
**UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO**

**FACULTAD DE INGENIERÍA**

**TÍTULO DE LA TESIS:**

# APLICACIÓN DE LA NORMA NFPA-1600 "PLANES DE EMERGENCIA/ DESASTRES Y CONTINUIDAD DE NEGOCIOS" EN LA EXPLOTACIÓN PETROLERA

QUE PARA OBTENER EL GRADO DE:

**INGENIERA PETROLERA**

PRESENTA:

**NAYELLI MENDOZA ROCHA**

DIRECTOR DE TESIS:

**ING. RAMÓN DOMÍNGUEZ BETANCOURT**

**2013**

# Contenido

**CAPÍTULO 5. EL PLAN DE CONTINUIDAD DE NEGOCIO Y EL PLAN DE RECUPERACIÓN DE DESASTRES**

## Relación de Figuras



## Relación de Tablas

# DEDICATORIA

Jaz, Abue, Caro, Elo, Fano, Mariana, Mago, Juan y no me puedo olvidar de ustedes Ratonas.

No puede impedirse el viento, pero pueden construirse molinos.

Proverbio holandés

# Introducción

Las carreras de Ingeniería no deben concentrarse solamente en el desarrollo de habilidades técnicas independientemente de que las ciencias exactas son la prioridad en nuestra formación, no deben ser lo único, pues un ingeniero saldrá a la industria y se enfrentará a que saber sumar y restar no le bastará para desarrollarse como un profesional integral, es por esto, que los ingenieros nos debemos meter a la Administración y en este caso a la Gestión del Riesgo, ya que durante nuestro desarrollo profesional administraremos recursos, tanto materiales como humanos y debemos estar preparados para hacerlo de manera óptima.

En la elaboración de esta tesis se pretende realizar una guía para la elaboración de un Plan de Continuidad de Negocio con la finalidad de ser aplicada a la Industria Petrolera. Se plantean algunas preguntas; ¿Qué haríamos si la industria petrolera mexicana se detuviera por un día, ya sea por algún disturbio social, un fenómeno natural, un error humano, algún fenómeno tecnológico, un fenómeno biológico o hasta por la caída de un meteorito?, ¿Realmente nuestra sociedad y en particular la industria está preparada para afrontar este tipos de eventos? Sí la respuesta a estas dos preguntas es NO, sería una crisis para nuestra sociedad debido a nuestra dependencia hacia los hidrocarburos. Los hidrocarburos son la principal fuente de energía en México, al representar el 90% del consumo total, pues el 62% proviene del petróleo y el 28% del gas.

La norma NFPA 1600 es la única Norma Nacional e Internacional a base de procesos existente que identifica áreas funcionales clave y una estrategia global para estado de preparación de desastres y continuidad de negocios, tanto para organizaciones privadas como del sector público.

El Plan de Continuidad de Negocios también conocido como BCP por sus siglas en inglés (Business Continuity Plan), según la NFPA es un proceso continuo que con el apoyo de la alta dirección y los fondos para asegurar los pasos necesarios para identificar el impacto de las pérdidas potenciales, mantener estrategias viables de recuperación, planes de recuperación y continuidad de los servicios. Es un plan documentado y probado con el fin de responder ante una emergencia de manera adecuada, logrando así el mínimo impacto a la operación del negocio.

Un Plan de Continuidad de Negocio se compone de varias fases que comienzan con un análisis de los procesos que componen la organización. Este análisis servirá para priorizar qué procesos son críticos para el negocio y establecer una política de recuperación ante un desastre. Por cada proceso se identifican los impactos potenciales que amenazan la organización, estableciendo un plan que permita continuar con la actividad empresarial en caso de una interrupción.

Un Plan de Continuidad de Negocio, a diferencia de una Plan de Contingencia, está orientado al mantenimiento del negocio de la organización, con lo que priorizará las ***operaciones críticas de negocio*** necesarias para continuar en funcionamiento después de un incidente no planificado.

Existen muchos eventos importantes sobre los que no sabemos todo lo que quisiéramos saber. Entre ellos está el clima, que puede provocar desde una pequeña incomodidad hasta enormes tragedias; la confiabilidad de las instalaciones industriales, con su enorme cantidad de componentes que pueden fallar, la salud de nuestro cuerpo, con los dramáticos cambios que puede producir en nuestra forma de vida; y la aceptación por parte del consumidor de los productos o servicios que brindamos, de lo cual depende de la viabilidad de la industria; entre

muchos otros eventos. Esta breve lista sugiere que lo que no sabemos nos puede dañar y, desde luego, el cerrar los ojos a ello no nos protege del posible daño, sino que nos hace más vulnerables.

Los costos económicos de los desastres han aumentado significativamente, principalmente porque las actividades económicas se han ubicado en zonas con alta densidad de población, y con la alta vulnerabilidad hacia desastres de origen natural y humano. El mundo hoy ha acumulado más riqueza y bienestar, por lo que el riesgo también ha aumentado. (The Economist, 2012).

Al igual que con otros retos en la vida, el primer paso para lidiar con la incertidumbre y el riesgo es reconocer su existencia. Este primer paso generalmente no es difícil de dar una vez que nos preguntamos sobre la existencia de riesgo, sin embargo este primer paso no se da muchas veces simplemente porque uno no se pregunta si existe el riesgo. Y, al no cuestionarse su existencia, se asume implícitamente que no existe. Aparentemente esa es la manera como funciona nuestra mente: se asume certeza hasta que da uno cuenta de lo contrario.

El hecho que algunos riesgos se materialicen, es decir, que dejen de ser una mera probabilidad para transformarse en una mera realidad puede traer aparejado un sinnúmero de consecuencias esencialmente negativas, las cuales a la hora de evaluarlas económicamente se transformarán indefectiblemente en pérdidas económicas.

Ante los riesgos internos o externos que afectan la estrategia, los procesos y la información de una empresa, organización o proyecto, la Administración de Riesgos presenta una forma integrada y sistemática de identificar todos los recursos de dichos riesgos y responder ante ellos.

Cualquier riesgo identificado es un elemento o factor de falla del proyecto, de ahí la importancia de identificarlos para incorporarlos al análisis de riesgos del proyecto. Para realizar una identificación adecuada de riesgos existen diferentes técnicas para la identificación y clasificación de riesgos.

Una vez que se han identificado y clasificado los riesgos será necesario llevar a cabo un análisis de los mismos, lo cual se considera como el punto central de la definición de una estrategia de seguridad.

La metodología para realizar un adecuado análisis de riesgo es el resultado de la combinación de diferentes propuestas existentes en la industria, y utiliza métodos tanto cualitativos, como cuantitativos, los primeros permiten agilidad en el proceso y facilidad en la asignación de valores de impacto o riesgo, y los segundos nos permiten la precisión y exactitud, necesarias a la hora de tomar decisiones de tipo financiero, para mitigar un posible evento negativo a la operación y continuidad del negocio.

Un Plan de Continuidad de Negocio reducirá el número y la magnitud de las decisiones que se toman durante un período en que los errores pueden resultar mayores. El Plan establecerá, organizará y documentará los riesgos, responsabilidades, políticas y procedimientos, acuerdos con entidades internas y externas.

Cabe aclarar que la Continuidad de Negocio surgió en el área de Tecnologías de la Información, mejor conocida por sus siglas en inglés (IT), por tal motivo la mayoría de la información disponible se encuentra enfocada a dicha área, de tal forma que algunos de los ejemplos citados a lo largo de este trabajo son de IT pero puestos porque fungen como una guía para nuestra industria.

# 1. ¿Qué es una crisis?

## 1.1 Crisis

Existen muchos eventos importantes sobre los que no sabemos todo lo que quisiéramos saber. Entre ellos está el clima, que puede provocar desde una pequeña incomodidad hasta enormes tragedias; la confiabilidad de las instalaciones industriales, con su enorme cantidad de componentes que pueden fallar, la salud de nuestro cuerpo, con los dramáticos cambios que puede producir en nuestra forma de vida; y la aceptación por parte del consumidor de los productos o servicios que brindamos, de lo cual depende de la viabilidad de la empresa; entre muchos otros eventos. Esta breve lista sugiere que lo que no sabemos nos puede dañar y, desde luego, el cerrar los ojos a ello no nos protege del posible daño, sino que nos hace más vulnerables.

Una parte crítica al administrar cualquier proyecto es definir, analizar y administrar los tipos de crisis que se pueden encontrar. Pero para poder identificar las posibles crisis primero debemos definir ¿qué es una crisis?, y para esta pregunta existen diversas respuestas, pero de acuerdo a la Real Academia de la Lengua Española, una **crisis** es una mutación importante en el desarrollo de otros procesos o una situación de un asunto o proceso cuando está en duda la continuación, modificación o cese. Es decir, una crisis es cualquier incidente, evento, circunstancia, o series de incidentes o eventos, que representan o tienen el potencial de impacto en los resultados financieros, imagen, reputación o relación con clientes, inversionistas, reguladores, empleados o público en general. Todo esto genera una publicidad negativa y representa un tiempo extraordinario por parte del equipo directivo para enfrentarlo.

Cada crisis es distinta por naturaleza pero existen una serie de denominadores comunes, que derivan en recomendaciones que pueden ser aplicables a todas ellas como lo es planes de acción y sobre todo la prevención.

Muy pocas empresas tienen un plan anti-crisis, y las poquísimas que lo tienen, éste se orienta casi exclusivamente hacia las crisis catastróficas o accidentales. Aún en los países con gran cultura corporativa existe un gran desinterés por este tema, no digamos en nuestros países latinoamericanos.

## 1.2 ¿Por qué este aparente desinterés?

Por imprevisión. Nadie espera una situación de estas, por lo tanto nadie se prepara. Esto es un error pues por muy buena que sea nuestra campaña de imagen institucional, si nuestra institución es de servicio público o es de alta competitividad comercial, de cualquier forma se encuentra expuesta, pues cualquier actividad implica riesgo.

Infravalorar los riesgos potenciales. Sucede frecuentemente que menospreciamos y subestimamos algunas situaciones que después se convierten en escándalos que llevan a una crisis. Un cliente mal atendido, una negociación que no fue transparente, son suficientes para desencadenar una serie de situaciones negativas, pero generalmente no creemos que sea para tanto.

Identificación de la noción de crisis exclusivamente con catástrofes o accidentes imprevisibles. Creer que únicamente una inundación, una contaminación química o cualquier situación de estas connotaciones son críticas es un error que se paga caro.

Se puede decir que identificar y actuar rápido en la gestión de una crisis puede convertir a ésta en una magnífica oportunidad para lograr un reposicionamiento. Desde esta perspectiva, la comunicación de crisis debe ser entendida y asumida por la organización como un instrumento más para lograr una exitosa salida de la crisis.

Aunque toda crisis es diferente, dependiendo del tipo de empresa, existen una serie de patrones que pueden ayudar a prevenirla, o bien, a saber cómo actuar ante una eventualidad, donde el área de comunicación es fundamental.

La crisis tiene origen en incidentes operativos, legales, administrativos o financieros, pero crecen y generan nuevos problemas, erosionando la reputación de la firma por falta de una comunicación oportuna y efectiva.

## 1.3 Manejo de crisis

Hablar de enfrentarnos a una crisis, causada por un desastre natural o no, es hablar de manejo de crisis. Dicho manejo se entiende como aquellas acciones y/o medidas que se tomarán para enfrentarla en cada una de sus etapas. La pre crisis o etapa de prevención, la crisis y la post crisis o etapa de recuperación.

### 1.3.1Prevención

La primera etapa se trata de la de mayor importancia. La prevención es la clave para que una crisis sea superada de manera exitosa. Para esto se debe contar con un plan de crisis, que ofrezca las líneas de acción a seguir para una serie de escenarios que puedan predecirse y un grupo de personas que estén preparados para la toma oportuna de decisiones ante una crisis.

Durante la crisis el papel de grupo de expertos y su apego a lo establecido en el plan de crisis será de suma importancia. Una vez que la crisis ha sido superada, una vez que todo ha pasado, lo primero es cerciorarse de que la situación es real y de que no hay riesgos de que ésta vuelva a gestarse. Pero ninguna gestión de manejo de crisis puede cerrarse sin ser los hechos previamente evaluados y analizados pues la experiencia servirá para afrontar nuevas situaciones.

### 1.3.2 Comunicación

Aunque una crisis no se soluciona sólo con comunicación, sin ésta el problema se profundiza y prolonga; de esta manera el proceso comunicativo puede convertirse en el mejor aliado para una compañía, o bien, en su peor enemigo, señala José Luis López Aguirre, coordinador del grupo de investigación en redes sociales de la Universidad Panamericana.

La comunicación se concibe como el proceso dinámico que permite la interacción, cambios y progresos de los individuos. Se convierte en una función indispensable para el buen funcionamiento y desarrollo tanto de persona como de organizaciones.

En las empresas y organizaciones el papel de la comunicación no sólo es indispensable en el momento de hacer llegar los mensajes en los distintos niveles o hacia el exterior con fines de crecimiento o la búsqueda de ganancias.

La comunicación también juega un papel primordial cuando dichas organizaciones se enfrentan a problemas que, en ocasiones, pueden tomarles por sorpresa y traerles seria repercusiones para la misma.

El primer punto de partida para hablar de comunicación de crisis es entender qué es una crisis de comunicación. Se habla de comunicación de crisis cuando nos encontramos ante una situación crítica que puede dañar la imagen o reputación de la organización. En un sentido más amplio, la comunicación de crisis, puede hace referencia a todos los procesos comunicativos que se llevan a cabo cuando se está enfrentando una etapa de crisis.

Cuando llega el momento de enfrentar una crisis, es indispensable echar mano de la comunicación como la herramienta base para sobrellevar y posteriormente, recuperarse de una crisis. Al igual que la gestión de la crisis como tal, el manejo de la comunicación en esta etapa debe ser organizada y bien planeada.

## 1.4 El valor de la reputación

Según datos de la encuestadora Weber Shandwick, la reputación representa aproximadamente 63 por ciento del valor de mercado de una firma, y es lo primero que está en riesgo en una crisis.

"Las consecuencias de no actuar adecuadamente ante una situación adversa pueden ser catastróficas; a corto plazo se impactan las ventas, y en una situación muy grande puede llegarse incluso al cierre, por eso es importante estar preparados", dijo por su parte José Ramón Barreiro, director de Comunicación de la Universidad La Salle.

### 1.4.1 Ejemplos

**Buen manejo de crisis: Domino's Pizza**

En abril del año 2009, dos empleados de la empresa Domino's Pizza en Estados Unidos, publicaron un video en YouTube donde realizaban acciones desagradables mientras preparan la comida de la marca.

El hecho trascendió a los medios tradicionales de comunicación y la compañía respondió días después a través de radio, televisión y medios impresos; sin embargo, la problemática por internet aún no se atacaba.

La compañía identificó la audiencia de la crisis, creó una cuenta de Twitter y motivó a sus empleados para actualizar continuamente sus cuentas personales.

La compañía pudo contener el furor de los consumidores hasta que grabó y publicó en YouTube un video donde su presidente expresó su pesar por el hecho, calificándolo como aislado y resaltando los valores y el trabajo de la compañía.

Domino's reforzó sus medidas sanitarias y no ha tenido nuevos problemas y ha recobrado la confianza de sus consumidores.

**Mal manejo de crisis: British Petroleum**

A partir de 2010, el nombre de la británica British Petroleum (BP) es sinónimo de catástrofe ambiental.

El 20 de abril de ese año, una explosión en la plataforma petrolera Deepwater Horizon en el Golfo de México inició la peor crisis de imagen que la firma haya enfrentado desde su fundación en 1908.

La plataforma se hundió con un saldo de 11 muertos y provocó uno de los mayores derrames petroleros de la historia, con 60 mil barriles diarios.

En una muestra de mal manejo de crisis, la firma fue acusada de ocultar la gravedad del asunto.

Organizaciones ambientalistas hicieron manifestaciones públicas por todo el mundo sin una respuesta de la petrolera.

Además de las pérdidas en operaciones de limpieza y gastos legales, la firma tuvo que pagar siete mil 800 millones de dólares de compensación a los afectados, y su imagen internacional quedó irremediablemente ligada a la catástrofe.


**Figura 1.1.- ¿Qué origina una crisis?**

## 1.5 Características de la crisis

♣ Ser inesperada, coarta la capacidad de reacción.

♣ Ser imprevisible.

♣ Ser de relevancia para públicos de la empresa como consumidores, accionistas, proveedores y vecinos.

♣ Tener una potencialidad causante de pánico, aumentado por la desinformación.

♣ En algunos casos, tener un origen ajeno a la comunicación.

♣ Disponibilidad de información incompleta.

♣ Escalado de acontecimientos, lo pequeño se hace inmenso.

♣ Sensación de pérdida de control.

♣ Estrés y pánico.

♣ Decisiones erróneas por enfoque a corto plazo.

## 1.6 Tipos de crisis

Se pueden dar diferentes situaciones que generan una crisis, pero las más comunes son:

• Acontecimientos políticos y conflictos sociales (protestas violentas, conflictos políticos y comerciales, etc.)

• Accidentes (relacionados con el transporte, que afecten el medio ambiente, incendios, derrames químicos, etc.)

• Eventos de origen criminal (secuestros, asesinatos, sabotajes, etc.)

• Asuntos jurídicos (de discriminación racial, de abuso sexual, plagios, etc.)

• Hechos de tipo económico (bancarrota, fraude, corrupción, etc.)

• Retirada de productos (defectos de fabricación, por utilizar sustancias prohibidas en su elaboración, etc.)

• Ataques informáticos (virus, entrada de hackers a sistemas, etc.)

Una vez que se encuentra definido lo que es una crisis, sus características así como algunos tipos de crisis que existen es necesario analizar este tema pero en la Industria Petrolera.

El petróleo ha sido determinante en México, para su economía, finanzas públicas, industria, desarrollo tecnológico, balanza comercial, y sus relaciones con el exterior, en particular con los Estados Unidos. Pero, más aún, ha sido un elemento determinante para la consolidación de México como Estado nacional y como un país con una economía emergente, con un nivel de desarrollo medio.

Por todo lo anterior mencionado es evidente que la dependencia de nuestra sociedad respecto del petróleo y el impacto que tiene en nuestras vidas es tan alta que resulta fundamental asegurar el abastecimiento ininterrumpido a la población. Los esfuerzos por reducir tal dependencia de parte de nuestro país comprenden varias iniciativas y proyectos que aprovechas fuentes nuevas y renovables de energía (celdas fotovoltaicas, turbinas eólicas, energía geotérmica además de la hidroeléctrica) como alternativas garantizadoras del desarrollo energético sostenible. Pero la dependencia persiste: el 60% de la energía que consumimos es producida a partir de la combustión de derivados de petróleo.

# 2. Análisis de Riesgo

## 2.1 Riesgo

¿Qué es un riesgo?, un riesgo es un peligro cuantificado e involucra dos factores:

- *Consecuencia o Severidad*: Cuánto de qué causa cuánto daño a quién por el incidente.
- *Frecuencia o Probabilidad*: Qué tan seguido se puede esperar que ocurra el incidente.

**RIESGO= Frecuencia X Consecuencia**

El hecho que algunos riesgos se materialicen, es decir, que dejen de ser una mera probabilidad para transformarse en una mera realidad puede traer aparejado un sinnúmero de consecuencias esencialmente negativas, las cuales a la hora de evaluarlas económicamente se transformarán indefectiblemente en pérdidas económicas.

Al hablar de riesgos se abre un gigantesco nicho de definiciones, situaciones, medidas de contención y tratamiento, pero el riesgo a su vez, por facilidad y el impacto que puede representar para una organización afectada se puede establecer en varios campos o tipos:

- Operativo
- Financiero
- De Negocio
- Legal
- Reputacional o de imagen
- Ambiental
- Tecnológico
- Entre otros

Hay varios factores o puntos a tener en cuenta al hablar de riesgo:

- El riesgo se identifica, evalúa y trata a partir de controles.
- Al hablar de riesgo, implícitamente se habla de amenazas, atacantes, vulnerabilidades e impacto.
- Cómo se maneje o categorice el riesgo depende de la organización/ empresa/ proyecto, dado que para la gerencia o administración un riesgo puede representar una oportunidad, esto se asocia al “apetito de riesgo” de estos directivos.
- El análisis de riesgos se puede desarrollar sobre activos y/o procesos, la visión que se seleccione al evaluar y controlar los riesgos depende del tipo de negocio y facilidad de manejo, para algunos puede resultar más sencillo analizar procesos previamente identificados más que un listado interminable de activos en la organización.
- Se pueden realizar evaluaciones cuantitativas y cualitativas dentro del análisis de riesgo.
- El riesgo no desaparece, siempre estará latente, lo que se busca con los controles es reducirlo a 0 o al mínimo posible.

