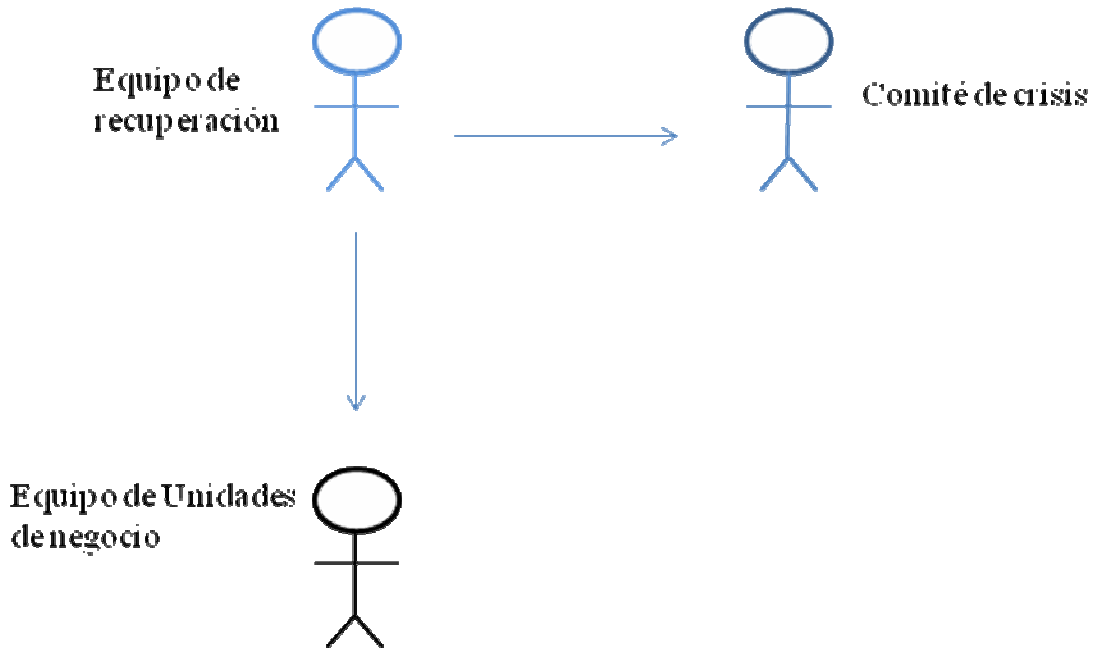
Parte de puesta en marcha del centro de recuperación: Una vez desplegados los equipos en el centro de recuperación y habiendo obtenido todos los materiales necesarios, se comienza con el calibrado de las aplicaciones, usualmente actualizadas, que si no lo estuvieran por acontecer la contingencia en un período de actualización tardía, sería necesaria una actualización rápida del software de los sistemas de información. Sobre la marcha, cualquier material necesario será solicitado al equipo de logística.

Fase de recuperación: Una vez establecidas las bases para comenzar la recuperación, se procede a la carga de datos y la restauración de los servicios críticos por orden de prioridad estratégica establecida.

Procedimientos de restauración: Orden de recuperación en función de su criticidad para nuestra organización. En nuestro caso Restauración de SSOO (en su caso), Pedido clientes, gestión de stocks, revisión de sistemas, gestión de altas de clientes y proveedores, RRHH, correo, baja de clientes y proveedores, reclamación clientes, nóminas.

Procedimientos de soporte y gestión: Acometida la restauración de los procesos y sistemas, realizamos comprobaciones del funcionamiento sobre los mismos; se avisará a los equipos de los departamentos que gestionen los sistemas, para que realicen las comprobaciones necesarias

que certifiquen que funcionen de manera correcta y pueda continuarse dando servicio. Serán los integrantes del equipo de unidades de negocio los encargados de verificar el correcto funcionamiento de los procesos. El equipo de seguridad deberá comprobar que existen las garantías de seguridad necesarias (confidencialidad, integridad, disponibilidad) antes de finalizar la recuperación.