- En una organización establecer un buen mapa de riesgos permite conocer a que se enfrentan en el medio que se desarrollan. Los controles establecidos o administración seleccionada para estos riesgos ofrecen medios para evitar la incidencia de estos en la organización y su impacto.

## 2.2 Reconocimiento del Riesgo

Al igual que con otros retos en la vida, el primer paso para lidiar con la incertidumbre y el riesgo es reconocer su existencia. Este primer paso generalmente no es difícil de dar una vez que nos preguntamos sobre la existencia de riesgo, sin embargo este primer paso no se da muchas veces simplemente porque uno no se pregunta si existe el riesgo. Y, al no cuestionarse su existencia, se asume implícitamente que no existe. Aparentemente esa es la manera como funciona nuestra mente: se asume certeza hasta que da uno cuenta de lo contrario.

Existen obstáculos cognoscitivos, organizacionales y culturales para reconocer el riesgo e incertidumbre e integrarla en nuestra manera de pensar y decidir. Desde el punto de vista cognoscitivo debemos tener en cuenta que nuestras mentes tienen una capacidad limitada de manejo de información, por lo que abordamos la realidad mediante simplificaciones conceptuales o modelos de la realidad. Una de estas simplificaciones es la supresión de la incertidumbre. Generalmente la incertidumbre se suprime inconscientemente, y cuando se suprime conscientemente se argumenta que la incertidumbre es muy pequeña para que valga la pena tomarla en cuenta. Algunas veces estos argumentos son válidos y otras sólo indican la falta de deseo o capacidad para tomar en cuenta la incertidumbre. Si los argumentos son válidos, el obstáculo puede ser superado usando herramientas de análisis de decisiones que amplían nuestra capacidad cognoscitiva.

Desde el punto de vista organizacional, la mayoría de los formatos, procedimientos y sistemas de información de las empresas y otras organizaciones requieres que se asignen valores únicos; no permiten utilizar expresiones explícitas de incertidumbre por lo que aún cuando estas estén disponibles no tendrán cabida en la organización. Adicionalmente, nuestra cultura asocia la certeza con características personales positivas como la confianza en sí mismo, el éxito y el poder, por lo que la supresión de la incertidumbre puede derivarse del deseo de preservar una imagen de persona de negocios segura y exitosa. Finalmente, la supresión de la incertidumbre es un viejo hábito de la mayoría de los decisores y éste es difícil de cambiar. Superar los obstáculos organizacionales y culturales requiere una actitud racional que valore las ventajas personales y colectivas de hacer explícita la incertidumbre.

Al estar el riesgo definido en función de la probabilidad de que ocurra un suceso no deseado. Por lo tanto, una vez que se suprime la incertidumbre se deja de pensar en los riesgos, si se suprimió la incertidumbre de que algo deseable suceda, se asume que el riesgo es un hecho seguro y se actúa en consecuencia. En ambos casos el decisor estaría siendo víctima de esta forma especial de miopía que es no ver el espectro completo de sucesos asociados a un evento incierto.

Aún cuando se superan los obstáculos culturales, la integración de la medición de la incertidumbre en nuestra forma de pensar y de decidir no es automática: se requieren recursos técnicos para manejar la incertidumbre.

## 3.3 Análisis de Decisiones

El análisis de decisiones es una disciplina para ayudar a empresas e individuos que enfrentan situaciones de decisiones complejas, inciertas, de gran importancia, con elementos conflictivos o, en general, difíciles. Generalmente esta disciplina no se usa para decisiones rutinarias o de poca

importancia. Es el impacto de una decisión importante lo que justifica el análisis profesional de objetivos, alternativas, información y posibles resultados.

El objetivo del análisis de decisiones es que, al concluir el proceso de análisis, el decisor sepa con claridad lo que desea y cuanto lo valora, entienda la naturaleza de la situación de decisión que enfrenta, y conozca el impacto de las acciones que puede emprender. Como resultado de esto, el decisor sabrá con claridad lo que más le conviene hacer. Esto significa que el análisis de decisiones aspira a dar al decisor mucho más que sólo la recomendación sobre qué alternativa elegir.

### 2.3.1 Preferencias, alternativas, eventos inciertos y resultados

Al describir una situación de decisión podemos mencionar todos los elementos que forman parte de la situación de decisión. Dado que existe un número infinito de posibles situaciones de decisión, puede parecer que hay una gran variedad de esos elementos. Sin embargo, en toda decisión podemos identificar sólo cuatro tipos de elementos: preferencias, alternativas, eventos inciertos y resultados.

Distinguir estos tipos de elementos es una de las primeras tareas para tomar buenas decisiones. Esto es tan valioso que frecuentemente la sola identificación de estos elementos aclara significativamente la situación de decisión.

Las preferencias son lo que el decisor desea lograr, las alternativas son lo que el decisor puede hacer, los eventos inciertos son lo que puede pasar fuera del control del decisor, y los resultados son los efectos que surgen de las combinaciones de alternativas y sucesos.

## 2.4 Administración de Riesgo

Debido a que dentro de las operaciones de cualquier proyecto, actividad o negocio, se sucintan riesgos externos (ambiente como son: acciones de competidores, clientes, legisladores, gobiernos, grupos de interese especiales, las variables: tasas de interés e inflación, cambios reglamentarios, demanda en el mercado, oferta de mano de obra, posibles eventos catastróficos: tormentas, terremoto, guerras, terrorismo, etc.) e internos (relativos al uso adecuado de las tecnologías, la atención a clientes, a los empleados, a los proveedores, al cumplimiento de objetivos mediante los procesos operativos, los posibles eventos que interrumpirán las actividades como son: las prácticas poco éticas, fraudes, actos ilegales y pérdida de control de negocio y/o servicios) que afectan adversamente la capacidad de una organización para ejercitar exitosamente sus estrategias y alcanzar sus objetivos.

Ante tales riesgos que afectan la estrategia, los procesos y la información de una empresa, organización o proyecto la Administración de Riesgos presenta una forma integrada y sistemática de identificar todos los recursos de dichos riesgos y responder ante ellos.

### 2.4.1 Conceptos básicos de la Administración de Riesgos

#### 2.4.1.1 Incertidumbre

¿Es lo mismo riesgo que incertidumbre? Desde el punto de vista técnico, no. En el caso del riesgo, identifico una variable aleatoria y puedo determinar los niveles que tomará esa variable; además, también tengo elementos (objetivos o subjetivos) para calcular la probabilidad de ocurrencia de esos niveles. En el caso de la incertidumbre, si bien identifico la variable aleatoria y puedo determinar sus niveles, no hay forma de calcular las probabilidades de que ocurra.

Siempre hay incertidumbre sobre el futuro, pero también puede haber incertidumbre sobre eventos presentes o pasados. La incertidumbre nos rodea y su medición numérica puede ayudar a lograr coherencia en el manejo de este importante componente de las decisiones.

Hay muchos eventos inciertos y el primer paso hacia su medición es reconocer que algunos eventos son más inciertos que otros. En un afán por distinguir entre diferentes niveles de incertidumbre, cotidianamente se utilizan expresiones verbales para referirse a eventos inciertos. Algunos ejemplos son; es probable, casi no hay posibilidad, es lo más probable, es seguro, hay una buena probabilidad, es prácticamente imposible, es poco probable, es creíble, es altamente improbable. Sin embargo estas expresiones tienen serias limitaciones para su uso formal porque son ambiguas: al asignar valores a las expresiones por diferentes personas, los valores no sólo no son iguales, sino que frecuentemente ni siquiera son cercanos.

Expresar numéricamente la incertidumbre usando valores de probabilidad evita esas ambigüedades y permite usar todo el poder de las matemáticas para entender la incertidumbre y trabajar con ella. **La incertidumbre es sólo ausencia de información completa sobre el suceso.**

#### 2.4.1.2 Probabilidad de ocurrencia

Las probabilidades constituyen una rama de las matemáticas que se ocupa de medir o determinar cuantitativamente la posibilidad de que un suceso o experimento produzca un determinado resultado. La probabilidad constituye un importante parámetro en la determinación de las diversas casualidades obtenidas tras una serie de eventos esperados dentro de un rango estadístico.

Todo evento tiene una probabilidad de ocurrir, la forma de medir esa probabilidad es con una escala continua en % o con una escala continua de 0 a 1.

#### *2.4.1.3 Axiomas de probabilidad*

- *Axioma 1Los valores de probabilidad están entre 0 y 1.*
  Los valores numéricos de probabilidad se restringen al rango entre 0 y 1, inclusive. Esto es, $0 \leq \{A|\&\} \leq 1$ para cualquier suceso A. Las expresiones comunes de probabilidad en términos de porcentaje son una transformación de los valores de probabilidad al multiplicarse por 100.

- *Axioma 2 La probabilidad de un conjunto exhaustivo de suceso es 1*
  La probabilidad de la unión de todos los sucesos que pueden ocurrir en un evento incierto determinado es la unidad. Esto es, {$A_1$, o $A_2$, o…$A_n$|&}=1donde $A_1$, $A_2$,…, $A_n$ son todos los sucesos que pueden ocurrir en el evento incierto de interés.
- *Axioma 3 la probabilidad de la unión de sucesos excluyentes es la suma de sus probabilidades.*
  Si A y B son dos eventos mutuamente excluyentes, la probabilidad de que ocurra uno o el otro está dada por:

  {A o B|&}= {A|&} + {B|&}.

  Se dice que dos sucesos son excluyentes (o mutuamente excluyentes) cuando es imposible que ocurran los dos; ocurre uno u otro. Por ejemplo el ganar un contrato o no ganarlo son sucesos excluyentes. Si A y B son sucesos excluyentes tenemos que: {A,B|&}=0 (la probabilidad de que ocurra A y B a la vez es cero).

El valor de probabilidad de 1 significa certeza, seguridad de que el suceso va a ocurrir; el valor de probabilidad de cero, también significa certeza, la seguridad de que el suceso no va a ocurrir. Desde luego, a la gran mayoría de los sucesos se les asigna algún valor intermedio.

#### 2.4.1.4 Mediana

Es una medida de tendencia central; es el valor que se encuentra justo en medio de un conjunto de valores.

#### 2.4.1.5 Moda

En un conjunto de valores, es aquel o aquello que más veces se repiten dentro de ese conjunto.

#### 2.4.1.6 Curtosis

También llamada medida de concentración central. Es una medida del apuntamiento de distribución de probabilidad, la cual se enfoca en estudiar la zona de mayor y/o menor concentración de frecuencias alrededor de la media y en la zona central de la distribución. Compara una distribución x con una de tipo normal.

$$\boldsymbol{g = n * \sum_{i=1}^{n} \frac{(x_i - \overline{x})^4}{(\sum_{i=i}^{n}(x_i - \overline{x})^2)^2} - 3}$$

Donde:

g: curtosis

$\bar{x}$: Media aritmética

n: número de elementos

$x_i$: elemento i

#### 2.4.1.7 Media aritmética

Es un valor obtenido al sumar los valores de un conjunto y dividirlo entre el número de elementos de dicho conjunto, es decir, un promedio. Se representa con la siguiente ecuación:

$$\bar{x} = \frac{\sum_{i=1}^{n} x_i}{n}$$

Donde:

$\bar{x}$: Media aritmética

n: número de elementos

$x_i$: elemento i

#### 2.4.1.8 Desviación estándar (σ)

La desviación estándar o desviación típica es una medida de centralización o dispersión para variables de razón (ratio o cociente) y de intervalo, de gran utilidad en la estadística descriptiva. Es la raíz cuadrada de la varianza. Cuanto más pequeña sea la desviación estándar, más estrecha será distribución de probabilidad y más bajo será el riesgo de la alternativa.

$$\sigma = \sqrt{\sum_{i=1}^{n} \frac{(x_i - \bar{x})^2}{n-1}}$$

Donde:

$\bar{x}$: Media aritmética

n: número de elementos

$x_i$: elemento i

#### 2.4.1.9 Distribución de probabilidad

La distribución de probabilidad de un conjunto de valores de una variable x, es una función la cual asigna a cada valor de la variable x la probabilidad de que dicho valor aparezca.

Cuando la variable aleatoria toma valores en el conjunto de los números reales, la distribución de probabilidad está completamente especificada por la función de distribución, cuyo valor en cada real *y* es la probabilidad de que la variable aleatoria sea menor o igual que *y.* Las distribuciones de probabilidad se clasifican en:

#### 2.4.1.9.1 Distribución Normal

Conocida como distribución de Gauss, es una distribución de variable continua, de forma simétrica en la cual la moda, la media y la mediana coinciden en el mismo punto. Se le conoce también como "curva de campana" debido a su forma.

A continuación se muestra su fórmula:

$$\boldsymbol{f(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{(x-\mu)^2}{2\sigma^2}}, para -\infty \leq x \geq \infty}$$

Donde:

σ: desviación estándar

μ: media

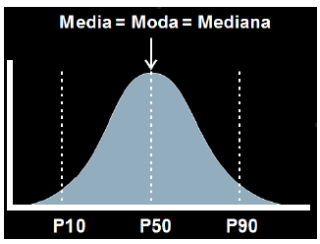


**Figura 2.1.- Distribución Normal**

#### 2.4.1.9.2 Distribución triangular

Una distribución triangular se define por tres parámetros: el mínimo, el máximo y el valor más probable. La distribución puede ser simétrica o no. Usualmente se utiliza como una aproximación de otras distribuciones.

Está definida por la siguiente función de probabilidad:

$$f(x) = \frac{2(x-a)}{\{(b-a)(m-a)\}} \; cuando \; a \leq x \leq m \; y \; a \leq m \leq b$$

$$= \frac{2(b-x)}{\{(b-a)(b-m)\}} \; cuando \; m \leq x \; b \; y \; a \leq m \leq b$$

$$= 0 \; en \; todos \; los \; demás \; casos$$

Donde:

a: valor mínimo

b: valor máximo

m: moda

La ubicación de la moda, media y mediana se muestra comúnmente en esta distribución de la siguiente manera:

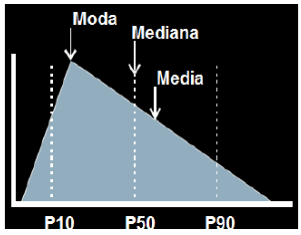


**Figura 2.2.- Distribución Triangular**

#### 2.4.1.9.3 Distribución log-normal

Es una distribución asimétrica, que comienza a partir de cero, aumenta hasta llegar a un máximo y luego va disminuyendo lentamente hacia infinito. Se relaciona a una distribución normal, ya que. X tiene una distribución log-normal cuando ln(X) tiene una distribución normal. Su función es la siguiente:

$$\boldsymbol{f(x) = \frac{1}{\sigma_1 x\sqrt{2\pi}} e^{\frac{(lnx-\mu_1)^2}{2\sigma_1^2}}, para \; 0 \leq x \leq \infty}$$

Donde:

σ: desviación estándar

μ: media

En la distribución log-normal la Moda < Mediana < Media

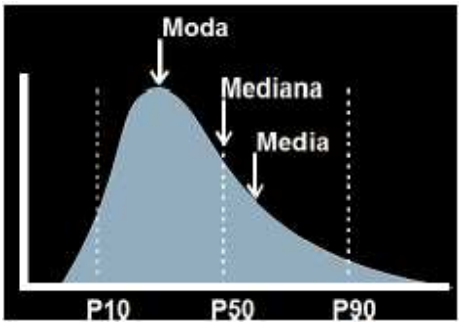


**Figura 2.3.- Distribución log-normal**

#### 2.4.1.9.4 Distribución Uniforme

Es una distribución en donde en un rango de valores todos tienen la misma probabilidad de ocurrir. La Moda, la Mediana y la Media son iguales en sus correspondientes percentiles.

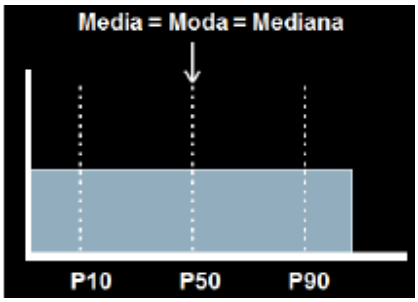


**Figura 2.4.- Distribución Uniforme**

#### 2.4.1.10 Teorema de límite central

El Teorema del Límite Central plantea que si una gama de valores está distribuida de modo normal, la distribución de los valores medios de la gama que se obtienen, también lo estarán respecto a cualquier tamaño de la muestra. Aún si la gama de valores no es normal, la distribución de los valores medios de la muestra será aproximadamente normal si el tamaño de la muestra es grande. Indica que no es necesario saber cuál es la distribución de la población para estar en condiciones de obtener inferencias con respecto a la gama a partir de datos muestrales. La única restricción es que el tamaño de la muestra sea grande, de 30 a más observaciones.

El Teorema del Límite Central es:

- Si la gama de valores muestreada está distribuida de manera normal, la distribución de los valores medios de la muestra estarán normalmente distribuidos respecto a todos los tamaños muestrales.
- Si la gama de valores no es normal, la distribución de los valores medios de la muestra serán aproximadamente normal respecto a un tamaño muestral grande.

#### 2.4.1.11 Valor Esperado

Sea X una variable aleatoria discreta con función de probabilidades f(x). Entonces, el valor esperado de la variable aleatoria X, el cual se representa por E(X), está definido por:

$$E(X) = \sum x_i \ f(x_i)$$

El valor esperado representa el valor promedio que se espera suceda, al repetir el experimento en forma independiente una gran cantidad de veces. El valor esperado se interpreta físicamente como el centro de masa o centro de gravedad de la distribución de probabilidad, por lo que es igual a la media o promedio aritmético, los cuales se representan con la letra μ.

El valor esperado proporciona una buena estimación de los beneficios o costos esperados por el evento riesgoso.

**Valor Esperado = Probabilidad X Impacto**

El valor esperado proporciona una idea de los costos pero no se debe emplear para tomar decisiones.

#### 2.4.1.12 Riesgos imprevistos

Los riesgos imprevistos son aquellos que pueden ocurrir sin haber anticipado su ocurrencia. Normalmente dependen de una inusual combinación de factores que no se pudieron detectar con anticipación, por lo tanto son los más peligrosos y de ahí la importancia de identificar la mayor cantidad de posibles eventos imprevistos durante el procesos de planeación del riesgo.

#### 2.4.1.13 Impacto del Riesgo

El impacto del riesgo no es más que una consecuencia cuantificable del riesgo. Una medida del grado de daño o cambio sobre un activo.

### 2.4.2 ¿Qué se puede hacer con los Riesgos?

*Regla de la 4 T´s de Frank Bird*

- **Terminarlos.-** No realizar la actividad o proyecto elimina al riesgo.
- **Tolerarlos.-** Realizar la actividad o proyecto y que ocurra lo que tenga que ocurrir.

- **Tratarlos.-** Administrar al riesgo tomando las medidas para que no ocurra o en caso de que ocurra.
- **Transferirlos.-** Pagar a alguien se haga cargo de las consecuencias del riesgo.

Sin embargo, por más que el riesgo se reduzca o transfiera, siempre seguirán existiendo riesgos residuales inevitables.

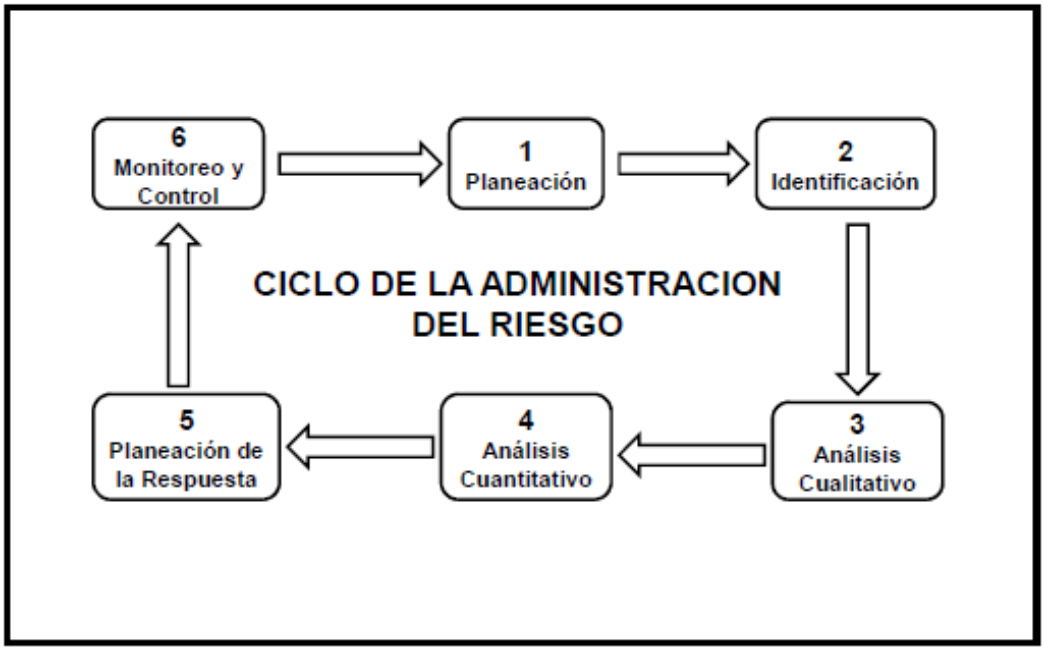


**Figura 2.5.- Ciclo de la Administración del Riesgo**

### 2.4.3 Metodología para la Administración de los Riesgos

[5]La Administración de Riesgo puede ser definida como el proceso sistemático de planear, identificar, analizar, responder y controlar los riesgos de una actividad o proyecto. Este proceso trata de maximizar la probabilidad de ocurrencia de sucesos positivos y minimizar la de sucesos adversos. Es decir, este proceso busca alinear la estrategia, los procesos, las personas, la tecnología y el conocimiento con el propósito de evaluar y administrar las incertidumbres que la actividad o proyecto enfrenta al crear valor.

#### 2.4.3.1 *Planeación de la Administración del Riesgo*

Como cualquier otro proceso, la Administración del riesgo debe planearse y programarse de manera que haga parte de todo el quehacer de la entidad.

Para el diseño de esta planeación es fundamental tener claridad en la misión de la empresa, en sus objetivos y tener una visión sistemática de manera que no se perciba la administración del riesgo como algo aislado. Igualmente es necesario conocer sobre el tema de riesgos y la metodología propuesta.

Dicha planeación debe contener: ¿Cuándo va a empezar a manejarse el tema dentro de la entidad?, ¿Quiénes van a participar directamente en el proceso?, ¿Cuándo van a realizarse las capacitaciones y a quién van a ir dirigidas? Y ¿Cómo se va a articular el tema dentro de la planeación y con los procesos?, entre otros.

#### 2.4.3.2 *Identificación del Riesgo*

El proceso de identificación del riesgo debe ser permanente e interactivo integrado al proceso de planeación y debe partir de la claridad de los objetivos estratégicos de la entidad para la obtención de resultados.

Previa a la identificación de los riesgos es importante tener en cuenta tal como se mencionó anteriormente, los factores que pueden incidir en la aparición de los mismos, los cuales pueden ser externos e internos y llegar a afectar la organización en cualquier momento.

Deben considerarse también los factores externos relacionados con la entidad como son: económicos, sociales, de orden público, políticos, legales y cambios tecnológicos entre otros y como factores internos: la naturaleza de las actividades de la entidad, la estructura organizacional, los sistema de información, los proceso y procedimientos y los recursos económicos.

Para la identificación se recomienda la aplicación de varias herramientas y técnicas como por ejemplo: entrevistas estructuradas con expertos en el área de interés, reuniones con directivos y con personas de todos los niveles en la entidad, evaluaciones individuales usando cuestionarios, lluvias de ideas con los servidores de la entidad, entrevistas e indagaciones con personas ajenas a la entidad, usar diagramas, análisis de escenarios y hacer revisiones periódicas de factores económicos y tecnológicos que puedan afectar la organización, entre otros.

Igualmente pueden utilizarse diferentes fuentes de información de la entidad, tales como registros históricos, experiencias significativas registradas, opiniones de especialistas y expertos, informes de años anteriores, los cuales pueden proporcionar información importante, la técnica utilizada dependerá de las necesidades y naturaleza de la entidad.

Cualquier riesgo identificado es un elemento o factor de falla del proyecto, de ahí la importancia de identificarlos para incorporarlos al análisis de riesgos del proyecto.

Una manera de visualizar los riesgos es a través de la utilización del formato de identificación de riesgos el cual permite hacer un inventario de los mismos, definiendo en primera instancia los riesgos, posteriormente presentando una descripción de cada uno de estos y finalmente definiendo las posibles consecuencias. Es importante centrarse en los riesgos más significativos para la entidad.

| Riesgo | Descripción | Posibles Consecuencias |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

**Tabla 2.1.- Formato de Identificación de Riesgos**

**Riesgo:** posibilidad de ocurrencia de aquella situación que pueda entorpecer el normal desarrollo de las funciones de la entidad y le impidan el logro de sus objetivos.

**Descripción:** se refiere a las características generales o las formas en que se observa o manifiesta el riesgo identificado.

**Posibles consecuencias:** corresponde a los posibles efectos ocasionados por el riesgo, los cuales se pueden traducir en daños de tipo económico, social, administrativo, entre otros.

**Técnicas de identificación de riesgos**

Existen múltiples técnicas que pueden ayudar a identificar riesgos. A continuación se muestran algunas de las más conocidas:

**Técnicas de Recopilación de Información**

- *Tormenta de ideas*.- es una herramienta de trabajo grupal que facilita el surgimiento de ideas sobre un tema. La lluvia o tormenta de ideas, habitualmente conocida como "brainstorming", es una técnica de grupo para generar ideas originales en un ambiente relajado. La meta de la tormenta de ideas es obtener una lista completa de los riesgos del proyecto. El equipo del proyecto suele realizar tormentas de ideas, a menudo con un grupo multidisciplinario de expertos que no pertenecen al equipo. Se generan ideas acerca de los riesgos del proyecto bajo el liderazgo de un facilitador. Los riesgos luego son identificados y categorizados por tipo y sus definiciones son refinadas.

- *Técnica Delphi.-* La técnica Delphi es una forma de llegar a un consenso de expertos. Es la búsqueda de consenso entre especialistas (expertos) sobre eventos futuros. Los expertos en riesgos de proyectos participan en esta técnica de forma anónima. Un facilitador emplea un cuestionario con definición clara de objetivos y resultados deseados, para solicitar ideas acerca de los riesgos importantes del proyecto. Las respuestas son resumidas y luego enviadas nuevamente a los expertos para que realicen comentarios adicionales. En pocas rondas de este proceso se puede lograr el consenso. La técnica Delphi ayuda a reducir sesgos en los datos y evita que cualquier persona ejerza influencias impropias en el resultado. Esta técnica está caracterizada por realizar cuestionarios de forma anónima, con un tratamiento estadístico simple y una re evaluación de respuestas para nuevo cuestionario. Los expertos que forman parte de esta técnica han de tener un amplio conocimiento sobre los riesgos.

- *Entrevistas.-* Entrevistar a participantes experimentados del proyecto, interesados y expertos en la materia puede servir para identificar riesgos. Las entrevistas son una de las principales fuentes de recopilación de datos para la identificación de riesgos.

***Clasificación del riesgo***

Durante el proceso de identificación del riesgo se recomienda hacer una clasificación de los mismos teniendo en cuenta los siguientes conceptos:

**Riesgo Estratégico:** Se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.

**Riesgos Operativos:** Comprende los riesgos relacionados tanto con la parte operativa como técnica de la entidad, incluye riesgos provenientes de deficiencias en los sistemas de información, en la definición de los procesos, en la estructura de la entidad, la desarticulación entre dependencias, lo cual conduce a ineficiencias, oportunidades de corrupción e incumplimiento de los compromisos institucionales.

**Riesgos de Negocio:** Como leyes nuevas, cambios de gobierno, evolución macroeconómica; la gestión de estos riesgos suele formar parte del proceso de planificación empresarial.

**Riesgos de Control:** Están directamente relacionados con inadecuados o inexistentes puntos de control y en otros casos, con puntos de control obsoletos, inoperantes o poco efectivos.

**Riesgos Financieros:** Se relacionan con el manejo de los recursos de la entidad que incluye, la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes de cada entidad. De la eficiencia y transparencia en el manejo de los recursos, así como su interacción con las demás áreas dependerá en gran parte el éxito o fracaso de toda entidad.

**Riesgos de Cumplimiento:** Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.

**Riesgos de Tecnología:** Se asocian con la capacidad de la Entidad para que la tecnología disponible satisfaga las necesidades actuales y futuras de la entidad y soporten el cumplimiento de la misión.

**Riesgo en proyectos**

A continuación se enlistan algunas de las características del riesgo en proyectos:

- El riesgo se encuentra en el futuro del proyecto.
- Un riesgo es un evento o condición incierta que si sucede, tiene efecto en cuando menos uno de los objetivos del proyecto.
- Un riesgo puede tener una o más causas y, si ocurre puede tener uno o más impactos.
- Una causa puede ser un requisito, un supuesto, una restricción o una condición.

Los impactos de los riesgos en proyectos se van a reflejar en sus tres restricciones básicas, mejor conocidas como "Restricción Triple" del proyecto. En todo proyecto se dice que existe una restricción triple, que es el tiempo, el costo y el alcance. Digámoslo de otra forma, la modificación de cada una de ellas tiene un claro impacto en las otras dos.

- Alcance (¿mejor?)
- Tiempo (¿más rápido?)
- Costos (¿más barato?)

Pero realmente no sólo son tres restricciones la que tiene un proyecto sino cinco, es decir, a las tres anteriores se le agregan objetivo y recursos/organización. El objetivo del proyecto es una restricción ya que condiciona a las demás, sobre todo si está bien definido y los recursos que dispongamos para la realización del proyecto es otra restricción clave, ya que nos condicionará bastante en la forma en la cual decidamos realizar el proyecto.

Finalmente un factor adicional y clave para entender la complejidad de los proyectos, es que estos 5 factores no son estáticos y que por tanto cambian a los largo del recorrido de un proyecto derivados tanto de los condicionantes internos del proyecto de los condicionantes externos, es decir, del entorno tan cambiante que nos rodea.


**Figura 2.6.- Restricción quíntuple de un proyecto**

La clave del éxito en los proyectos consiste en NO ignorar los riesgos o estar pendiente de ellos, sino en analizarlos y controlarlos de manera efectiva. La gran ventaja del análisis y control de riesgos es que permite descubrir oportunidades que, de otra forma, no se llevarían a cabo por ser considerados, a priori, demasiado riesgosos.

Es necesario analizar los riesgos que se encuentran latentes en la organización y/o empresa, proyectos, etc. En la práctica, gran parte de los riesgos del proyecto están relacionados con los cambios de agenda y los desvíos de presupuesto que ocurren durante la ejecución del proyecto. Por lo tanto, para poder evitar efectos negativos del riesgo ante cambios de planes es necesaria una administración del riesgo para alcanzar los resultados del proyecto.

El análisis de Riesgo se considera como el punto central de la definición de una estrategia de seguridad, perfectamente alineada con la visión de la organización, dentro de su entorno de operación.

La metodología para realizar un adecuado análisis de riesgo es el resultado de la combinación de diferentes propuestas existentes en la industria, y utiliza métodos tanto cualitativos, como

cuantitativos, los primeros permiten agilidad en el proceso y facilidad en la asignación de valores de impacto o riesgo, y los segundos nos permiten la precisión y exactitud, necesarias a la hora de tomar decisiones de tipo financiero, para mitigar un posible evento negativo a la operación y continuidad del negocio.

Se han establecido dos aspectos para realizar el análisis de los riesgos identificados:

- **Probabilidad:** la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de frecuencia o teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado.
- **Impacto:** consecuencias que puede ocasionar a la organización la materialización del riesgo.

A continuación se presentan algunos ejemplos de las escalas que pueden implementarse para analizar los riesgos.

## 2.5 Análisis Cualitativo

Se refiere a la utilización de formas descriptivas para presentar la magnitud de consecuencias potenciales y la posibilidad de ocurrencia. Se diseñan escalas ajustadas a las circunstancias de acuerdo a las necesidades particulares de cada organización o el concepto particular del riesgo evaluado.

Escala de medida cualitativa de **PROBABILIDAD**: se deben establecer las categorías a utilizar y la descripción de cada una de ellas, con el fin de que cada persona que aplique la escala mida a través de ella los mismos ítems, por ejemplo:

**ALTA:** es muy factible que el hecho se presente.

**MEDIA:** es factible que el hecho se presente.

**BAJA:** es muy poco factible que el hecho se presente.

Con el fin de derivar una probabilidad o una estimación de la ocurrencia de un evento, los siguientes factores deben ser tomados en cuenta:

- ✓ Fuente de amenaza y su capacidad.
- ✓ Naturaleza de la vulnerabilidad.

Una vulnerabilidad es la potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre un activo.

Para estimar la vulnerabilidad o frecuencia potencial de las amenazas que afectan a cada activo o grupo, debe participar el responsable y por tanto buen conocedor de cada activo, suficientemente informado por el especialista para que comprenda o imagine con objetividad la acción potencial de las amenazas.

Se puede considerar tres tipos de vulnerabilidades:

- Vulnerabilidad intrínseca, si sólo depende del activo y de la amenaza.
- Vulnerabilidad efectiva, resultante de la aplicación de las salvaguardas existentes.
- Vulnerabilidad residual, resultante de aplicar las salvaguardas complementarias, aconsejadas como resultado del análisis y gestión de riesgos.

Debemos medir la vulnerabilidad, considerando la *distancia* entre la amenaza potencial y su materialización como agresión real sobre el activo. Siempre que sea posible, calcularemos la frecuencia de ocurrencia a partir de hechos objetivos (estadísticas de incidentes o series empíricas). Por ejemplo, una ocurrencia por semana laboral lleva a una frecuencia de 1:5=0,2; una ocurrencia por mes laboral de una frecuencia de 1:20=0,05.

La vulnerabilidad, es para nuestros efectos un peligro que en caso de manifestarse tiene el potencial de comprometer el normal funcionamiento de la compañía, proyecto y/u organización o pueden dañar profundamente su imagen corporativa.

Si consideramos a lo anterior, a la evaluación de riesgos basada en la severidad y probabilidad le hace falta un componente muy importante, este es el nivel de preocupación o conmoción que dicho evento puede generar en la sociedad, es decir, el grado de atención que la manifestación de esta vulnerabilidad puede despertar en los medios de prensa, autoridades, comunidad y/o trabajadores.

La probabilidad que una vulnerabilidad potencial pueda ser explotada por una fuente de amenaza la podemos clasificar en alta, media-alta, media, media-baja y baja, como se describe a continuación.

Con el fin de poder determinar la probabilidad de ocurrencia de ciertos eventos, se define una escala en la cual, a una probabilidad alta, le asignamos el valor de P=5, para una probabilidad media e asignamos el valor P=3 y por último para una probabilidad baja le asignamos el valor P=1, esta asignación se define en proporción directa al número de veces que el evento puede ocurrir en un periodo de un año. Para el caso P=5 se considera que ocurre al menos dos veces al año.

| Nivel | Definición |
|---|---|
| **Alta = 5** | *La amenaza esta altamente motivada y es suficientemente capaz de llevarse a cabo.* |
| **Media-Alta =4** | *La amenaza está fundamentada y es posible.* |
| **Media = 3** | *La amenaza es posible.* |
| **Media-Baja = 2** | *La amenaza no posee la suficiente capacidad.* |
| **Baja = 1** | *La amenaza no posee la suficiente motivación y capacidad.* |

**Tabla 2.2.- Probabilidad de Ocurrencia de un Evento**

### 2.5.1 Técnicas de valoración cualitativa de riesgos

- *Delphi.-* La técnica Delphi es de utilidad cuando se quiere llegar a un consenso entre un número de personas evitando la influencia entre las mismas. La técnica Delphi es utilizada en multitud de situaciones. Un ejemplo de ello es su uso durante la fase de identificación de riesgos. También se suele utilizar durante la fase de análisis cualitativo del proceso de gestión de riesgos.

- *Matriz Probabilidad-Impacto.-* La matriz de probabilidad impacto es una técnica comúnmente utilizada para realizar valoraciones cualitativas de riesgos. Se explica en más profundidad en el apartado de análisis de riesgos.

## 2.6 Análisis Cuantitativo

El análisis de riesgo cuantitativo es la evolución matemática de la probabilidad de cada riesgo y sus consecuencias en las salidas del proyecto. El análisis de riesgo cuantitativo utiliza técnicas para:

- Determinar la probabilidad de conseguir los objetivos específicos del proyecto
- Cuantificar el valor esperado del proyecto y sus probabilidades, y determinar el coste y la programación para reservas de contingencia
- Identificar objetivos de coste, cronograma o alcance realistas y viables

- Determinar la mejor decisión de dirección de proyectos cuando algunas condiciones o resultados son inciertos

El análisis de riesgos cuantitativo generalmente sigue al análisis de riesgos cualitativos, aunque en ocasiones se lleva a cabo directamente tras la identificación de riesgos. Los elementos de riesgos complejos pueden requerir una repetición del análisis mediante herramientas de software sofisticadas. El análisis cuantitativo de riesgos debe repetirse después de la planificación de la respuesta a los riesgos, también como parte del seguimiento y control de riesgos, para determinar si el riesgo general del proyecto ha sido reducido satisfactoriamente. Las tendencias pueden indicar la necesidad de más o menos acciones de gestión de riesgos.

El análisis cuantitativo puede ser complicado por una serie de factores:

- Los riesgos pueden interactuar de formas no esperadas
- Un único evento puede causar múltiples efectos
- Las oportunidades (reducir costos) para un involucrado en el negocio, pueden ser un riesgo para otro (reducir beneficios)
- No todos los riesgos son cuantificables, algunos pueden definirse de forma cualitativa
- Las técnicas matemáticas utilizadas pueden dar una falsa impresión de la precisión y la fiabilidad

En las situaciones anteriores, es necesario que el equipo de proyecto utilice su mejor juicio, documentando sus valoraciones y todos los factores relacionados.

***a) Determinar el impacto de ocurrencia de riesgos de forma cuantitativa***

Durante esta etapa, el impacto del riesgo debería cuantificarse en términos monetarios cuando sea posible. El impacto podría afectar al coste, a la programación, al alcance, a la calidad o a una combinación de los factores anteriores. El equipo debería definir no solo cómo de grande es el impacto sino también qué elementos son los más afectados y documentar los resultados en el registro de riesgos.

Por ejemplo si un riesgo implicara un coste adicional de 5000 euros, esta cantidad será identificada como el impacto asignado a dicho riesgo. O si por ejemplo un determinado evento causase un aumento de una semana en la agenda, también sería considerado como impacto de un riesgo y como tal también debería ser asociado a un coste, por ejemplo, el coste que implicaría cubrir los recursos que se van a utilizar durante esa semana. Por lo tanto, los impactos del riesgo normalmente deberían representarse en forma de costes, siempre aplicando ciertos márgenes.

***b) Estimar la probabilidad de ocurrencia de riesgo de forma cuantitativa***

Durante esta etapa, la probabilidad de ocurrencia del riesgo está cuantificada, dando así un valor porcentual real.

***c)* Calcular el valor esperado**

El valor esperado es un dato estadístico que proporciona significado acerca de las pérdidas o ganancias que se tendrían en caso de que el riesgo ocurriese. Esto deriva de un simple cálculo:

Valor esperado = Impacto del riesgo * Probabilidad del riesgo

El impacto del riesgo debería indicarse en formato monetario o en duración días/semanas, y la probabilidad de riesgo será un número dentro del rango 0.01 - 0.99.

También podría tenerse en cuenta un factor para cuantificar aún más el riesgo, en cuyo caso se utilizaría la siguiente fórmula:

Impacto total de riesgo = Impacto * Probabilidad * Factor

Si se utilizan métodos cuantitativos para determinar la probabilidad y el impacto del riesgo, el proceso no es tan sencillo. En este caso la valoración a realizar es subjetiva y el único método que puede utilizarse es el método 'juicio de expertos' comentado con anterioridad, donde los expertos en la materia expresan sus opiniones sobre la probabilidad, el impacto y el riesgo total asociado a ese determinado riesgo.

Es importante ir documentando el proceso de análisis (tanto cualitativo como cuantitativo) y la priorización de los riesgos. Podría utilizarse para ello un registro de riesgos, y así ir registrando las conclusiones obtenidas del análisis de riesgos, incluyendo la prioridad, el impacto y la categoría de cada impacto.