Fase de vuelta a la normalidad

Una vez acontecido el siniestro y habiendo recuperado los procesos críticos, hay que realizar diferentes actuaciones para volver a la normalidad total de funcionamiento.

- Celebración de reuniones: Reunión de planificación de vuelta a las instalaciones restauradas, llevada a cabo por el equipo de gestión de incidentes (recuperación), y que determinará la estrategia general del regreso. También celebración de reunión de planificación de cada equipo de recuperación, ante el retorno a las instalaciones permanentes desde el lugar alternativo.

- Evaluación de daños: Valoración detallada de los equipos e instalaciones dañadas para definir la estrategia de vuelta a la normalidad. El equipo de recuperación junto con el de seguridad, realizarán un listado de los elementos que han sido dañados gravemente y son irrecuperables, así como todo el material que se puede recuperar. Esta evaluación será comunicada al equipo director para que determinen las acciones necesarias que lleven a la operación habitual lo antes posible.

- Priorización de actividades: Asignamos temporalmente, y en función de las circunstancias, a gente reubicándola para que realice tareas más importantes en función de nuestras necesidades estratégicas, y de apoyo a las actividades afectadas. Una de ellas, y consecuencia del punto anterior sería la adquisición de nuevo material, contactando con el seguro de la compañía, para ver qué partes cubre el seguro, y qué inversión tendrá que hacer la compañía. Asimismo contactaremos con los proveedores lo antes posible para reponer los elementos dañados.

- Ejecución de actividades: Equipos dedicados a los trabajos de recuperación específicamente. Reportarán diariamente los resultados y avances. 1º Restauración de servicios desde la zona de respaldo, 2º desde el lugar habitual de operación evitando cualquier lapso de tiempo de pérdida o reducción del servicio.

- Evaluación de resultados: Evaluamos objetivamente los resultados. De aquí sacaremos las recomendaciones.

- Retroalimentación: De esta experiencia obtenemos resultados mejorados para próximas ocasiones. Analizando dificultades y contratiempos, y refinando nuestras recuperaciones.

Dependiendo de la gravedad del incidente, la vuelta a la normalidad de operación puede variar entre unos días (si no hay elementos clave afectados), a algunos meses (elementos clave afectados). Lo importante es que durante el transcurso de este tiempo de vuelta a la normalidad, se sigue dando servicio a los clientes y trabajadores por parte de la compañía y que la incidencia afecte lo menos posible al negocio. Desarrollaremos a partir

de aquí un programa nuevo aprobado y revisado con todo el personal participante, apuntando sus puntos de vista y experiencia, a lo largo de esta y otras fases del plan.

Como conclusión podemos aseverar que en nuestra empresa ejemplo1 s.a., es completamente necesaria la presencia de un plan de contingencia que sustente a la organización. Ya que su no implantación, como hemos visto, puede desembocar en una catástrofe para la empresa. Por tanto necesitamos la implantación de un plan de contingencia, que nos permita seguir ofreciendo nuestros servicios en los sistemas de información, para que nuestra empresa siga siendo competitiva y no sufra menoscabo de su capacidad productora y comercial.

Evaluación o valoración de la fase:

Desarrollo del plan		**Puntuación**
1	Situaciones y sucesos contemplados en adecuadamente	3
2	Precisión del procedimiento a seguir antes de declarar una situación de emergencia	3
3	Responsabilidades de ejecución asignadas, y conocidas por todos los empleados	3
4	Actuaciones de recuperación definidas y priorizadas	3
5	Identificación de los componentes de los procedimientos de respuesta ante emergencias	4