En los procedimientos de gestión de riesgos se podrían definir, por ejemplo, la siguiente información como resultado del análisis de riesgos:

- Probabilidad cualitativa (bajo, medio, alto, muy alto)

- Impacto cualitativo (bajo, medio, alto, muy alto)

- Impacto del costos (si aplica)

- Categorías de riesgos (bajo, medio, alto; Matriz)

- Probabilidad cuantitativa (%)

- Impacto cuantitativo ($)

- Valor esperado (si aplica)

Ejemplo de escala de probabilidad:

| Probabilidad de Ocurrencia | Nivel | Calificación |
|---|---|---|
| 0 - 25 | Baja | 1 |
| 26 - 70 | Media | 2 |
| 71 - 100 | Alta | 3 |

**Tabla 2.3.- Escala de Probabilidad**

Al igual que para determinar las escalas cualitativas, el diseño de las escalas cuantitativas debe contar con la participación de las personas encargadas de los procesos y con el grupo encargado de liderar la administración del riesgo.

### 2.6.1 Técnicas de valoración cuantitativas de riesgos

- *Análisis Costo-Beneficio.-* Es una herramienta que mide la relación entre los costos y beneficios asociados a un proyecto con el fin de evaluar su rentabilidad. El análisis coste-beneficio puede ser de ayuda para realizar juicios sobre si las medidas tomadas para la reducción de riesgos son o no factibles, es decir, si su coste no es desproporcionadamente grande frente a sus beneficios. Por ello todos los elementos o puntos positivos deberían situarse “en un lado de la balanza” y los negativos “en la otra parte de la balanza” para ver qué merece la pena.

- *Modelado y simulación.-* Las simulaciones utilizan un modelo de proyecto que traduce las incertidumbres específicas a un nivel detallado en impacto potencial sobre los objetivos a nivel de proyecto. Las simulaciones de proyecto utilizan modelos de computación y estimaciones de riesgo normalmente expresadas como una distribución de probabilidad de costo y duración posible a nivel detallado de trabajo. La técnica más utilizada suele ser el análisis Monte Carlo. La simulación utiliza una representación o modelo de un sistema para analizar el comportamiento esperado o rendimiento de un sistema. Para usar la simulación Monte Carlo se debe tener 3 estimaciones (muy probable, pesimista, optimista) más una estimación de la probabilidad de la estimación existente entre los valores más optimistas y probables. Los pasos a seguir son:

1. Valorar el rango de variables a considerar.
2. Determinar la probabilidad de distribución de cada variable.
3. Para cada variable seleccionar un valor aleatorio basándose en la distribución de probabilidad.
4. Ejecutar un análisis determinista.
5. Repetir los pasos 3 y 4 para obtener la distribución de probabilidad de los resultados.

- *Análisis de valor ganado.-* El análisis del valor monetario esperado es un concepto estadístico que calcula el resultado promedio cuando el futuro incluye escenarios que pueden ocurrir o no (es decir, análisis con incertidumbre). El valor monetario esperado de las oportunidades generalmente se expresará con valores positivos, mientras que el de los riesgos será negativo. El valor monetario esperado se calcula multiplicando el valor de cada posible resultado por su probabilidad de ocurrencia, y sumando los resultados. Este tipo de análisis se usa comúnmente en el análisis mediante árbol de decisiones. Se recomienda el uso del modelado y la simulación para el análisis de los riesgos de costos y del cronograma, porque son más efectivos y están menos sujetos a errores de aplicación que el análisis del valor monetario esperado.

- *Análisis de Sensibilidad.-* El análisis de sensibilidad ayuda a determinar qué riesgos tienen el mayor impacto posible sobre el proyecto. Este método examina la medida en que la incertidumbre de cada elemento del proyecto afecta al objetivo que está siendo examinado, cuando todos los demás elementos inciertos se mantienen en sus valores de línea base. Una representación típica del análisis de sensibilidad es el diagrama con forma de tornado, que es útil para comparar la importancia relativa de las variables que tienen un alto grado de incertidumbre con aquellas que son más estables.

- *Árboles de Decisión.-* Los árboles de decisión son útiles a la hora de seleccionar el mejor camino de acción cuando las salidas futuras son inciertas. El análisis mediante árbol de decisiones normalmente se estructura usando un diagrama de árbol de decisiones que describe una serie de posibles alternativas a elegir y las implicaciones de elegir unas u otras y los posibles escenarios. Incorpora el costo de cada opción disponible, las probabilidades de cada escenario posible y las recompensas de cada camino lógico alternativo. Es utilizado cuando escenarios futuros o salidas de acciones son inciertos. Incorpora probabilidades y los costos de cada camino lógico de eventos y futuras decisiones, y utiliza análisis de valor monetario esperado para ayudar a la organización a identificar los valores relativos de acciones alternativas.

## 2.7 Priorización de Riesgos

Aunque es importante identificar el mayor número posible de riesgos del proyecto, en muchos casos el número de riesgos identificados puede ser abrumador, y lógicamente el equipo de trabajo no podrá realizar un seguimiento ni una gestión efectiva de todos ellos. Una solución sería agrupar los riesgos en función de sus prioridades de tal forma que el equipo pueda centrarse en los más críticos.

La evaluación de la importancia de cada riesgo y, por consiguiente, de su prioridad, generalmente se realiza usando una matriz de probabilidad e impacto (matriz P-I). Esta matriz asignará categorías

a los riesgos basándose en la combinación de dichos factores (probabilidad e impacto) que llevan a la calificación de los riesgos como de prioridad baja, moderada o alta. Pueden usarse términos descriptivos o valores numéricos, dependiendo de la preferencia de la organización. Las reglas para calificar los riesgos pueden adaptarse al proyecto específico en el proceso planificación de la gestión de riesgos.

Una vez realizado el análisis de los riesgos con base en los aspectos de probabilidad e impacto, se recomienda utilizar la matriz de priorización que permite determinar cuáles requieren de un tratamiento inmediato**.**

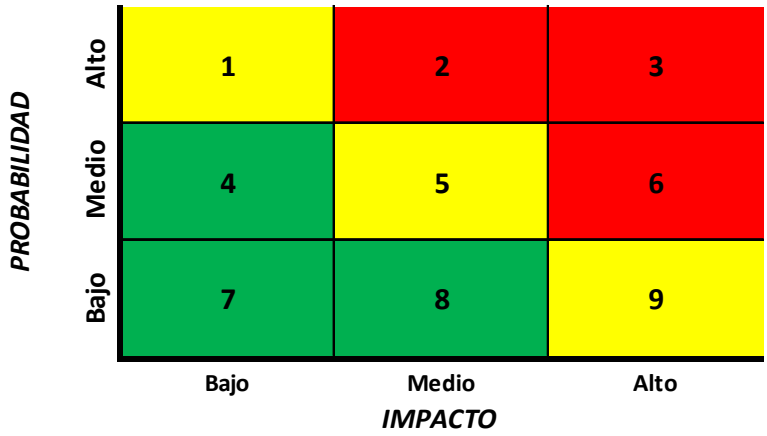


**Figura 3.7.- Matriz de Priorización de Riesgos**

Cuando se ubican los riesgos en la matriz se define cuáles de ellos requieren acciones inmediatas, que en este caso son los ubicados en los rectángulos 2, 3 y 6, los de **alto impacto y alta probabilidad.** Los que no requieren acciones inmediatas (pero desde luego requieren que se formulen) son los ubicados en los rectángulos 4, 7 y 8 que son los de **bajo impacto y baja probabilidad.** Respecto a los ubicados en las casillas 1, 5 y 9 es la entidad la que debe seleccionar de acuerdo a la naturaleza del riesgo cuáles va a trabajar primero, los de **alto impacto pero baja probabilidad** o los de **alta probabilidad y bajo impacto,** ya que estos pueden ser peligrosos para el logro de los objetivos institucionales, por las consecuencias que presenta en el caso de las casillas 5 y 9, o por lo constante de su presencia en el caso de la casilla 1.

En caso de que haya un número alto de riesgos dentro de la categoría 'Rojo', es recomendable priorizar dichos riesgos identificando los "n" riesgos más altos dentro de esta categoría, siendo este número determinado por la organización en función de su situación. Entre los indicadores de prioridad pueden incluirse:

- Las categorías determinadas para el riesgo
- El impacto de los riesgos identificados
- El número de riesgos
- El tipo de riesgos
- El tiempo para dar una respuesta a los riesgos

El resto de riesgos no seleccionados se deberán vigilar en la fase de monitorización y control ya que pueden cambiar su estado (aumente su probabilidad o cambie su impacto potencial).

## 2.8 Determinación del nivel de Riesgo

La determinación del nivel de riesgo es el resultado de confrontar el impacto y la probabilidad con los controles existentes al interior de los diferentes procesos y procedimientos que se realizan. Para adelantar esta etapa se deben tener muy claros los puntos de control existentes en los diferentes procesos, los cuales permiten obtener información para efectos de tomar decisiones, estos niveles de riesgo pueden ser:

- **ALTO:** Cuando el riesgo hace altamente vulnerable a la entidad o unidad. (Impacto y probabilidad alta vs controles)

- **MEDIO:** Cuando el riesgo presenta una vulnerabilidad media. (impacto alto – probabilidad baja o Impacto bajo – probabilidad alta vs controles).

- **BAJO:** Cuando el riesgo presenta vulnerabilidad baja. (Impacto y probabilidad baja vs controles).

Un ejemplo de la determinación del nivel del riesgo y del grado de exposición al mismo:

**Riesgo:** Perdida de información debido a la entrada de un virus en la red de información de la entidad.

**Probabilidad:** Alta, porque todos los computadores de la entidad están conectados a la red de Internet e intranet.

**Impacto:** Alto, porque la pérdida de información traería consecuencias graves para el quehacer de la entidad.

**Controles existentes**: la entidad tiene establecidos controles semanales haciendo backup o copias de seguridad y vacunando todos los programas y equipos; además guarda la información más relevante desconectada de la red en un centro de información.

**Resultado Nivel de riesgo:** Medio por los controles establecidos.

Lo anterior significa que a pesar de que la probabilidad y el impacto son altos confrontado con los controles, se puede afirmar que el nivel de riesgo es medio y por lo tanto las acciones que se implementen entrarán a reforzar los controles existentes y a valorar la efectividad de los mismos.

## 2.9 Manejo de Riesgos

Cualquier esfuerzo que emprendan las entidades en torno a la valoración del riesgo llega a ser en vano, si no culmina en un adecuado manejo y control de los mismos.

### 2.9.1 Consideración de Acciones

Para el manejo de los riesgos se deben analizar las posibles acciones a emprender las cuales deben ser factibles y efectivas, tales como: la implementación de políticas, definición de estándares, optimización de procesos y procedimientos y cambios físicos entre otros.

Se pueden tener en cuenta algunas de las siguientes opciones, las cuales pueden considerarse cada una de ellas independientemente, interrelacionadas o en conjunto.

**Evitar el riesgo:** es siempre la primera alternativa a considerar. Se logra cuando al interior de los procesos se genera cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas. Un ejemplo de esto puede ser el control de calidad, manejo de los insumos, mantenimiento preventivo de los equipos, desarrollo tecnológico, etc.

**Reducir el riesgo:** si el riesgo no puede ser evitado porque crea grandes dificultades operacionales, el siguiente paso es reducirlo al más bajo nivel posible. La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles. Se consigue mediante la optimización de los procedimientos y la implementación de controles. Ejemplo: Planes de contingencia.

**Dispersar y atomizar el riesgo:** Se logra mediante la distribución o localización del riesgo en diversos lugares. Es así como por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar.

**Transferir el riesgo:** Hace referencia a buscar respaldo y compartir con otro parte del riesgo como por ejemplo tomar pólizas de seguros, esta técnica es usada para eliminar el riesgo de un lugar y pasarlo a otro o de un grupo a otro. Así mismo, el riesgo puede ser minimizado compartiéndolo con otro grupo o dependencia.

**Asumir el riesgo:** Luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso el gerente del proceso simplemente acepta la pérdida residual probable y elabora planes de contingencia para su manejo.

Una vez establecidas cuales de las anteriores opciones de manejo del riesgo se van a concretar, estas deben evaluarse con relación al beneficio-costo para proceder a elaborar el mapa de riesgos, el cual permitirá visualizar todo el proceso de valoración, análisis y manejo de los riesgos.

## 2.10 Elaboración del Mapa de riesgos

Para la consolidación del Mapa de Riesgos, adicional a las consideraciones expuestas, es necesario identificar las causas que los pueden ocasionar, lo cual facilita el proceso de definición de acciones para mitigar los mismos.

La selección de las acciones más convenientes debe considerar la viabilidad jurídica, técnica, institucional, financiera y económica y se puede realizar con base en los siguientes factores:

a) El nivel del riesgo
b) El balance entre el costo de la implementación de cada acción contra el beneficio de la misma

Así mismo en el Mapa de Riesgos se deben identificar los controles existentes, las áreas o dependencias responsables de llevar a cabo las acciones, definir un cronograma y unos indicadores que permitan verificar el cumplimiento para tomar medidas correctivas cuando sea necesario.

| Riesgo | Impacto | Probabilidad | Control Existente | Nivel de Riesgo | Causas | Acciones | Responsables | Cronograma | Indicadores |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

**Figura 2.8.- Mapa de Riesgos**

***Descripción del Mapa de Riesgos***

**Riesgo:** posibilidad de ocurrencia de aquella situación que pueda entorpecer el normal desarrollo de las funciones de la entidad y le impidan el logro de sus objetivos.

**Impacto:** consecuencias que puede ocasionar a la organización la materialización del riesgo.

**Probabilidad:** entendida como la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de frecuencia o teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo aunque este no se haya presentado nunca.

**Control existente:** especificar cuál es el control que la entidad tiene implementado para combatir, minimizar o prevenir el riesgo.

**Nivel de riesgo:** El resultado de la aplicación de la escala escogida para determinar el nivel de riesgo de acuerdo a la posibilidad de ocurrencia, teniendo en cuenta los controles existentes.

**Causas:** Son los medios, circunstancias y agentes que generan los riesgos.

**Acciones:** es la aplicación concreta de las opciones del manejo del riesgo que entrarán a prevenir o a reducir el riesgo y harán parte del plan de manejo del riesgo.

**Responsables**: Son las dependencias o áreas encargadas de adelantar las acciones propuestas.

**Cronograma:** son las fechas establecidas para implementar las acciones por parte del grupo de trabajo.

**Indicadores:** se consignan los indicadores diseñados para evaluar el desarrollo de las acciones implementadas.

Finalmente, partiendo de que el fin último de la administración del riesgo es propender por el cumplimiento de la misión y objetivos institucionales, los cuales están consignados en la planeación anual de la entidad, se sugiere articular el mapa de riesgos con la planeación de manera que no sean planes aislados sino complementarios.

#### 2.10.1 Implementación de acciones

Definido el Mapa de Riesgos con sus acciones, responsables y cronogramas, es fundamental comenzar a ejecutar dichas acciones con el fin de determinar su efectividad en el menor tiempo posible.

## 2.11 Plan de respuesta a los riesgos

La planeación de la respuesta a los riesgos consiste en desarrollar procedimientos y técnicas que permitan mejorar las oportunidades y disminuir las amenazas que inciden en el proyecto. Esta suele ser la etapa más importante de todo el proceso de administración de riesgos, pues es aquí donde se toma la decisión de cómo responder a cada evento riesgoso identificado. La decisión que se adopte está en función de la calidad de la información disponible. También en función de la calidad del análisis de dicha información y de la creatividad del que tome la decisión.

Existen distintas estrategias de respuesta a los riesgos. Es importante seleccionar la más efectiva dentro de cada proyecto. Parar elegir la correcta, puede ser de ayuda el uso de herramientas de análisis de riesgos como por ejemplo el uso de árboles de decisiones.

Luego se desarrollan acciones específicas para implementar esa estrategia. Se pueden seleccionar estrategias principales y de refuerzo. También puede desarrollarse un plan de reserva, que será implementado si la estrategia seleccionada no resulta ser totalmente efectiva o si se produce un riesgo aceptado. A menudo, se asigna una reserva para contingencias de tiempo o coste. Finalmente, pueden desarrollarse planes para contingencias, junto con la identificación de las condiciones que disparan su ejecución.

#### 2.11.1 Estrategias para riesgos negativos o amenazas

Existen tres estrategias que normalmente se ocupan de las amenazas o los riesgos que pueden tener impactos negativos sobre los objetivos del proyecto en caso de ocurrir. Estas estrategias son evitar, transferir o mitigar.

- *Evitar.-* Evitar el riesgo implica cambiar el plan de gestión del proyecto para eliminar la amenaza que representa un riesgo adverso, aislar los objetivos del proyecto del impacto

del riesgo o disminuir el objetivo que está en peligro. Normalmente se elimina la causa del mismo (cambiando una situación), de tal forma que el riesgo no pueda afectar al proyecto. Ejemplos de este tipo de estrategia sería reducir el alcance para evitar ciertas actividades, añadir recursos, extender la programación o adoptar tecnología estable. Algunos riesgos que surgen en las etapas tempranas del proyecto pueden ser evitados aclarando los requisitos, obteniendo información, mejorando la comunicación o adquiriendo experiencia. Se trata de eliminar un riesgo específico, normalmente eliminando la causa del mismo (cambiando una situación) de tal forma que el riesgo no pueda afectar al proyecto. Ejemplos de este tipo de estrategia serían reducir el alcance para evitar ciertas actividades, añadir recursos, extender la programación o adoptar tecnología estable.

- *Transferir.-* Transferir el riesgo requiere trasladar el impacto negativo de una amenaza y la responsabilidad del mismo a un tercero para su gestión. No se elimina el riesgo, pero se minimizan las consecuencias para la empresa. Transferir la responsabilidad del riesgo es más efectivo cuando se trata de exposición a riesgos financieros. Transferir el riesgo casi siempre supone el pago de una prima de riesgo a la parte que toma el riesgo. Las herramientas de transferencia pueden ser bastante diversas e incluyen, entre otras, el uso de seguros, garantías de cumplimiento, certificados de garantía, etc. Pueden usarse contratos para transferir a un tercero la responsabilidad por riesgos especificados. En muchos casos, se puede usar un tipo de contrato de costes para transferir el riesgo de costos al comprador, mientras que un contrato de precio fijo puede transferir el riesgo al vendedor, si el diseño del proyecto es estable.

- *Mitigar.-* Mitigar el riesgo implica reducir la probabilidad y/o el impacto de un evento de riesgo adverso a un umbral aceptable. Adoptar acciones tempranas para reducir la probabilidad de la ocurrencia de un riesgo y/o su impacto sobre el proyecto a menudo es más efectivo que tratar de reparar el daño después de que ha ocurrido el riesgo. Normalmente esto requiere cambios en el plan del proyecto, como por ejemplo añadir actividades y recursos, adoptar procesos menos complejos, realizar más pruebas o seleccionar un proveedor más estable para tratar de forma proactiva el riesgo. Todos estos son ejemplos de acciones de mitigación (**plan de mitigación)**. Los costes asociados a los planes de respuesta con estrategias de mitigar, transferir y evitar deben ser incluidos en el presupuesto del proyecto, no en el presupuesto de reserva de riesgos ya que en estos casos se sabe qué costo y cuándo se acomete para responder a cada riesgo. Donde no es posible reducir la probabilidad, una respuesta de mitigación puede tratar el impacto del riesgo, dirigiéndose específicamente a los elementos que determinan su severidad. Por ejemplo, diseñando redundancia en un subsistema se puede reducir el impacto que resulta de un fallo del componente original.

### 2.11.2 Estrategias para riesgos positivos u oportunidades

Se sugieren tres respuestas para tratar los riesgos que tienen posibles impactos positivos sobre los objetivos del proyecto. Estas estrategias son explotar, compartir o mejorar.

- *Explotar.-* Se puede seleccionar esta estrategia para los riesgos con impactos positivos, cuando la organización desea asegurarse de que la oportunidad se haga realidad. Esta estrategia busca eliminar la incertidumbre asociada con un riesgo del lado positivo en particular haciendo que la oportunidad definitivamente se concrete. Explotar las respuestas directamente incluye asignar recursos más talentosos al proyecto para reducir el tiempo hasta la conclusión, o para ofrecer una mejor calidad que la planificada originalmente.

- *Compartir.-* Compartir un riesgo positivo implica asignar la propiedad a un tercero que está mejor capacitado para capturar la oportunidad para beneficio del proyecto. Entre los ejemplos de acciones para compartir se incluyen: formar asociaciones de riesgo conjunto, equipos, empresas con finalidades especiales o uniones temporales de empresas, que se pueden establecer con la finalidad expresa de gestionar oportunidades.

- *Mejorar.-* Esta estrategia modifica el "tamaño" de una oportunidad, aumentando la probabilidad y/o los impactos positivos, e identificando y maximizando las fuerzas impulsoras clave de estos riesgos de impacto positivo. Buscar facilitar o fortalecer la causa de la oportunidad, y dirigirse de forma proactiva a las condiciones que la disparan y reforzarlas, puede aumentar la probabilidad. También puede centrarse en las fuerzas impulsoras del impacto, buscando aumentar la susceptibilidad del proyecto a la oportunidad.

## 2.12 Control y Monitoreo del Riesgo

Una vez diseñado y validado el plan para administrar los riesgos, en el mapa de riesgos, es necesario monitorearlo teniendo en cuenta que estos nunca dejan de representar una amenaza para la organización.

El monitoreo es esencial para asegurar que las acciones se están llevando a cabo y evaluar la eficiencia en su implementación adelantando revisiones sobre la marcha para evidenciar todas aquellas situaciones o factores que pueden estar influyendo en la aplicación de las acciones preventivas.

El monitoreo debe estar a cargo de la Oficina de Control Interno y los responsables de las diferentes áreas y su finalidad principal será la de aplicar y sugerir los correctivos y ajustes necesarios para asegurar un efectivo manejo del riesgo. La Oficina de Control Interno dentro de su función asesora comunicará y presentará luego del monitoreo, sus resultados y propuestas de mejoramiento y tratamiento a las situaciones detectadas.

Los riesgos, su probabilidad de ocurrencia y su impacto están continuamente cambiando. Aparecen nuevos riesgos y los antiguos desaparecen. Implementar acciones de mitigación de riesgos puede crear nuevos riesgos no predecibles, o cambiar el efecto de riesgos ya existentes. Por lo tanto evaluar de forma periódica el plan es una actividad esencial, y las revisiones periódicas deberían ser especificadas en la programación del proyecto.

Los grandes hitos son puntos importantes en la gestión del proyecto. Ayudan a evaluar cómo va el proyecto y evaluar los cambios en el entorno. Cada vez que se propone un importante cambio en el proyecto y se aprueba su implementación, el equipo del proyecto debería estudiar cómo afectará este cambio al proyecto y determinar si se introducirán nuevos riesgos debidos al cambio. También será necesario desarrollar nuevas estrategias de respuestas a estos riesgos.

Otros disparadores que pueden provocar una evaluación de los riesgos son:

- Variación significativa en los costos respecto a lo esperado
- Inconsistencia en la programación/agenda respecto a lo esperado
- Cambios en las predicciones de fechas del proyecto
- Cambios en la actitud de los involucrados en el negocio
- Cualquier cambio durante el proyecto que amenace los objetivos del mismo.

Para realizar la valoración y actualización del registro de riesgos seguir los siguientes pasos:

- Revisar los planes de respuesta de los riesgos que han sido implementados para evaluar su efectividad y detectar la necesidad de tomar acciones correctivas.
- Revisar y actualizar la probabilidad, impacto, prioridad y el estado de los riesgos previamente identificados.
- Desarrollar nuevas estrategias de respuesta de riesgos o modificar las antiguas en caso de que la estrategia actual no funcione según lo previsto.
- Identificar nuevos riesgos residuales previamente filtrados, o aquellos riesgos con una categoría media o alta.
- Actualizar el plan del proyecto para que refleje cambios en los planes de respuesta de riesgos.
- Volver a analizar los riesgos residuales previamente filtrados, o aquellos riesgos con una categoría media o alta.
- Volver a evaluar la reserva de riesgos del proyecto para determinar si el buffer existente del proyecto es suficiente.
- Determinar si los umbrales y disparadores establecidos se han modificado (aumentaron) o si el plan de reserva de riesgos es probable que sea sobrepasado.

Una buena práctica sería documentar los esfuerzos de respuesta de riesgos en el registro de riesgos para generar un histórico de las acciones y resultados obtenidos. De esta manera los jefes de proyecto pueden aprender de experiencias pasadas, como por ejemplo, podrán conocer qué estrategias y acciones llevadas a cabo funcionaron y cuáles no. La documentación de la gestión de riesgos (plan de gestión de riesgos, registro de riesgos y herramientas asociadas) debería desarrollarse de la forma más simple posible, a la vez que debe ser completa, exacta y estar actualizada.

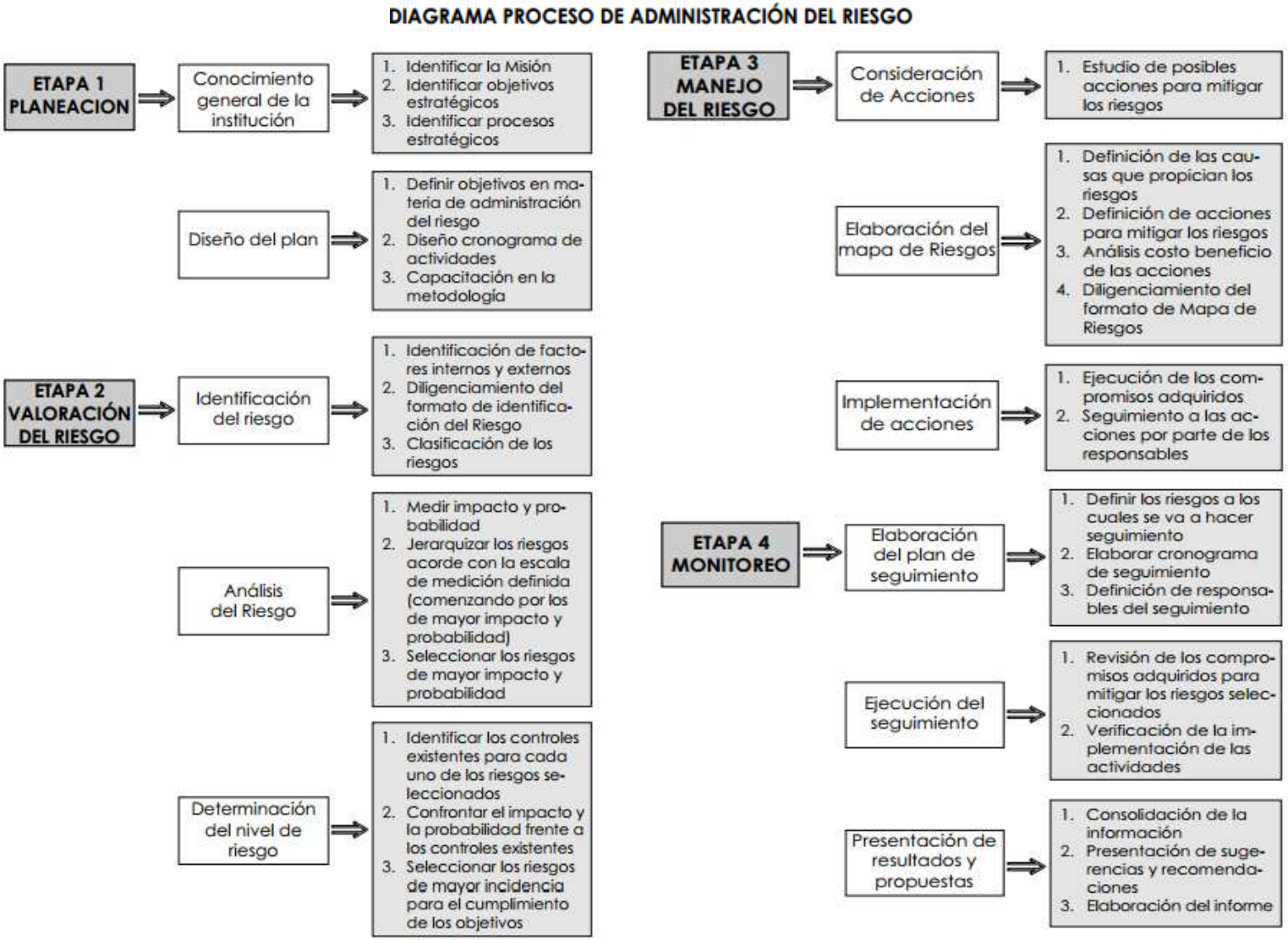


**Figura 2.9.- Diagrama Proceso de Administración de Riesgos**

# 3. Ley General de Protección Civil

La ley General de Protección Civil (LGPC) vigente a la fecha, cuenta con siete capítulos y 40 artículos, es de orden público e interés social y tiene por objeto establecer las bases de coordinación entre los tres órdenes de gobierno en materia de protección civil.

## 3.1 Disposiciones Generales

La LGPC define como **Protección Civil** al conjunto de disposiciones, medidas y acciones destinadas a las prevención, auxilio y recuperación de la población ante la eventualidad de un desastre. Así mismo también define como **Agentes Destructivos** a los fenómenos de carácter geológico, hidrometeorológico, químico-tecnológico, sanitario-ecológico y socio-organizativo que pueda producir riesgo, emergencia o desastre.

**Continuidad de Operaciones:** Al proceso de planeación, documentación y actuación que garantiza que las actividades sustantivas de las instituciones públicas, privadas y sociales, afectadas por un agente perturbador, puedan recuperarse y regresar a la normalidad en un tiempo mínimo. Esta planeación deberá estar contenida en un documento o serie de documentos cuyo contenido se dirija hacia la prevención, respuesta inmediata y restauración, todas ellas avaladas por sesiones de capacitación continua y realización de simulacros.

**Desastre:** Al resultado de la ocurrencia de uno o más agentes perturbadores severos y/o extremos, concatenados o no, de origen natural o de la actividad humana, que cuando acontecen en un tiempo y en una zona determinada, causan daños y que por su magnitud exceden la capacidad de respuesta de la comunidad afectada.

**Emergencia: S**ituación anormal que puede causar un daño a la sociedad y propiciar un riesgo excesivo para la seguridad e integridad de la población en general, generada o asociada con inminencia, alta probabilidad o presencia de un agente perturbador.

**Fenómeno Antropogénico:** Agente perturbador producido por la actividad humana.

**Fenómeno Natural Perturbador:** Agente perturbador producido por la naturaleza.

**Fenómeno Geológico**: Calamidad que tiene como causa las acciones y movimientos violentos de la corteza terrestre. A esta categoría pertenecen los sismos o terremotos, las erupciones volcánicas, los tsunamis o maremotos y la inestabilidad de suelos, también conocida como movimientos de tierra, los que pueden adoptar diferentes formas: arrastre lento o reptación, deslizamiento, flujo o corriente, avalancha o alud, derrumbe y hundimiento.

**Fenómeno Hidrometeorológico:** Calamidad que se genera por la acción violenta de los agentes atmosféricos, tales como: huracanes, inundaciones pluviales, fluviales, costeras y lacustres; tormentas de nieve, granizo, polvo y electricidad; heladas; sequías y las ondas cálidas y gélidas.

**Fenómeno Químico-Tecnológico:** Calamidad que se genera por la acción violenta de diferentes sustancias derivadas de su interacción molecular o nuclear. Comprende fenómenos destructivos tales como: incendios de todo tipo, explosiones, fugas tóxicas y radiaciones.

**Fenómeno Sanitario-Ecológico:** Calamidad que se genera por la acción patógena de agentes biológicos que atacan a la población, a los animales y a las cosechas, causando su muerte o la alteración de su salud. Las epidemias o plagas constituyen un desastre sanitario en el sentido estricto del término. En esta clasificación también se ubica la contaminación del aire, agua, suelo y alimentos.

**Fenómeno Socio-Organizativo:** Calamidad generada por motivo de errores humanos o por acciones **premeditadas**, que se dan en el marco de grandes concentraciones o movimientos masivos de población.

**Identificación de Riesgos:** Reconocer y valorar las pérdidas o daños probables sobre los agentes afectables y su distribución geográfica, a través del análisis de los peligros y la vulnerabilidad.

**Instrumentos de administración y transferencia de riesgos:** Son aquellos programas o mecanismos financieros que permiten a las entidades públicas, compartir o cubrir sus riesgos catastróficos, transfiriendo el coso total o parcial a instituciones financieras nacionales o internacionales.

**Mitigación:** Es toda acción orientada a disminuir el impacto a daños ante la presencia de una agente perturbador sobre un agente afectable.

**Peligro:** Probabilidad de ocurrencia de un agente perturbador potencialmente dañino de cierta intensidad, durante un cierto período y en un sitio determinado.

**Riesgo:** Daños o pérdidas probables sobre un agente afectable, resultado de la interacción entre su vulnerabilidad y la presencia de un agente perturbador.

La LGPC establece que corresponde al Ejecutivo Federal dictar los lineamientos generales para inducir y conducir las labores de protección civil, a fin de lograr la participación de los diferentes sectores y grupos de la sociedad. Así como, incluir r en el proyecto de Presupuesto de Egresos de la Federación, el Fondo de Desastres y el Fondo para la Prevención de Desastres, estableciendo los montos para la operación de cada uno de ellos.

## 3.2 Del Sistema Nacional

El Sistema Nacional de Protección Civil es un conjunto orgánico y articulado de estructuras, relaciones funcionales, métodos y procedimientos que establecen las dependencias y entidades del sector público entre sí, con las organizaciones de los diversos grupos voluntarios, sociales, privados y con las autoridades de los estados, el Distrito Federal y los municipios, a fin de efectuar acciones coordinadas, destinadas a la protección contra los peligros que se presenten y a la recuperación de la población, en la eventualidad de un desastre.

El objetivo del Sistema Nacional es el de proteger a la persona y a la sociedad ante la eventualidad de un desastre, provocado por agentes naturales o humanos, a través de acciones que reduzcan o eliminen la pérdida de vidas, la afectación de la planta productiva, la destrucción de bienes materiales, el daño a la naturaleza y la interrupción de las funciones esenciales de la sociedad, así

como el de procurar la recuperación de la población y su entorno a las condiciones de vida que tenían antes del desastre.

El Sistema Nacional se encuentra integrado por el Presidente de la República, por el Consejo Nacional, por las Dependencias, Organismos e Instituciones de la Administración Pública Federal, por el Centro Nacional de Prevención de Desastres, por los grupos voluntarios, vecinales y no-gubernamentales, y por los sistemas de protección civil de las entidades federativas, del Distrito Federal y de los municipios. La coordinación ejecutiva del Sistema Nacional recaerá en la Secretaría de Gobernación.

En una situación de emergencia, el auxilio a la población debe constituirse en una función prioritaria de la protección civil, por lo que las instancias de coordinación deberán actuar en forma conjunta y ordenada, en los términos de esta Ley y de las demás disposiciones aplicables.

Con la finalidad de iniciar las actividades de auxilio en caso de emergencia, la primera autoridad que tome conocimiento de ésta, deberá proceder a la inmediata prestación de ayuda e informar tan pronto como sea posible a las instancias especializadas de protección civil.

La primera instancia de actuación especializada, corresponde a la autoridad municipal o delegacional que conozca de la situación de emergencia. En caso de que ésta supere su capacidad de respuesta, acudirá a la instancia estatal correspondiente, en los términos de la legislación aplicable.

## 3.3 Del Consejo Nacional

El Consejo Nacional de Protección Civil es un órgano consultivo en materia de planeación de la protección civil. Entre sus atribuciones se encuentran las siguientes:

- Fungir como órgano de consulta y de coordinación de acciones del Gobierno Federal para convocar, concertar, inducir e integrar las actividades de los diversos participantes e interesados en la materia, a fin de garantizar la consecución del objetivo del Sistema Nacional;

- Fomentar la participación comprometida y corresponsable de todos los sectores de la sociedad, en la formulación y ejecución de los programas destinados a satisfacer las necesidades de protección civil en el territorio nacional;

- Promover el estudio, la investigación y la capacitación en materia de protección civil, identificando sus problemas y tendencias, y proponiendo las normas y programas que permitan su solución, así como la ampliación del conocimiento sobre los elementos básicos del Sistema Nacional y el fortalecimiento de su estructura;

El Consejo Nacional estará integrado por el Presidente de la República, quien lo presidirá y por los titulares de las Secretarías de Gobernación; Relaciones Exteriores; Defensa Nacional; Marina; Hacienda y Crédito Público; Desarrollo Social; Medio Ambiente y Recursos Naturales; Energía; Agricultura, Ganadería, Desarrollo Rural, Pesca y Alimentación; Comunicaciones y Transportes; Función Pública; Educación Pública; Salud; por los Gobernadores de los Estados y del Jefe de

Gobierno del Distrito Federal. Cada titular designará un suplente, siendo para el caso de los Secretarios un Subsecretario; para los Gobernadores y Jefe de Gobierno del Distrito Federal, el Secretario General de Gobierno. En el caso del Secretario de Gobernación, lo suplirá el Coordinador General de Protección Civil.

## 3.4 De los Grupos Voluntarios

Se reconoce como grupos voluntarios a las instituciones, organizaciones y asociaciones municipales, estatales, regionales y nacionales que obtengan su registro ante la instancia correspondiente. Los grupos voluntarios de carácter regional y nacional tramitarán su registro ante la Secretaría de Gobernación; los estatales y municipales según lo establezca la legislación local respectiva.

Todo grupo voluntario debe disponer del reconocimiento oficial una vez obtenido su registro, y que éste se haya publicado en el Diario Oficial de la Federación; y se deben considerar a sus programas de capacitación y adiestramiento como parte del Programa Nacional; así como están obligados a comunicar a las autoridades de protección civil la presencia de una situación de probable o inminente riesgo y coordinarse bajo el mando de las autoridades en caso de un riesgo, emergencia o desastre.

## 3.5 Del Programa Nacional

El Programa Nacional es el conjunto de objetivos, políticas, estrategias, líneas de acción y metas para cumplir con el objetivo del Sistema Nacional, según lo dispuesto por la Ley de Planeación. **.-** Los programas estatales y municipales de protección civil deberán elaborarse, de conformidad con las líneas generales que establezca el Programa Nacional. Se podrán elaborar programas especiales de protección civil cuando:

- Se identifiquen riesgos específicos que puedan afectar de manera grave a la población, y
- Se trate de grupos específicos, como personas minusválidas, de tercera edad, jóvenes, menores de edad y grupos étnicos.

## 3.6 De las Declaratorias de Emergencia y de Desastre

Le competerá a la Federación, sin perjuicio de lo que en términos de las disposiciones locales les corresponda realizar a las entidades federativas y municipios, lo siguiente:

**I.** Realizar las acciones de emergencia para dar atención a las necesidades prioritarias de la población, particularmente en materia de protección a la vida, salud, alimentación, atención médica, vestido, albergue temporal, el restablecimiento de las vías de comunicación que impliquen facilitar el movimiento de personas y bienes, incluyendo la limpieza inmediata y urgente de escombros y derrumbes en calles, caminos, carreteras y accesos, así como para la reanudación del servicio eléctrico y el abastecimiento de agua;

**II.** Consolidar, reestructurar, o en su caso, reconstruir los monumentos arqueológicos y los inmuebles artísticos e históricos que tengan acuerdo de destino, se encuentren bajo custodia de ésta o dedicados al culto público, de conformidad con las leyes y demás disposiciones de la materia, y

**III.** Destinar recursos del Fondo de Desastres autorizado para la atención de emergencias y desastres, en la realización de acciones preventivas, ante circunstancias que valorarán los órganos administrativos correspondientes que se deriven de lo dispuesto en el primer párrafo del artículo 32 de este ordenamiento; y

**IV.** Las demás que determinen las leyes, reglamentos y otras disposiciones administrativas.

Ante la inminencia o alta probabilidad de que ocurra un desastre que ponga en riesgo la vida humana, y cuando la rapidez de la actuación del Sistema Nacional de Protección Civil sea esencial, la Secretaría de Gobernación podrá emitir una declaratoria de emergencia, la cual se divulgará a través de los medios masivos de comunicación.

Una vez realizada la declaratoria de emergencia, la Secretaría de Gobernación deberá erogar, con cargo al Fondo Revolvente asignado, los montos que a juicio de dicha Secretaría se consideren suficientes para atenuar los efectos del posible desastre, así como para responder en forma inmediata a las necesidades urgentes generadas por el mismo.

La declaratoria de desastre es el acto mediante el cual la Secretaría de Gobernación, reconoce que uno o varios fenómenos perturbadores han causado daños severos cuya atención rebase las capacidades locales.