6	Existe un comité de dirección de la reanudación y un responsable del mismo	3
7	Equipos claramente definidos funcionalmente y en torno a personal.	3
8	Definidas las necesidades de recuperación para aplicaciones críticas	3
9	Definición de procedimiento de obtención de copias, así como de procesos y protocolos alternativos	3
10	Documentación de aplicaciones críticas existente y replicada	2
11	Ubicación de centros alternativos para proceso y copias, detallado junto con los protocolos de actuación	3
12	Detallados características y requerimientos específicos para las contingencias, tanto software como hardware	3
13	Procedimientos manuales de respaldo	2
14	Identificación de necesidades de dirección y sus procedimientos	3
15	Procedimientos detallados de respuesta ante emergencias, tanto en acciones a tomar, como en evaluación de daños y protección del personal	4

16	Concienciación de reorientación del plan en función de la experiencia acontecida en los siniestros	4
8	Puntuación de la sección	49
9	Nota media	3,06
10	Puntuación Objetivo	48
11	Nota media objetivo	3

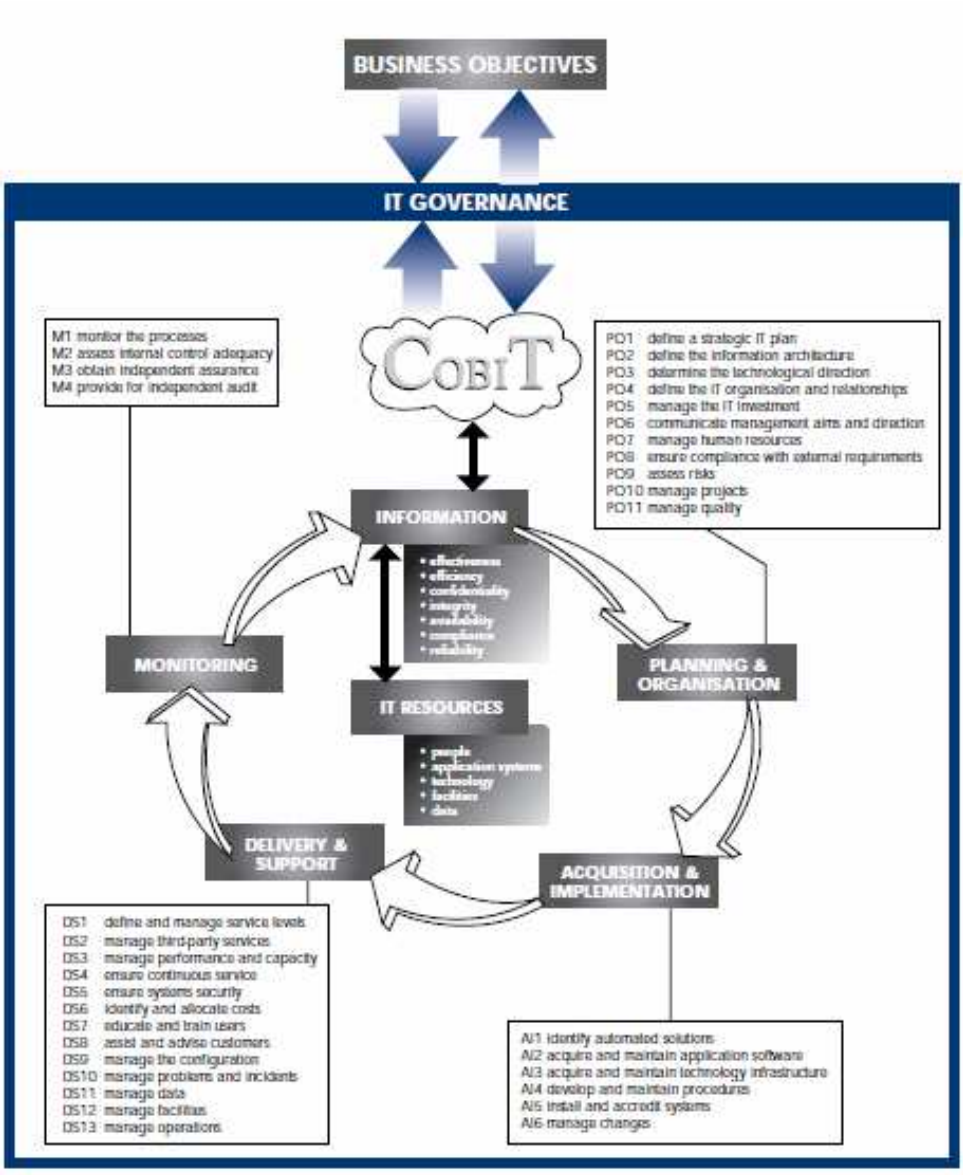
Como comprobamos la puntuación del desarrollo del plan es ligeramente superior a la media objetivo, por tanto es un desarrollo adecuado, incluso algo mejor de lo que esperábamos pero sin ningún tipo de sobreestimación. En función de cada una de las parcelas de esta fase se ha puntuado de manera lo más objetiva posible, para darnos una idea del estado real de nuestro plan.

El mantenimiento y pruebas entraría dentro de una fase de rutina de la empresa para la comprobación del funcionamiento del nuevo plan de contingencia, y que en este ejemplo no desarrollamos.

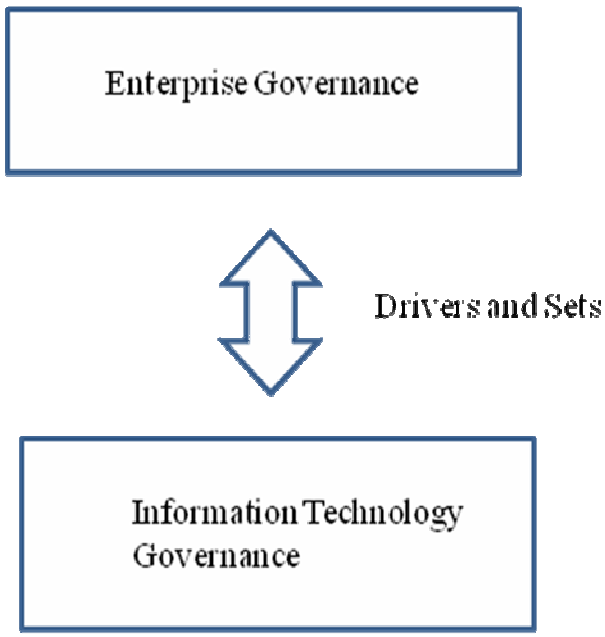
Anexo I:

(Gráficos sobre COBIT)

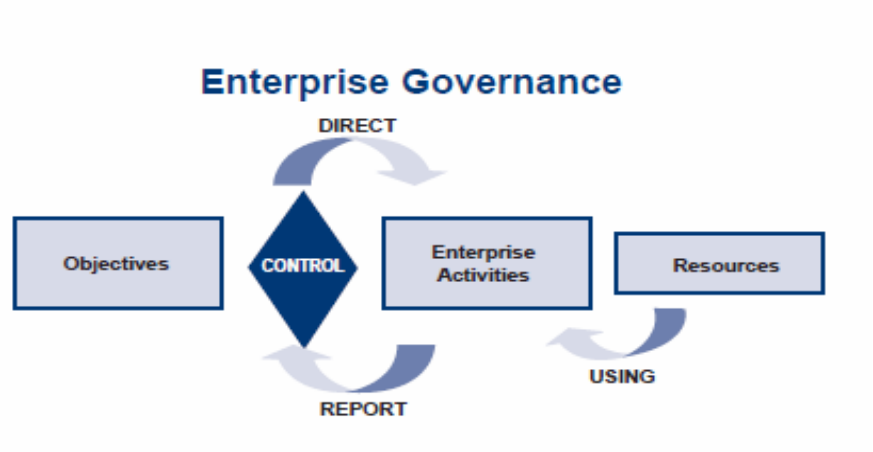
1.