Las solicitudes de declaratoria de desastre podrán realizarse a través de:

**I.** Los gobiernos de las entidades federativas cuando la atención de los daños causados por el desastre rebase su capacidad operativa y financiera, y

**II.** Las dependencias o entidades federales.

Las disposiciones administrativas establecerán los procedimientos y demás requisitos para la emisión de las declaratorias de emergencia y de desastre, así como del acceso a recursos para la realización de las acciones preventivas previstas en el presente Capítulo, atendiendo al principio de inmediatez.

## 3.7 De las Medidas de Seguridad

En caso de riesgo inminente, sin perjuicio de la emisión de la declaratoria de emergencia y de lo que establezcan otras disposiciones, las dependencias y entidades de la Administración Pública Federal, Estatal y Municipal ejecutarán las medidas de seguridad que les competan, a fin de proteger la vida de la población y sus bienes, la planta productiva y el medio ambiente, para garantizar el funcionamiento de los servicios esenciales de la comunidad.

Las Unidades Estatales o Municipales de Protección Civil, así como las del Distrito Federal, podrán aplicar las siguientes medidas de seguridad:

**I.** Identificación y delimitación de lugares o zonas de riesgo;

**II.** Acciones preventivas para la movilización precautoria de la población y su instalación y atención en refugios temporales, y

**III.** Las demás que en materia de protección civil determinen las disposiciones reglamentarias y la legislación local correspondiente, tendientes a evitar que se generen o sigan causando riesgos.

Cuando se apliquen alguna o algunas de las medidas de seguridad previstas anteriormente, se indicará su temporalidad y, en su caso, las acciones que se deben llevar a cabo para ordenar el retiro de las mismas.

# 4. Funciones Críticas y Procedimientos Operacionales

Una de las tareas de planeación más complejas dentro de una organización es la solución a problemas. “La solución de problemas puede definirse como el proceso de identificar una diferencia entre el estado actual de las cosas y el estado deseado y luego emprender una acción para reducir o eliminar la diferencia (Anderson, 2004)”.

Para poder realizar con éxito esta actividad, la organización debe contar con capacitación y estar preparada, además de contar con herramientas que faciliten y agilicen este procedimiento. Solucionar problemas es una parte fundamental en una empresa u organización y el hacerlo correctamente puede evitar que se entre en una crisis de la cual el costo de tiempo, recursos e inclusive la reputación puede afectar gravemente a la organización.

Para poder resolver problemas relacionados con las funciones de la organización de manera satisfactoria será necesario en primer lugar, identificar las funciones críticas de la organización y una vez definidas se podrán establecer procedimientos operacionales cuyo objetivo sea en primer lugar, evitar que haya alguna interrupción de dichas funciones, en segundo lugar, si existe alguna interrupción, poder restablecerla exitosamente en la brevedad posible.

## 4.1 Funciones

Una organización y/o empresa puede ser visualizada como un conjunto de unidades de las cuales cada una cumple con una función, para que en conjunto toda la empresa realice una o varias funciones. Las funciones pueden ser repartidas entre diferentes actividades y se busca que el departamento al cual se le asignan sea el más calificado para realizar estas.

Las funciones que se realizan en una organización o empresa son principalmente:

- Función Técnica.- Es la función central y el propósito general de toda empresa u organización. La función técnica define que es lo que se va a producir o vender, según sea el caso.
- Función Financiera.- Es la función que se encarga de administrar los recursos financieros de la organización.
- Función Contable.- Es la función que se encarga de llevar las cuentas administrativas de la organización.
- Función Social.- Es la función que administra los recurso humanos de la organización.
- Función Comercial.- Es la función encargada de comercializar el producto.
- Función Administrativa.- Es la función encargada de administrar a cada una de las unidades en el cumplimiento de sus funciones.

Cada departamento es, por lo general, responsable de realizar unas determinadas funciones de la organización y/o negocio. Estas deben ser definidas a nivel genérico, sin entrar en detalle de actividades necesarias para realizarlas.

A modo de ejemplo, no limitativo, se puede citar las siguientes:

| Departamentos | Funciones típicas |
|---|---|
| Comercial | Ventas y marketing |
| | Gestión de pedidos |
| | Servicio post-venta |
| Financiero | Contabilidad |
| | Facturación |
| | Gestión de Tesorería |
| Recursos Humanos | Nóminas |
| | Administración del personal |
| Seguridad | Control de accesos |
| Servicios generales | Comunicaciones de voz |
| | Correo interno |

**Tabla 5.1.- Funciones Típicas por Departamentos**

Aún siendo todas ellas necesarias para la consecución de los objetivos de la organización, algunas de estas funciones se considerarán críticas en función del impacto que sufriría la organización si se produjera una interrupción significativa de las mismas.

### 4.1.1 Tipos de funciones

**Críticas**

- ✓ Funciones que pueden realizarse sólo si las capacidades se reemplazan por otras idénticas.
- ✓ No pueden reemplazarse por métodos manuales.
- ✓ Muy baja tolerancia a interrupciones.

**Vitales**

- ✓ Pueden realizarse manualmente por un período breve.
- ✓ Costo de interrupción un poco más bajos, sólo si son restaurados dentro de un tiempo determinado (5 o menos días, por ejemplo).

**Sensitivos**

- ✓ Funciones que pueden realizarse manualmente por un período prolongado a un costo tolerable.
- ✓ El proceso manual puede ser complicado y requeriría de personal adicional.

**No críticos**

- ✓ Funciones que pueden interrumpirse por tiempos prolongados a un costo pequeño o nulo.

## 4.2 ¿Qué es un procedimiento?

Los Procedimientos Operativos son documentos que recogen la interrelación en el tiempo que existen entre diferentes departamentos, normalizando los procedimientos de actuación y evitando las indefiniciones e improvisaciones que pueden producir problemas o deficiencias en la realización del trabajo.

Los Procedimientos Operativos son complementarios del Manual de Calidad y describen con detalle **cómo**, **quién**, **cuándo**, **dónde**, se realizan las actividades definidas en el Manual de Calidad. El Manual de Calidad debe hacer referencia a los Procedimientos.

Los procedimientos aseguran:

1. Que las actividades se realizan de una forma independiente de la persona responsable de llevarlas a cabo.

2. Que se realizan de una forma ordenada y sin improvisaciones.

3. Que conducen al objetivo cubierto por el procedimiento.

## 4.3 ¿Qué son las instrucciones de trabajo?

Las instrucciones de trabajo son documentos que recogen cómo deben desarrollarse cada una de las tareas indicadas en los procedimientos. A diferencia de los Procedimientos Operativos, Las instrucciones únicamente afectan a una unidad funcional.

### 4.3.1 Ventajas de redactar Procedimientos Operativo s e Instrucciones de Trabajo

- **Facilita la comprensión** de los procedimientos operativos, evitando la redacción de procedimientos demasiado extensos que pudieran entorpecer la comprensión del documento.

- **Facilita la gestión de la documentación**, reduciendo el número de documentos a editar. En efecto, si fuere necesario realizar algún cambio que afectase a una instrucción existente, bastaría con emitir una nueva revisión de la Instrucción, sin tener que modificar el procedimiento como tal. Si no existiere la Instrucción de forma separada del Procedimiento, por más pequeño que fuese el cambio a realizar, se debería de emitir una nueva revisión del procedimiento completo, con todo el problema que ello acarrea, para la administración de la documentación del sistema.

- **Disminuye la toma de decisiones,** y con esto reduce la probabilidad de errores durante la ejecución del proceso.

## 4.4 Fases en la elaboración de Procedimientos

La elaboración de un procedimiento se puede dividir en las siguientes fases:

- **Fase de Elaboración del borrador:** El gestor de calidad junto con las personas designadas para la elaboración de procedimiento, realizan un primer borrador del documento que será la recisión cero.

- **Fase de lanzamiento:** El borrador redactado en la fase anterior, se distribuye a todas las personas afectadas por el mismo para que puedan sugerir modificaciones que mejoren la comprensión del procedimiento – La fase de lanzamiento finaliza con la redacción definitiva, en base al borrador y las sugerencias recibidas.

- **Fase de Aprobación:** Antes de su distribución, el documento debe ser aprobado por la persona responsable previamente asignada. Normalmente se designa a la Dirección para la aprobación de los documentos de primer nivel (Manual de Calidad), al equipo directivo (Jefe de uso público) para los documentos de nivel dos (Procedimientos) y los mando intermedios, para los de nivel tres. Es decir, un estamento superior al encargado de la redacción.

- **Fase de Distribución:** Una vez aprobado, el documento debe ser distribuido de forma controlada a las personas o departamentos implicados, conservando un registro de su distribución para asegurar que siempre se mantiene la última versión vigente.

- **Fase de Revisión:** La revisión de los documentos puede ser puesta en marcha tanto a solicitud de un empleado como de un cliente, para mejorar algún aspecto de los mismos. En este caso, se seguirán las fases anteriores expuestas.

## 4.5 Redacción de los Procedimientos

En la redacción de la documentación del Sistema de Calidad se debe buscar la implicación de todo el personal de la organización. De esta forma, se conseguirá un sentido de pertenencia de todos los empleados hacia el Sistema de Calidad y lograremos que el sistema sea más eficaz al ser elaborado en base a mayor información.

Los procedimientos deben ser redactados por las personas implicadas en el desarrollo de los procesos, pues serán quienes mejores conozcan las tareas que día a día se llevan a cabo para el cumplimiento de los objetivos.

El gestor de la calidad debe liderar la redacción de la documentación del Sistema de Calidad, identificando que procedimientos e instrucciones deben ser redactados, la persona responsable de la redacción y el plazo asignado para ello.

Los procedimientos operativos hacen referencia a la organización de los procesos y en su redacción deben colaborar los mandos intermedios (jefes de área, responsables de departamentos) o equipos interdepartamentales.

Es importante que los procedimientos sean escritos pensando en el destinatario. Los detalles excesivos y el uso de terminología no familiar pueden afectar adversamente la implantación, efectividad y eficacia del sistema de calidad. Los procedimientos mal diseñados son fuente común de frustraciones y pueden desprestigiar el sistema entero.

A continuación se ofrecen algunas recomendaciones generales para la redacción de los procedimientos:

- Evitar términos ambiguos.
- Escribir las frases en presente y en orden cronológico.
- Ser exacto.
- Plantear los objetivos que se pretenden cubrir con el procedimiento y una vez redactado, comprobar que el documento los cumple.
- Utilizar diagramas de flujo, que permitan obtener una visión global del procedimiento.

# 5. Plan de Continuidad de Negocios y Plan de Recuperación de Desastres

## 5.1 ¿Qué es un Plan de Continuidad del Negocio?

También conocido como BCP por sus siglas en inglés (Business Continuity Plan), según la NFPA es un proceso continuo que con el apoyo de la alta dirección y los fondos para asegurar los pasos necesarios para identificar el impacto de las pérdidas potenciales, mantener estrategias viables de recuperación, planes de recuperación y continuidad de los servicios. Es un plan documentado y probado con el fin de responder ante una emergencia de manera adecuada, logrando así el mínimo impacto a la operación del negocio.

Un Plan de Continuidad de Negocio se compone de varias fases que comienzan con un análisis de los procesos que componen la organización. Este análisis servirá para priorizar qué procesos son críticos para el negocio y establecer una política de recuperación ante un desastre. Por cada proceso se identifican los impactos potenciales que amenazan la organización, estableciendo un plan que permita continuar con la actividad empresarial en caso de una interrupción.

Un Plan de Continuidad de Negocio, a diferencia de una Plan de Contingencia, está orientado al mantenimiento del negocio de la organización, con lo que priorizará las ***operaciones críticas de negocio*** necesarias para continuar en funcionamiento después de un incidente no planificado.

En el desarrollo de un Plan de Continuidad de Negocio existen dos preguntas clave:

• ¿Cuáles son los ***recursos*** relacionados con los procesos críticos del negocio de la compañía?

• ¿Cuál es el período de ***tiempo de recuperación crítico*** para los recursos de información en el cual se debe establecer el procesamiento del negocio antes de que se experimenten pérdidas significativas o aceptables?

Un Plan de Continuidad reducirá el número y la magnitud de las decisiones que se toman durante un período en que los errores pueden resultar mayores. El Plan establecerá, organizará y documentará los riesgos, responsabilidades, políticas y procedimientos, acuerdos con entidades internas y externas.

La activación de un Plan de Continuidad debería producirse solamente en situaciones de emergencia y *cuando las medidas de seguridad hayan fallado.*

### 5.1.1 BENEFICIOS

- Identifica los diversos eventos que podrían impactar sobre la continuidad de las operaciones y su impacto financiero, humano y de reputación sobre la organización.
- Obliga a conocer los tiempos críticos de recuperación para volver a la situación anterior al desastre sin comprometer al negocio.
- Previene o minimiza las pérdidas para el negocio en caso de desastre.
- Clasifica los activos para priorizar su protección en caso de desastre.
- Aporta una ventaja competitiva frente a la competencia.

- Fomenta e implica a los recursos humanos de la compañía en las actividades de continuidad.

El propósito general de un Plan de Continuidad es obtener un mapa de acciones que reduzcan "la toma de decisiones" durante las operaciones de recuperación, restaure los servicios críticos rápidamente y permita un normal funcionamiento de los sistemas y procesos lo antes posible, minimizando costes y aumentando la efectividad.

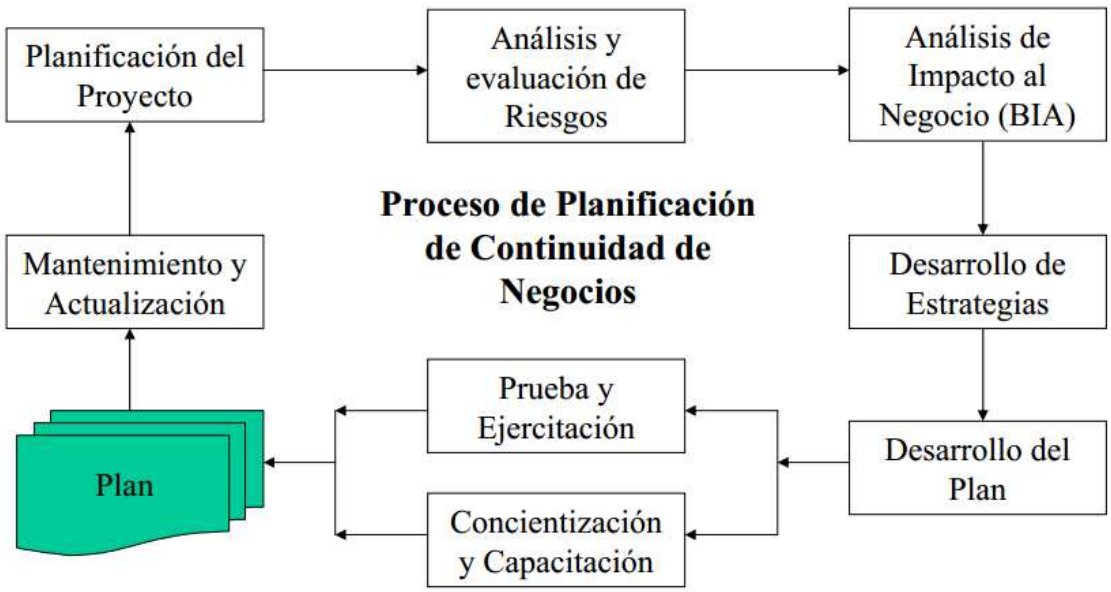


**Figura 5.1.- Metodología del BCP**

### 5.1.2 OBJETIVOS:

Un plan de Continuidad de Negocios debería hacer frente a estos objetivos específicos:

- Aumentar la probabilidad de continuidad de las funciones críticas de la organización en caso de que un incidente interrumpa las operaciones.
- Proporcionar un enfoque organizado y consolidado para dirigir actividades de respuesta y recuperación ante cualquier incidente o interrupción de trabajo imprevista, evitando confusión y reduciendo la situación de tensión.
- Proporcionar una respuesta rápida y apropiada a cualquier incidente imprevisto, reduciendo así los impactos resultantes de interrupciones de trabajo a corto plazo.
- Recuperar las funciones críticas de negocio de manera oportuna, aumentando la capacidad de la organización para recuperarlas ante un incidente que haya dejado las instalaciones dañadas o destruidas.
- Aumentar la probabilidad de continuidad del servicio de la organización en caso de que un incidente interrumpa sus operaciones normales.

- Reducir el tiempo de recuperación, y como consecuencia, las pérdidas económicas, directas e inducidas, como resultado de un desastre.
- Reducir el impacto, tangible o intangible, en las áreas funcionales como consecuencia de una interrupción del servicio.
- Realizar la recuperación de las funciones críticas, mediante el desarrollo de los procedimientos necesarios para:
  - reducir la duración de la recuperación;
  - minimizar el coste de la recuperación;
  - evitar la confusión y reducir el riesgo de errores:
  - evitar la duplicación de esfuerzos.

### 5.1.3 ALCANCE DEL PLAN

El Plan de Continuidad de Negocio debe ser diseñado para crear una situación de preparación que proporcione una respuesta inmediata diseñada en función de una serie de posibles escenarios previamente definidos.

En primer lugar, será preciso definir qué departamentos, dependencias, instalaciones, etc., van a ser incluidas en el plan. No es lo mismo desarrollar un Plan de Contingencia que abarque solamente la recuperación y continuidad de las actividades que un Plan de Continuidad de Negocio que considere todas las funciones críticas de la organización.

Después, será preciso elegir, entre todo el catálogo de posibles amenazas, cuáles de ellas son más probables y descartar aquellas que, aun siendo posibles, su probabilidad de ocurrencia es mucho menor. Aquí juega un papel muy importante el presupuesto disponible para la implementación del plan. La consideración de algunas amenazas puede entrañar la necesidad de implementación de medidas que supongan unos costos importantes. Es decir, a la hora de definir el alcance del plan se debe tener muy en cuenta las limitaciones presupuestarias y dimensionar el mismo de acuerdo con esas limitaciones. Cada uno de los supuestos elegidos puede requerir soluciones muy diferentes en su diseño y costo. Por otra parte, como muchas otras que habrá que tomar a lo largo del desarrollo e implementación, la decisión del alcance del plan debe estar aprobada por la dirección.

### 5.1.4 CONDICIONES INICIALES

Aparte de la definición del alcance del plan, es preciso definir y acotar una serie de supuestos sobre los cuales basar todas actuaciones en las que se fundamenta el plan. La posibilidad de aplicación de las medidas planificadas puede depender de múltiples factores externos. En la medida que esos factores se comporten de una u otra forma, las medidas previstas serán aplicables o no. Conviene pues, enumerar esos supuestos para, si la dirección considera que son excesivamente optimistas o pesimistas, corregir el plan a la baja o al alza, ya que ello repercutirá, como siempre, no sólo en el coste de las medidas a implantar sino en una mayor o menor índica de cobertura.