BUSINESS OBJECTIVES
IT GOVERNANCE
COBIT
M1 monitor the processes
M2 assess internal control adequacy
M3 obtain independent assurance
M4 provide for independent audit
PO1 define a strategic IT plan
PO2 define the information architecture
PO3 determine the technological direction
PO4 define the IT organisation and relationships
PO5 manage the IT investment
PO6 communicate management aims and direction
PO7 manage human resources
PO8 ensure compliance with external requirements
PO9 assess risks
PO10 manage projects
PO11 manage quality
INFORMATION
• effectiveness
• efficiency
• confidentiality
• integrity
• availability
• compliance
• reliability
MONITORING
PLANNING & ORGANISATION
IT RESOURCES
• people
• application systems
• technology
• facilities
• data
DELIVERY & SUPPORT
ACQUISITION & IMPLEMENTATION
DS1 define and manage service levels
DS2 manage third-party services
DS3 manage performance and capacity
DS4 ensure continuous service
DS5 ensure systems security
DS6 identify and allocate costs
DS7 educate and train users
DS8 assist and advise customers
DS9 manage the configuration
DS10 manage problems and incidents
DS11 manage data
DS12 manage facilities
DS13 manage operations
AI1 identify automated solutions
AI2 acquire and maintain application software
AI3 acquire and maintain technology infrastructure
AI4 develop and maintain procedures
AI5 install and accredit systems
AI6 manage changes

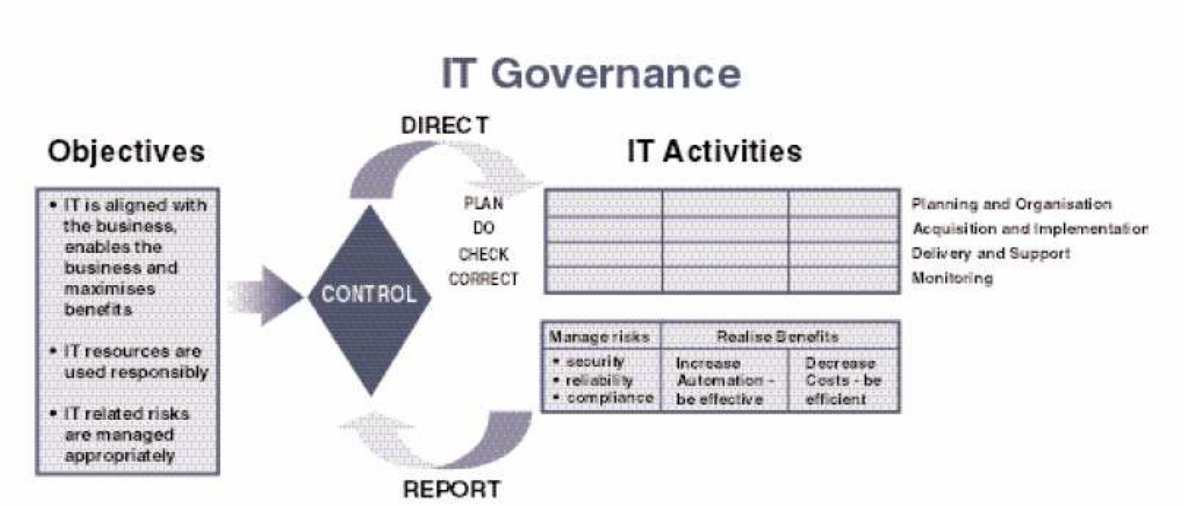
2.


Enterprise Governance
Drivers and Sets
Information Technology Governance

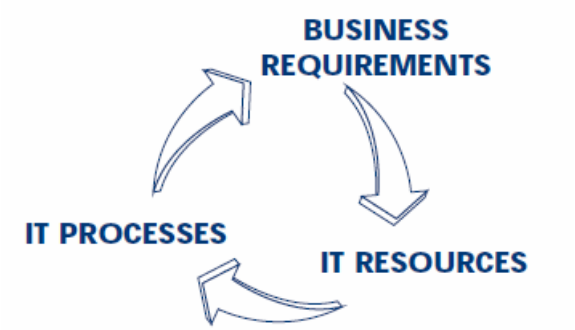
3.