**Alcance del plan**

1. El plan abarca las siguientes instalaciones... (oficinas centrales, sucursales, centro de proceso de datos, informática distribuida, etc.) y las siguientes áreas funcionales... (financiero, comercial, RR HH, fabricación, etc.).
2. Se consideran los siguientes tipos de incidentes:
   - Los que causen un daño físico en las instalaciones o equipos, como fuego, humo o daños por agua.
   - Los que afecten de forma indirecta la posibilidad de acceso a las instalaciones, como evacuación de emergencia por amenaza de bomba, o amenazas externas tales como incendios en instalaciones cercanas, fuga de gases tóxicos, etc.
   - Desastres regionales no previstos o inesperados, tales como huracanes o inundaciones, que puedan causar daños en las instalaciones y equipos.
   - Desastres regionales no previstos o inesperados, que puedan impedir el acceso normal al personal encargado de las operaciones informáticas, aunque las instalaciones estén intactas, tales como grandes nevadas, inundaciones, etc.
   - Cualquier incidente externo que pudiera potencialmente causar una interrupción de las operaciones del negocio, tales como la pérdida de los servicios de suministro eléctrico o de telecomunicaciones.
   - Cualquier incidente que afecte al funcionamiento del hardware o del software y que suponga una interrupción superior a las 24 horas.
   - Cualquier incidente que suponga la paralización de actividades de la organización por motivos ajenos a la tecnología, tales como problemas laborales propios o del sector o problemas laborales que afecten al área geográfica donde se encuentra ubicada la organización.
   - ..... (*)
3. Se descartan los siguientes tipos de incidentes:
   - ..... (**)

(*) Ejemplos genéricos. Sustituir por datos potencialmente probables.
(**) Relacionar aquí las amenazas descartadas y razones para ello (probabilidad o coste)

| Preparado por: | Conforme: | Aprobado por: |
|---|---|---|
| Fecha: | Fecha: | Fecha: |

**Figura 5.2.- Ejemplo de Formulario para Alcance del Plan**

**Condiciones Iniciales**

El Plan se ha desarrollado sobre los siguientes supuestos:

- Sólo el área habitual de trabajo ha sido afectada por el incidente; todos los lugares alternativos predesignados están intactos.
- Los almacenes externos de archivos críticos de backup e información están intactos y accesibles.
- El personal cualificado en cantidad suficiente (identificado en los capítulos correspondientes) está disponible para realizar los trabajos de recuperación.
- Los trabajos de recuperación se están realizando de acuerdo con los procedimientos que han sido descritos en el Plan de Continuidad del Negocio.
- Las copias de seguridad y su correspondiente rotación (incluyendo papel, fichas, películas, y soportes electrónicos) se han realizado correctamente, y se ha corregido cualquier riesgo identificado.
- El backup de las telecomunicaciones y las estrategias de recuperación identificadas en otros capítulos del Plan están completamente realizadas y comprobadas.
- Las estrategias de recursos y soluciones de recuperación (por ejemplo: soluciones de reposición de ordenadores) están disponibles, realizadas y comprobadas satisfactoriamente.
- Las organizaciones externas como clientes, suministradores y organismos públicos, cooperarán razonablemente durante el periodo de los trabajos de recuperación.
- Se han realizado adecuadamente los programas de pruebas del Plan y las modificaciones pertinentes como consecuencia de su resultado.
- La revisión del Plan, mantenimiento, y actualizaciones están realizadas con periodicidad para asegurar que responde a las necesidades de cada momento.
- Se han realizado adecuadamente los programas de sensibilización y entrenamiento.

| Preparado por: | Conforme: | Aprobado por: |
|---|---|---|
| | | |

**Figura 5.3.- Ejemplo de Formulario para Condiciones Iniciales**

## 5.2 Administración del Programa

### 5.2.1 Directivas y compromiso

El proceso de elaboración e implementación del plan debe ser cuidadosamente realizado y previamente propuesto a la directiva para su aprobación, por tanto, para la mayor parte de los incidentes, los procedimientos de respuesta y recuperación están previamente estudiados y aprobados. Las funciones de la directiva se limitan a la revisión y aprobación de cualquier acción que exceda de las estrategias de respuesta y recuperación planificadas y previamente aprobadas.

Las directivas de la entidad deben demostrar el compromiso con el programa para prevenir, mitigar las consecuencias de, prepararse para, responder ante, mantener la continuidad durante y recuperarse de los incidentes

Solamente en aquellos casos en los que el incidente haya sobrepasado las previsiones será precisa la intervención directa de los órganos directivos.

En estos casos, el equipo de Gestión de Incidentes es responsable de la preparación de informe para la Dirección, con la que ayudar a la gestión del día adía y a la toma de decisiones acerca de cuestiones no previstas en el plan.

El compromiso de las directivas debe incluir lo siguiente:

1. Políticas, planes y procedimientos a desarrollar, implementar y mantener el programa.
2. Recursos para apoyar el programa.
3. Revisiones y evaluaciones para asegurar la efectividad del programa.
4. Corrección de deficiencias.

La entidad se debe adherir a las políticas, ejecutar los planes y seguir los procedimientos establecidos para soportar el programa.

### 5.2.2 Coordinador del programa

El coordinador del programa debe ser asignado por la entidad y autorizado para desarrollar, implementar, administrar, evaluar y mantener el programa.

### 5.2.3 Comité del programa

Un comité del programa debe ser establecido por la entidad en concordancia con su política. El comité debe proveer lineamientos para, y/o apoyar en, la coordinación de la preparación, el desarrollo, la implementación, la evaluación y el mantenimiento del programa.

El Comité debe incluir al coordinador del programa y a otras personas que rengan la experiencia, el conocimiento de la entidad y la capacidad para identificar recursos de todas las áreas funcionales claves dentro de la entidad, y debe solicitar representantes de entidades extremas relacionadas.

### 5.2.4 Administración del Programa

La entidad debe tener un programa escrito con el siguiente contenido:

- Política ejecutiva, incluyendo la cisión, declaración de misión, roles y responsabilidades y delegaciones de autoridad.
- Alcance del programa, metas, objetivos y método de evaluación del mismo.
- Planes y procedimientos que incluyan lo siguiente:
    a) Costos estimados.
    b) Prioridades.
    c) Cronograma.
    d) Recursos requeridos.
- Autoridades relacionadas, legislación, regulaciones y códigos de práctica de la industria aplicables.
- Presupuesto del programa y cronograma incluyendo hitos o puntos de control para el seguimiento.
- Directrices para el manejo de archivos.

### 5.2.5 Leyes y autoridades

El programa debe cumplir con la legislación aplicable, políticas, requerimientos regulatorios y directrices. La entidad debe establecer y mantener el o los procedimientos para cumplir la legislación aplicable, políticas, requerimientos regulatorios y directrices. Así como implementar una estrategia para atender las necesidades de revisión frente a la legislación, regulaciones y códigos de práctica de la industria.

### 5.2.6 Objetivos de desempeño

La entidad debe establecer objetivos de desempeño frente a los requisitos del programa. Estos objetivos deben depender de los resultados de la identificación de peligros, evaluación de los riesgos, y análisis de impacto en el negocio.

Los objetivos de desempeño deben ser desarrollados por la entidad para atender las necesidades a corto y largo plazo. Y cada entidad deberá definir los términos de corto y largo plazo.

### 5.2.7 Administración y finanzas

La entidad debe desarrollar procedimientos administrativos y financieros para sostener el programa antes, durante y después del incidente.

Debe existir una estructura para el manejo financiero y administrativo, que cumpla con los requerimientos del programa de la entidad y esté ligado únicamente con las operaciones de respuesta, continuidad y recuperación.

Procedimientos adecuados de manejo de crisis deben ser establecidos para proveer niveles coordinados de autorización, ante situaciones específicas, así como medidas de control apropiadas.

La estructura debe proveer máxima flexibilidad, para solicitud expedita, recibo, manejo y aplicación de fondos, tanto en momentos de no-emergencia, como en situaciones de emergencia, para asegurar el suministro oportuno de la asistencia.

El procedimiento administrativo debe ser documentado mediante procedimientos escritos.

El programa debe ser capaz de registrar la información financiera para recuperación posterior de gastos, así como identificar y acceder a fuentes alternativas de financiación y administrar fondos presupuestados y fondos especialmente asignados.

Deben crearse y mantenerse procedimientos para decisiones fiscales expeditas en concordancia con los niveles de autorización establecidos, principios de contabilidad y otras políticas fiscales. Es tos procedimientos deben incluir lo siguiente:

- Establecimiento y definición de responsabilidades para la autoridad financiera del programa, incluidos sus vínculos para reportar al coordinador del mismo.
- Procedimientos para adquisiciones del programa.
- Pago de nóminas.
- Sistemas de contabilidad para rastrear y documentar costos.
- Manejo de fondos de fuentes externas.

### 5.2.8 Manejo de registros

La entidad debe desarrollar un programa de manejo de registros.

Deben crearse, aprobarse y aplicarse políticas dirigidas a lo siguiente:

- Clasificación de registros.
- Mantenimiento de la confidencialidad.
- Mantenimiento de la integridad incorporando trazabilidad para auditoría.
- Retención de registros.
- Almacenamiento de los registros.
- Archivo de los registros.
- Control de acceso
- Control documentario.

La entidad debe aplicar el programa tanto para los registros existentes, como para los que sean creados. También debe desarrollar y aplicar procedimientos coordinando el acceso y circulación de registros dentro y fuera de la organización, así como, ejecutar el programa de manejo de registros.

## 5.3 Planeación del Programa

El programa debe seguir un proceso de planeación para desarrollar los planes: estratégicos, de manejo de crisis, de prevención, de mitigación, de operaciones de emergencia/respuesta, de continuidad y de recuperación.

# Capítulo 5 Plan de Continuidad de Negocio y Plan de Recuperación de Desastre

La planeación estratégica debe definir la visión, misión y metas. La planeación de la administración de crisis debe atender los aspectos que amenacen la estrategia, la imagen y los elementos intangibles de la entidad. La entidad debe incluir a otras partes interesadas claves en el proceso de planeación.

### 5.3.1 ¿Por dónde empezamos?

Para desarrollar un Plan de Continuidad de Negocio tenemos que empezar por obtener un conocimiento de la empresa/organización: sus productos/servicios, sus objetivos, procesos internos, etc.

El propósito general de un Plan de recuperación es **obtener un mapa de acciones** que reduzcan "la toma de decisiones" durante las operaciones de recuperación, restaure los servicios críticos rápidamente y permita un normal funcionamiento de los sistemas y procesos los antes posible, minimizando costes y aumentando la efectividad.

### 5.3.2 Identificación de Peligros

La entidad debe realizar una evaluación del riesgo para identificar estrategias para la prevención y mitigación y para recolectar información para el desarrollo de planes para respuesta, continuidad y recuperación. Se deben identificar los peligros y monitorear su probabilidad de ocurrencia.

Una evaluación completa de riesgo identifica el rango de posibles peligros o emergencias que han impactado o podrían impactar a la entidad, el área que la rodea o la estructura de soporte crítico. El impacto potencial de cada peligro, amenaza o emergencia está determinado por la severidad de cada uno y la vulnerabilidad de las personas, propiedad, operaciones, medio ambiente y la entidad ante cada peligro o emergencia. La evaluación de riesgo debería categorizar peligros o emergencias de acuerdo con su frecuencia y severidad relativas, teniendo en mente que pueden haber muchas combinaciones posibles de frecuencias y severidad para cada una de ellas. La entidad debería procurar planes para prevenir, mitigar, prepararse para, responder ante y recuperarse de, aquellos peligros o emergencias que son capaces de un impacto significativo sobre las personas, propiedad, operaciones, medio ambiente o la entidad misma.

La evaluación de riesgo es un proceso para la identificación de peligros y su relativa probabilidad de ocurrencia, la identificación de bienes en riesgo, evaluación de su vulnerabilidad ante los peligros identificados y cuantificación del impacto potencial del peligro sobre tales bienes. Muchos peligros potenciales deberían ser inicialmente evaluados y una re-evaluación periódica sería necesaria según cambien la entidad y los peligros a lo largo del tiempo.

Los peligros a ser evaluados incluyen los siguientes:

#### 5.3.2.1 Fenómenos naturales

Pueden presentarse sin influencia humana y tienen un impacto potencial directo o indirecto sobre la entidad (personas, propiedad, medio ambiente), tales como los siguientes:

a) Fenómenos geológicos (no incluyen asteroides, cometas, meteoros), como los siguientes:
    i. Terremoto

ii. Tsunami
iii. Erupción volcánica
iv. Deslizamiento de tierra, de lodo, hundimiento
v. Glaciar, iceberg

b) Fenómenos meteorológicos, como los siguientes:
   i. Inundación, inundación súbita, mareas, oleada
   ii. Sequía
   iii. Incendio (de bosques, de praderas, urbanos, forestales, de interface urbana)
   iv. Nieve, hielo, granizo, agua nieve, avalancha
   v. Ventiscas, ciclón tropical, huracán, tornado, aguas llevadas por el viento, tormentas de polvo/arena
   vi. Temperaturas extremas (calor, frío)
   vii. Rayos
   viii. Tormenta geomagnética

c) Fenómenos biológicos, como los siguientes:
   i. Brotes de enfermedades que afecten a los humanos, animales [peste, viruela, ántrax, virus del oeste del Nilo, fiebre aftosa, síndrome severo respiratorio agudo SARS, enfermedades pandémicas, encefalopatía bovina espongiforme (BSE, o enfermedad de las vacas locas)]
   ii. Infestación animal o de insectos y daños ocasionados por estos

#### 5.3.2.2 Eventos antropogénicos

Eventos causados por humanos, tales como los siguientes:

a) Fenómenos accidentales como los siguientes:
   i. Derrame o emisión de materiales peligrosos (explosivos, líquidos inflamables, gases inflamables, sólidos inflamables, oxidantes, venenos, radiológicos, corrosivos)
   ii. Explosión/incendio
   iii. Accidentes de transporte
   iv. Colapso de edificios/estructuras
   v. Falla de energía/potencia/servicios
   vi. Escasez de combustible/recursos
   vii. Polución de aire7agua, contaminación
   viii. Falla de estructuras de contención de agua/represas/diques
   ix. Asuntos financieros, depresión económica, inflación, colapso del sistema financiero
   x. Interrupción de los sistemas de comunicación
   xi. Pérdida de información
   xii. Hambruna
b) Fenómenos intencionales, como los siguientes:

i. Terrorismo (explosivo, químico, biológico, radiológico, nuclear, cibernético)
ii. Sabotaje
iii. Disturbios civiles, desordenes políticos, histeria colectiva, asonadas
iv. Ataque enemigo, guerra
v. Rebelión
vi. Huelga o contienda laboral
vii. Desinformación
viii. Actividad criminal (vandalismo, incendio intencional, robo, fraude, defraudación, robo informático)
ix. Pulso electromagnético
x. Violación de seguridad física o de información
xi. Violencia en el lugar de trabajo/colegio/universidad
xii. Defecto o contaminación de productos
xiii. Hostigamiento
xiv. Discriminación

#### 5.3.2.3 Eventos por causas tecnológicas

Eventos causados por la tecnología que pueden no estar relacionados con sucesos naturales o humanos como los siguientes:

a) Peligros del computador central, procesador central, servidor, software o de aplicación (interna/externa)
b) Peligros del equipo auxiliar de soporte
c) Peligros de telecomunicaciones
d) Peligros de electricidad/energía/servicios públicos

Se debe identificar, evaluar y monitorear la vulnerabilidad de las personas, de la propiedad, del medio ambiente y de la entidad. Todas las amenazas en los ejemplos anteriores comparten un efecto común: el potencial daño a la infraestructura de la organización.

## 5.4 Análisis de Impacto del Negocio (BIA)

El propósito fundamental del Análisis de Impacto del negocio, conocido más comúnmente como BIA, (Bussines Impact Analysis) es determinar y entender qué procesos son esenciales para la continuidad de las operaciones y calcular su posible impacto. Este proceso es parte fundamental dentro de la elaboración de un Plan de Continuidad de Negocio.

El resultado de un análisis de impacto es la diferencia entre las actividades críticas (urgentes) y actividades o funciones no críticas. Donde una función o actividad puede considerarse crítica si las consecuencias para las partes interesadas de los daños a la organización resultante se consideran inaceptables. Una función o actividad puede ser también considerada como crítica si así lo dicta la ley.

### 5.4.1 Objetivos del análisis

Las funciones que desempeña una organización no suelen tener el mismo grado de criticidad en función del tiempo. Aún admitiendo que todas ellas son necesarias, no todas tienen las mismas repercusiones en las operaciones de la organización y, como consecuencia, una interrupción de la ejecución de u otra causaría los mismos perjuicios, e incluso para una misma función, puede ocurrir que el impacto sea diferente dependiendo del día o mes en que ocurra.

El objetivo del Análisis de Impacto es proporcionar a la dirección la información necesaria para que pueda tomar decisiones en el desarrollo de su estrategia de recuperación. Para ello el análisis de impacto debe determinar el grado de criticidad de dichas funciones en la razón de ser de la organización y el tiempo máximo a partir del cual la interrupción de cada una de ellas es inaceptable.

El objetivo genérico se materializa en los siguientes objetivos básicos:

- Definir los tipos de impacto que se deberían considerar, (económico, comercial, operacional, de imagen, jurídico, etc.).
- Identificar las funciones críticas de la organización.
- Identificar el impacto causado a la organización por la interrupción de cada una de ellas.
- Informar a la dirección de los resultados anteriores para que pueda fijar prioridades, definiendo cuáles son las funciones consideradas prioritarias y establecer los umbrales máximos de recuperación para cada una de dichas funciones.
- Posibilitar la identificación de los recursos mínimos necesarios para una recuperación satisfactoria de las funciones definidas como críticas y justificar su adquisición.

### 5.4.2 Alcance del análisis

El análisis de impacto realizado se refiere exclusivamente a los efectos, tanto tangibles como intangibles, que causaría en la organización la interrupción de las siguientes funciones consideradas críticas por el equipo de la organización:

- AAAAAA
- BBBBBBB
- CCCCCCC

### 5.4.3 Resumen de resultados

De la elaboración de la información recibida, se desprende que si se produjera una interrupción de las funciones citadas, las pérdidas económicas totales en miles de pesos serían las que se reflejan en la **Figura 5.4.**

En los casos en que no fuera posible establecer una valoración cuantitativa, se realizaría una valoración cualitativa. Los resultados serían similares a los que se reflejan en la **Figura 5.5.**

Impacto económico (000$) (*)

| | Duración de la interrupción | | | |
|---|---|---|---|---|
| | 4 horas | 1 dia | 2 dias | 1 semana |
| Función A | 15 | 30 | 93 | 156 |
| Función B | 314 | 628 | 1.884 | 3.140 |
| Función C | 12,5 | 26 | 80 | 136 |
| Total | 341,5 | 684 | 2.057 | 3.432 |

(*) Valores ficticios. Sustituir por los valores reales

| Preparado por: | Conforme: | Aprobado por: |
|---|---|---|
| Fecha: | Fecha: | Fecha: |

**Figura 5.4.- Ejemplo de Formulario Impacto económico (000$)**

**Impacto cualitativo (*)**

| Función A | | | | |
|---|---|---|---|---|
| | Gravedad | | | |
| **Impacto** | **4 horas** | **1 día** | **2 días** | **1 semana** |
| Económico | Nulo | Leve | Medio | Catastrófico |
| Comercial | Nulo | Nulo | Nulo | Leve |
| Operacional | Nulo | Nulo | Nulo | Nulo |
| Imagen | Nulo | Leve | Leve | Leve |
| Legal | Nulo | Nulo | Nulo | Leve |
| | | | | |

| Función B | | | | |
|---|---|---|---|---|
| | Gravedad | | | |
| **Impacto** | **4 horas** | **1 día** | **2 días** | **1 semana** |
| Económico | Leve | Medio | Grave | Catastrófico |
| Comercial | Nulo | Nulo | Nulo | Nulo |
| Operacional | Leve | Medio | Grave | Catastrófico |
| Imagen | Nulo | Leve | Medio | Grave |
| Legal | Nulo | Nulo | Leve | Grave |
| | | | | |

| Función C | | | | |
|---|---|---|---|---|
| | Gravedad | | | |
| **Impacto** | **4 horas** | **1 día** | **2 días** | **1 semana** |
| Económico | Nulo | Nulo | Leve | Medio |
| Comercial | Nulo | Leve | Grave | Catastrófico |
| Operacional | Nulo | Leve | Grave | Catastrófico |
| Imagen | Nulo | Leve | Medio | Catastrófico |
| Legal | Nulo | Nulo | Leve | Medio |
| | | | | |

(*) Valores ficticios. Sustituir por los valores reales

| Preparado por: | Conforme: | Aprobado por: |
|---|---|---|
| Fecha: | Fecha: | Fecha: |

**Figura 5.5.- Ejemplo de Formulario: Impacto cualitativo**

### 5.4.4 Pauta para valoración de Impactos

Es una orientación respecto a la calificación de la gravedad de los distintos tipos de impacto.