Enterprise Governance
DIRECT
Objectives
CONTROL
Enterprise Activities
Resources
USING
REPORT

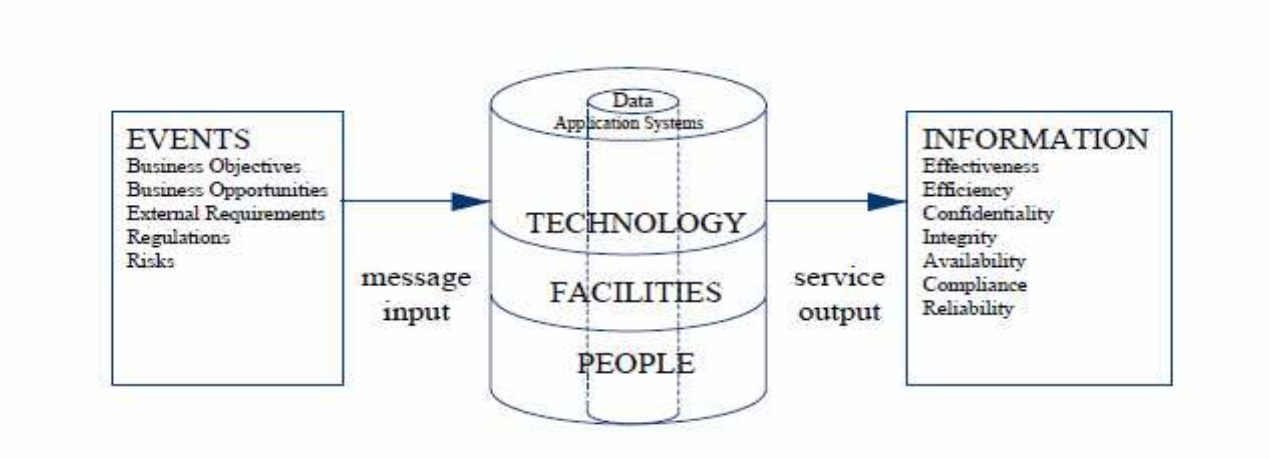
4.


IT Governance
Objectives
• IT is aligned with the business, enables the business and maximises benefits
• IT resources are used responsibly
• IT related risks are managed appropriately
DIRECT
CONTROL
PLAN
DO
CHECK
CORRECT
REPORT
IT Activities
Planning and Organisation
Acquisition and Implementation
Delivery and Support
Monitoring
Manage risks
• security
• reliability
• compliance
Realise Benefits
Increase Automation - be effective
Decrease Costs - be efficient

5.


BUSINESS
REQUIREMENTS
IT PROCESSES
IT RESOURCES

6.


EVENTS
Business Objectives
Business Opportunities
External Requirements
Regulations
Risks
message
input
Data
Application Systems
TECHNOLOGY
FACILITIES
PEOPLE
service
output
INFORMATION
Effectiveness
Efficiency
Confidentiality
Integrity
Availability
Compliance
Reliability

11. Conclusiones:

Como hemos visto, vivimos en un mundo cambiante donde la incertidumbre es un factor consustancial a cualquier actividad, y como no podía ser menos a los sistemas de información y su relación con el mundo empresarial y organizativo. Por tanto se hacen completamente imprescindibles una serie de medidas que como hemos visto vienen de la mano de los planes de contingencia.

Asimismo asumimos que debemos controlar de una manera efectiva estos planes para que se adecuen y estén actualizados a nuestras necesidades funcionales en todo momento. Por ello aparte de los propios planes, necesitamos el desarrollo de su evaluación fase por fase de la mano de la auditoría de estos planes. Estas auditorías nos darán la base para su evaluación, y corrección en su caso, lo que nos proveerá de planes adecuados funcionalmente hablando a nuestras organizaciones.

Como conclusión, llegamos a que una organización provista de un plan de contingencia adecuado y medidas de control previstas efectivas, tiene asegurada su continuidad en este mundo empresarial y organizativo cada vez más cambiante y competitivo.

12. Glosario:

Almacenamiento externo: Lugar acondicionado para la conservación de las copias de seguridad y situado a una distancia prudencial de las instalaciones principales.

Amenaza: Elemento que puede afectar de forma negativa contra la seguridad de una organización.

Análisis de impacto: Análisis destinado a conocer el impacto en una interrupción producido por la materialización de una amenaza. Identificación de las pérdidas producidas.

Análisis de riesgos: Estudio de las amenazas que pueden afectar a los activos y la probabilidad de su afectación determinando su vulnerabilidad.

BCM: Business Continuity Management. Enfoque global de la actividad de la salvaguarda de la actividad de un negocio.

Centro espejo: Instalación idéntica a otra y actualizada permanentemente, que permite un trasvase de la actividad empresarial inmediato. Suele tener un alto coste.

Contingencia: Evento que acontece y que puede provocar una interrupción del funcionamiento de una organización, pudiendo impactar de forma negativa en ésta.

Diagrama diferencial: Resultado Gráfico de la metodología MARION que muestra las diferencias entre el valor obtenido por el factor de seguridad analizado y el valor objetivo, ponderadas con la importancia de cada factor de seguridad.

Diagrama polar: Resultado gráfico de la metodología MARION que muestra los valores obtenidos por cada uno de los factores de seguridad analizados.

Equipos de recuperación: Grupos de personas definidos en el plan de contingencias para el ataque de un área específica de la organización cuando acontece una interrupción y estamos en la fase de recuperación. Formados por un jefe y uno o varios ayudantes que están en permanente contacto entre ellos y con la organización superior de la organización.

Evaluación cualitativa: Análisis de riesgo basada en la valoración de los parámetros por rango de importancia relativa.

Evaluación cuantitativa: Metodología de análisis de riesgo basada en valoración de parámetros por técnicas matemáticas y estadísticas y la aplicación de modelo.

Función crítica: Aquella cuya interrupción, por encima de un determinado umbral de tiempo, genera un impacto inadmisible.

Impacto: Consecuencia negativa que sufre una organización si las funciones que generan sus operaciones se vieran interrumpidas por cualquier circunstancia.

Impacto previsto: Impacto promedio estimado procedente de un suceso o riesgo determinado. Se calcula sobre la base de la experiencia y estadística histórica.

Incidente: Cualquier circunstancia o suceso no planificado que potencialmente puede interrumpir una o varias funciones críticas en el entorno operacional normal con consecuencias inaceptables para la organización.

Procedimientos de emergencia: Actuaciones inmediatas después de un incidente para proteger la integridad de las personas y para contrarrestar los efectos negativos en la inmediatez, dentro de nuestros activos de la organización.

Procedimientos de respuesta: Actuaciones que evalúan lo ocurrido y los daños producidos, y minimizar las consecuencias del suceso. Necesarios en muy corto plazo.

Procedimientos de recuperación: Restauran las operaciones de los equipos y programas y la carga de datos. Encaminados a conducir a la organización al estado que se encontraba antes del siniestro.

Registro vital: Conjunto de registros que son esenciales para preservar y continuar las operaciones de la organización y proteger sus derechos y los de sus empleados.

Salvaguardia: Proceso de realización de una copia preventiva o de reserva.

Umbral de recuperación: Tiempo máximo que una organización está dispuesta a aceptar desde que se produce la interrupción de una función hasta que se comienza a procesarla de nuevo de modo aceptable, aunque sea degradado.

Vulnerabilidad: Susceptibilidad de un sistema, producto o instalación a sufrir daños ante sucesos accidentales o intencionados. Susceptibilidad de la materialización de una amenaza sobre un activo.

13. Bibliografía:

PLANES DE CONTINGENCIA. La Continuidad del "negocio" en las organizaciones. Juan Gaspar Martínez. Editorial Díaz de Santos. 2004

"ANÁLISIS DEL PLAN DE CONTINUIDAD DEL NEGOCIO PARA UNA ENTIDAD BANCARIA, EN EL ÁREA DE CRÉDITO Y RIESGO INTEGRAL PARA ELPRODUCTO COMERCIAL FACTORING PARA EL AÑO 2009. Liliana Barbecho B. Andrea Montero Guevara. Instituto de Ciencias Matemáticas. Escuela Superior Politécnica del Litoral. Documentos electrónicos.

COBIT 4.1. IT Governance Institute. 2007. www.itgi.org

COBIT. 3rd Edition Audit Guidelines. July 2000. Released by the COBIT Steering Committee and the IT Governance Institute.

RECUPERACIÓN Y CONTINUIDAD DEL NEGOCIO. Alejandro Cerezo. INSYS. Semana de la seguridad informática. Aragón.

SISTEMAS DE ALMACENAMIENTO CENTRALIZADOS EN EL AYUNTAMIENTO DE GIJÓN. Alberto García.

GRUPO CEPSA. Sistemas de almacenamiento. Evolución.

V Reunión de auditores internos de banca central. AUDITORÍA A LOS PLANES DE CONTINGENCIA Y CONTINUIDAD. Rafael García Saura, Banco de España. Noviembre de 1999.

CONTINUIDAD DEL NEGOCIO. Manuel Ballester. ESNE. 2005. Conferencias FIST.

BUSINESS CONTINUITY INSTITUTE. BUSINESS CONTINUITY MANAGEMENT: GOOD PRACTICE GUIDELINES. David J. Smith FBCI. 2002.

NBC – SYSTEM. CONTINGENCY PLANNING AUDIT.
AUDIT PROGRAM. Deborah Ray, CISA. 1997.

Evaristo Prieto. SANITAS. 2002.

Guidelines on Business Continuity Management. 2001. Crown copyright.

Disaster recovery Meeting 2002. Como implementar arquitecturas y soluciones Disaster Recovery. Ernst & Young.

Qué Criterios seguir para dar respuesta a las cuestiones clave en DISASTER RECOVERY. Julián Marcelo. Universidad Politécnica de Valencia. Jornadas TotalData 2002.

Cómo asegurar la eficacia de un Plan de Recuperación de S. de I. a través de la Auditoría. J.Mª de Acuña – CISA.

International ISO/IEC STANDARD 17799. 2005.

BUSINESS CONTINUITY AND DISASTER RECOVERY PLANNING AND MANAGEMENT: PERSPECTIVE. 2001, Datapro.

BUSINESS CONTINUITY PLANNING. Paul Hugenberg, CISA, Sky Financial Group.

BELLSOUTH. Business Continuity. User´s Guide. 2001

Guía de desarrollo Plan de Continuidad del Negocio. Laura del Pino. 2007.

British Standards. 2006.
BS ISO/IEC 17799, Information technology _ Security techniques — Code of practice for information security management.

Internal Audit Business. Application Audit Program. April 2001

Comparex España, S.A. (Siniestro en el Edificio Windsor)
Soluciones de Continuidad de Negocio y Disaster Recovery. Yolanda Lafalla Marketing, Comparex Spain.

Seguridad de la información. Plan de contingencia. Versión 1.0. 10/1/2008.

Crisis Management Audit Plan
Denys Martin, MBA, CIA, FCPA. 1999

www.auditnet.org = >http://www.auditnet.org/docs/drpaudit.txt

Ami Johnson 1999

www.isaca.org

FIN