**Pauta para valoración de impactos (*)**

| TIPOS DE IMPACTO Y EFECTOS PRODUCIDOS | CRITERIOS Y VALORACIÓN | | | |
|---|---|---|---|---|
| | Leve | Medio | Grave | Catastrófico |
| Pérdida de ingresos | < de 0,1 M$ | De 0,1 a 1 M$ | De 1 a 10 M$ | > de 10 M$ |
| Pérdida de beneficios | < de 0,01 M$ | De 0,01 a 0,1 M$ | De 0,1 a 1 M$ | > de 1 M$ |
| Incremento de costes y/o gastos | < de 0,1 M$ | De 0,1 a 1 M$ | De 1 a 10 M$ | > de 10 M$ |
| Impacto comercial | Produce una interrupción leve en el suministro de servicios o productos con mínimo impacto en la operativa de los clientes. La pérdida de ventas se recupera al reanudar la actividad | Obliga al cliente a cambiar de proveedor de forma transitoria. Las ventas no realizadas no se recuperan | Pérdida de algunos clientes de forma definitiva. Impacto leve en la cartera de prospectos | Pérdida de clientes clave. Impacto grave en la cartera de prospectos |
| Impacto operacional | Produce retrasos en funciones no vitales | Produce retrasos leves en funciones vitales | Produce retrasos graves en funciones vitales | Produce la interrupción inmediata de funciones vitales |
| Impacto en la imagen | Conocido solamente por algunos clientes. Sin presencia en los medios de comunicación | Pérdida de confianza en un producto o servicio específico o en una parte de la organización. Comentarios adversos en medios locales | Pérdida de confianza en una gama de productos o servicios o en varias áreas de la organización. Comentarios adversos en los medios nacionales | Pérdida de la confianza del mercado y daños a la imagen de marca. Campaña continuada en los medios nacionales. Impacto en la Bolsa |
| Incumplimiento de obligaciones legales | Produce una falta leve en el cumplimiento de algún contrato. | Produce una falta en el cumplimiento de algún contrato que obliga a renegociar | Produce una falta grave en el cumplimiento de algún contrato que acarrea responsab. legales | Deja a la organización al margen de la ley |

(*) A modo de orientación

| | | |
|---|---|---|
| Preparado por: | Conforme: | Aprobado por: |
| Fecha: | Fecha: | Fecha: |

**Figura 5.6.- Ejemplo de Formulario Pauta para valoración de impactos**

*Los pasos claves son los siguientes:*

1. Confirmar, con base en la valoración del riesgo y la vulnerabilidad, los procesos clave de la organización y su función, para determinar la criticidad de los procesos.
2. Determinar las consecuencias de una disrupción de los procesos críticos identificados en términos financieros u operacionales, o ambos, sobre períodos definidos.
3. Identificar las interdependencias con las partes interesadas claves, internas y externas, las cuales podrían incluir el mapeo de la naturaleza de las interdependencias a través de la cadena de abastecimiento.
4. Determinar los recursos actualmente disponibles y el nivel esencial de recursos requeridos para continuar operando el nivel mínimo aceptable a continuación de la disrupción.
5. Identificar las formas para eludir problemas en procesos actualmente en uso o planeados para ser desarrollados. Podría ser necesario desarrollar procesos alternos cuando los recursos o la capacidad son inaccesibles o insuficientes durante la disrupción.
6. Determinar el tiempo máximo de aceptable de parada (TMP) [o tiempo máximo aceptable de interrupción de servicios (TMIS)] para cada proceso, con base en las consecuencias identificadas y los factores críticos de éxito para la operación. Los TMP (TMIS) representan el período máximo de tiempo que la organización puede tolerar la pérdida de capacidad.
7. Confirmar el nivel actual de preparación de los procesos críticos para manejar una disrupción. Esto puede incluir la evaluación del nivel de redundancia dentro del procesos (ej: equipo de reserva) o la existencia de proveedores alternos.

*Salidas o resultados*

Las salidas son las siguientes:

1. Impacto financiero para la organización o entidad debido al riesgo particular que se necesita mitigar, minimizar, prevenir o evitar; en consecuencia, la justificación del costo hecha con base en el monto del impacto determinado.
2. Impacto operacional para la entidad, incluidas las operaciones e interrelaciones hacia adelante y hacia atrás o el impacto en cascada, o ambos, tanto al nivel interno como externo a la entidad.
3. Lista de prioridades en los procesos críticos prioritarios e interdependencias asociadas.
4. Impactos financieros y operacionales, documentados, derivados de la pérdida de procesos críticos identificados.
5. <recursos de apoyo requeridos para los procesos críticos identificados.
6. Marcos de tiempo para las paradas de los procesos críticos y marcos de tiempo para la recuperación de la comunicación.

Dentro del análisis de impacto, la entidad deber considerar los impactos externos a su área de influencia que pudieran afectar la habilidad de la entidad para tratar con un incidente. Un ejemplo es el efecto cascada de un huracán. El impacto directo puede incluirlo los daños por vientos e inundaciones. El impacto secundario puede incluir comunicaciones, energía y disrupciones del transporte, tanto dentro como fuera del área de impacto directo, y el impacto potencial sobre la entidad, en términos cuantificables

También se debe considerar lo siguiente dentro del análisis de impacto:

- Salud y seguridad de las personas en el área afectada al tiempo del incidente (lesione y muerte).
- Salud y seguridad del personal que responde al incidente.
- Continuidad de las operaciones.

### 5.4.5 Requisitos para la recuperación

#### 5.4.5.1 Costo de la protección

La elección de las estrategias y soluciones de recuperación está dictada por dos factores: la capacidad de cumplir con los requisitos de tiempo de recuperación y el costo correspondiente. Estos dos factores están típicamente interrelacionados.

Según se ilustra en la **Figura 5.7**, los costos de las estrategias de recuperación, a menudo están en proporción directa a la rapidez con que se requiere obtener la recuperación.

Por ejemplo, si se requiere la recuperación inmediata de un gran departamento de pedidos telefónicos en una organización de venta por catálogo con varios cientos de estaciones, se necesitarán unas instalaciones redundantes con un costo muy superior así, el mismo departamento pudiera diferir la recuperación durante varias semanas. El espacio de oficinas y la reubicación de equipos y telecomunicaciones podrían instalarse durante el tiempo de recuperación y los costos correspondientes serían muy inferiores.

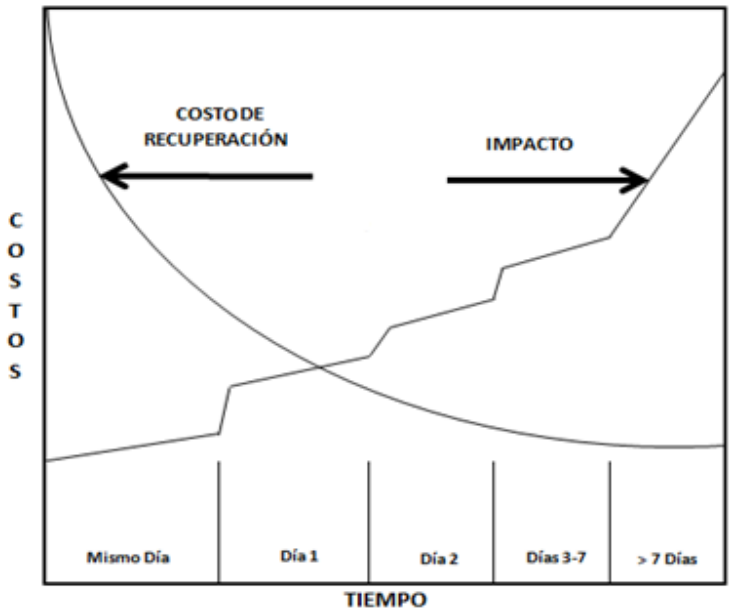


**Figura 5.7.- Gráfica Costos vs. Tiempo**

#### 5.4.5.2 Pérdidas asumibles

A la vista de esta contraposición entre los requisitos de recuperación y el costo de las medidas necesarias para conseguir que ésta efectúe en el menor tiempo posible, se hace imprescindible tomar la decisión acerca de las pérdidas que la organización puede asumir en el supuesto de una interrupción para tratar de optimizar los costos de las medidas a implantar.

#### 5.4.5.3 Umbrales de recuperación

El Análisis de Impacto proporciona la información necesaria para identificar las necesidades de recursos de recuperación (vg. Número de personas, categoría de los equipos, suministros específicos, etc.) Dentro de los plazos especificados, llamados umbrales de recuperación. El concepto de umbrales de recuperación está basado en las consideraciones siguientes:

- Las consecuencias de una interrupción de una función de negocio no ocurren inmediatamente. Muchas operaciones pueden diferirse durante algún tiempo sin que las consecuencias sean excesivas o inaceptables. Además, algunas acciones sencillas, por ejemplo, los procedimientos de respuesta, frecuentemente pueden retrasar otras consecuencias más graves.
- Las organizaciones pueden implementar algunas veces estos procedimientos de respuesta e incluso operar con éxito, durante un corto espacio de tiempo, con menos recursos de los que normalmente se necesitan.
- El tiempo necesario para obtener los recursos esenciales es generalmente predecible, permitiendo algunos ahorros de coste en la recuperación del negocio, retrasando la adquisición de algunos recursos hasta el último momento del desastre.

Del análisis de estas consideraciones, así como del equilibrio entre pérdidas asumibles y restricciones presupuestarias, se definirán los objetivos de la recuperación que usualmente viene definidos como:

##### 5.4.5.3.1 Tiempo de Recuperación Objetivo RTO, (Recovery Time Objective)

Es la duración de tiempo y el nivel de servicio en el que debe ser un proceso de negocio restaurado después de un desastre (o interrupción) con el fin de evitar consecuencias inaceptables derivados de una ruptura de continuidad del negocio. Este tiempo de recuperación objetivo debe asegurar que el período de interrupción máximo tolerables (MTPD) para cada actividad no sea superado.

##### 5.4.5.3.2 Punto de Recuperación Objetivo, RPO (Recovery Point Objective)

Es el punto en el tiempo al cual se debe de recuperar los datos tal como es definido por la organización. Esto es generalmente una definición de lo que la organización determina que es una “pérdida aceptable” en una situación de

desastre. Este punto de recuperación debe asegurar que el máximo tolerable de pérdida de datos para cada actividad no se supera.

#### 5.4.5.3.3 Tiempo Máximo de Interrupción, MAO (Maximum Aceptable Outage)

Umbral de tiempo máximo de interrupción durante el cual se debe hacer efectiva la recuperación para evitar que dicha interrupción ponga en peligro la consecución de los objetivos de la organización o su propia existencia.

Como resultado de la fijación de estos objetivos, las necesidades de recursos de recuperación pueden identificarse por tiempo, (es decir, umbrales de recuperación). Los hitos que se han establecido para determinar los umbrales de recuperación en el presente trabajo son los siguientes: 4 horas, 1 día, 2 días y una semana.


**Figura 5.8.- Análisis de Impacto**

## 5.5 Medidas a implantar

### 5.5.1 Estrategias de prevención

Puesto que la finalidad del análisis de impacto, a más o menos corto plazo es el desarrollo e implementación de un Plan de Continuidad de Negocio, parece sensato que, antes de la adopción de estas medidas se analicen cuáles son las amenazas más probables para la organización y la probabilidad que esas amenazas se materialicen causando la interrupción de las operaciones de la organización. Es decir, resulta muy recomendable realizar un análisis de riesgos y acometer las acciones que se deriven del mismo con objeto de reducir o eliminar los riesgos detectados y que la

activación de Plan de Continuidad de Negocio de 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.

Por ello, previamente al establecimiento de cualquier tipo de estrategia de respuesta o de reubicación, se debería establecer una estrategia de prevención que incluyera, en mayor o menor profundidad, la adopción de las siguientes medidas:

- Análisis y reducción de los riesgos a que está expuesta la organización.
- Identificación de amenazas y vulnerabilidades.
- Identificación de riesgos potenciales. Probabilidad y consecuencias.
- Determinación de niveles aceptables de riesgo.

### 5.5.2 Soluciones Para Registros Vitales

Las soluciones para registros vitales se desarrollan para protección de los recursos de información vital tales como los datos almacenados en papel, soportes magnéticos, ópticos o cualquier otro medio. La planificación de la estrategia determina cómo estará protegida esta información y cómo se recuperará en el momento de desastre.

- *Selección de las instalaciones de almacenamiento externo.* La recuperación con éxito de una pérdida catastrófica, (es decir, una que suponga daño físico para las instalaciones y su contenido), es a menudo dependiente de la información crítica y los recursos de recuperación almacenados en un lugar alternativo, lejos de las instalaciones habituales. Por ello, las copias de seguridad, (en soporte magnético, óptico, microfilm o papel), y la documentación y suministros críticos, deben almacenarse en unas instalaciones con garantía de supervivencia incluso en el caso de la destrucción total de las instalaciones habituales de la organización.
- *Consideraciones.* Al seleccionar la localización de unas instalaciones para el almacenamiento externo, se deben tener en cuenta dos consideraciones fundamentales: la seguridad y la accesibilidad.

Los datos y documentación vital para la organización custodiados en un almacenamiento externo tienen que estar rápidamente disponibles ante una posible recuperación. Al mismo tiempo, deben estar a una distancia no excesiva para facilitar las entregas y recogidas durante el trabajo del día a día. La situación ideal es que las instalaciones de almacenamiento externo tampoco estén excesivamente alejadas del centro de respaldo.

Para conseguir una seguridad adecuada, la documentación y datos vitales deben estar custodiados en unas instalaciones con los debidos controles de humedad y temperatura y protegidas contra incendios, inundaciones, accesos no autorizados, perturbaciones radioeléctricas, etc.

- *Ubicaciones posibles.* Es posible utilizar una variedad de diferentes opciones respecto a la utilización de instalaciones de almacenamiento externo.

**Posibles ubicaciones del almacenamiento externo (*)**

| Tipo de Estrategia | Ventajas Inconvenientes |
|---|---|
| Otra dependencia de la organización | ▪ Bajo coste de explotación<br>▪ Posibilidad de uso de los servicios de correo interno para el transporte del día a día<br>▪ Alto coste de la inversión en las instalaciones<br>▪ Riesgo de caer en falta del rigor necesario en la operativa de renovación de las copias de seguridad<br>▪ Riesgo de falta de control de las versiones custodiadas<br>▪ Falta de disponibilidad en casos de problemas laborales que impliquen dificultad de acceso a las instalaciones |
| Caja fuerte de un banco | ▪ Bajo coste de explotación<br>▪ Necesidad de uso de los servicios de correo interno para el transporte del día a día<br>▪ Falta de disponibilidad fuera del horario bancario<br>▪ Falta de disponibilidad en casos de problemas laborales en el sector de Banca |
| Contratación de un servicio externo | ▪ Garantía de disponibilidad 24/7<br>▪ Servicio de transporte fiable y programado<br>▪ Medidas de seguridad de alto nivel<br>▪ Aparente mayor coste de explotación si no se hace una comparación de costes adecuada |

(*) Ubicaciones teóricas. Sustituir por casos reales.

| Preparado por: | Conforme: | Aprobado por: |
|---|---|---|

**Figura 5.9.- Ejemplo de Formulario para Posibles Ubicaciones de Almacenamiento Externo**

En resumen, el almacenamiento externo de la información vital debe tener los mismos niveles de accesibilidad y condiciones de conservación que los existentes en las instalaciones habituales de explotación.

### 5.5.3 Estrategias de respuesta

Es posible elegir entre varias estrategias para la elección de las medidas a implantar:

1) Diferir la realización de las funciones del negocio.
2) Dispersar las operaciones de negocio para que ninguna interrupción individual de un área de la organización sea intolerable.

3) Reubicar las operaciones de negocio durante el tiempo de recuperación, Una variante de la reubicación de las operaciones de negocio es mitigar el impacto mediante algún tipo proceso de respuesta a corto plazo Las funciones de negocio individuales y los consecuentes impactos de su interrupción, determinan qué estrategias de proceso alternativo se pueden emplear. Al elegir la estrategia, debe tenerse la precaución de incluir el impacto de pérdida de información en la evaluación de las estrategias de recuperación apropiadas.
4) Posponer las funciones de negocio, (al menos hasta que pasen los efectos del incidente), es una estrategia de negocio, común y a menudo aceptable. En particular, las actividades de áreas de la organización que no tengan unos requisitos urgentes de tiempo, (por ejemplo, unidades de planificación estratégica, departamentos de auditoría, etc.), a menudo determinan que la mejor estrategia de recuperación consiste en aceptar el retraso de sus actividades. Esta estrategia funciona mejor cuando la función de negocio puede ser diferida lo suficiente como para permitir que la restauración sea realizada en el tiempo de la recuperación. Al mitigar los impactos a corto plazo de una interrupción del negocio mediante una planificación de la respuesta, (por ejemplo, respuestas telefónicas e históricas de transacciones), puede llevar, a menudo, algunas funciones de negocio a la categoría de “espera”.

Las estrategias de dispersión y reubicación están íntimamente relacionadas y pueden incluso solaparse. Por ejemplo, pueden utilizarse empresas de servicios externos para realizar lagunas funciones de negocio de forma regular o en emergencias, dispersando el impacto potencial de una interrupción de negocio. Estos servicios pueden ser ampliados para reubicar operaciones durante un desastre. Decidir qué estrategia o qué combinación de estrategias emplear requiere la comprensión general de las diversas estrategias de lugares alternativos disponibles.

### 5.5.4 Estrategias de Centros Alternativos

Es posible aplicar una variedad de diferentes estrategias de centros alternativos.

**Posibles estrategias de centros alternativos (*)**

| ESTRATEGIAS DE CENTROS ALTERNATIVOS | | |
|---|---|---|
| **Tipo de Estrategia** | **Marco del tiempo de recuperación.** | **Ejemplos: Ventajas /Inconvenientes** |
| Reparación/ Reconstrucción durante el desastre | Días - Meses | Reparar corte energía, Secar instalación por fallo de sprinklers:<br>-Coste bajo<br>-La mayor parte de las interrupciones son de corta duración<br>-Tiempo de recuperación |
| Adquisición de espacio para el tiempo que dure el desastre | 1 - 3 Días | Alquilar espacio de oficinas al ocurrir el desastre:<br>-Bajo coste para espacio y equipo de oficinas.<br>-Riesgo de disponibilidad.<br>-Disponibilidad de espacio especialmente acondicionado.<br>-Dificultad y necesidades de tiempo para la restauración de las comunicaciones de datos.<br>-Tiempo necesario para la instalación de cableado LAN. |
| Contratación de servicio móvil de Backup | 1 - 3 Días | Espacio móvil de oficina<br>-Fácil de usar.<br>-Puede resolver las necesidades de instalación de sistemas medios.<br>-Requiere planificación especial y autorizaciones.<br>-Difícil de instalar en un área metropolitana. |
| Oficina de servicios | 1 - 3 Días | Suministro externo de compañías de servicios, (por ejemplo, Servicios de copias, empresas de microfilmación)<br>Útil para la planificación de contingencias del día a día, (por ejemplo, sobrecargas de trabajo).<br>Efectivo en áreas con equipos especializados.<br>No disponible en la mayor parte de los entornos de negocio. |

**(*) Estrategias teóricas.**
**Sustituir por casos reales.**

(continúa)

*(continuación)*

| ESTRATEGIAS DE CENTROS ALTERNATIVOS (*) | | |
|---|---|---|
| Contratación de centro fijo | Horas | Compañías de servicio de centros alternativos<br>-Posibilidad de hacer pruebas<br>-Posibles problemas de disponibilidad en desastres regionales |
| Acuerdos Recíprocos | Horas | Espacio interno de oficinas<br>Instalaciones especializadas externas (por ejemplo, ensobradora)<br>Útil para equipos especializados en aplicaciones de bajo volumen<br>Aplicaciones limitadas<br>Posibles problemas de falta de capacidad<br>Posibles problemas de no compatibilidad a medio plazo |
| Instalaciones Redundantes | Inmediato | Solución propia<br>Mayor fiabilidad<br>Alto costo<br>Necesidad de mantener la compatibilidad de HW y SW de forma permanente |

**(*) Estrategias teóricas. Sustituir por casos reales**

| Preparado por: | Conforme: | Aprobado por: |
|---|---|---|

**Figura 5.10.- Ejemplo de Formulario de Posibles estrategias de Centros Alternativos**

El análisis de impacto puede ser desarrollado usando estudios de ingeniería, modelaciones matemáticas, procesos estocásticos, simulaciones, inspecciones, cuestionarios, entrevistas, talleres estructurados o combinación de todos estos, para obtener un entendimiento de los procesos, gente/personal, bienes y recursos, propiedades físicas y no físicas, críticos y los efectos financieros y operacionales de la pérdida de estos elementos.

## 5.6 Plan de Recuperación de Desastres

### 5.6.1 Estrategia de Continuidad

No se puede dar un modelo fijo de estrategia. En función de las características de cada organización, el grado de criticidad de sus funciones y aplicaciones, la disponibilidad de servicios alternativos, etc., se podrán diseñar unas soluciones u otras.

En cualquier caso la estrategia seleccionada para conseguir una continuidad del negocio aceptable debe basarse en la disponibilidad de un centro alternativo, propio o subcontratado, en el que se realizarán las operaciones que permitan la continuidad de las funciones críticas de un período inferior al definido por los umbrales de respuesta y recuperación.

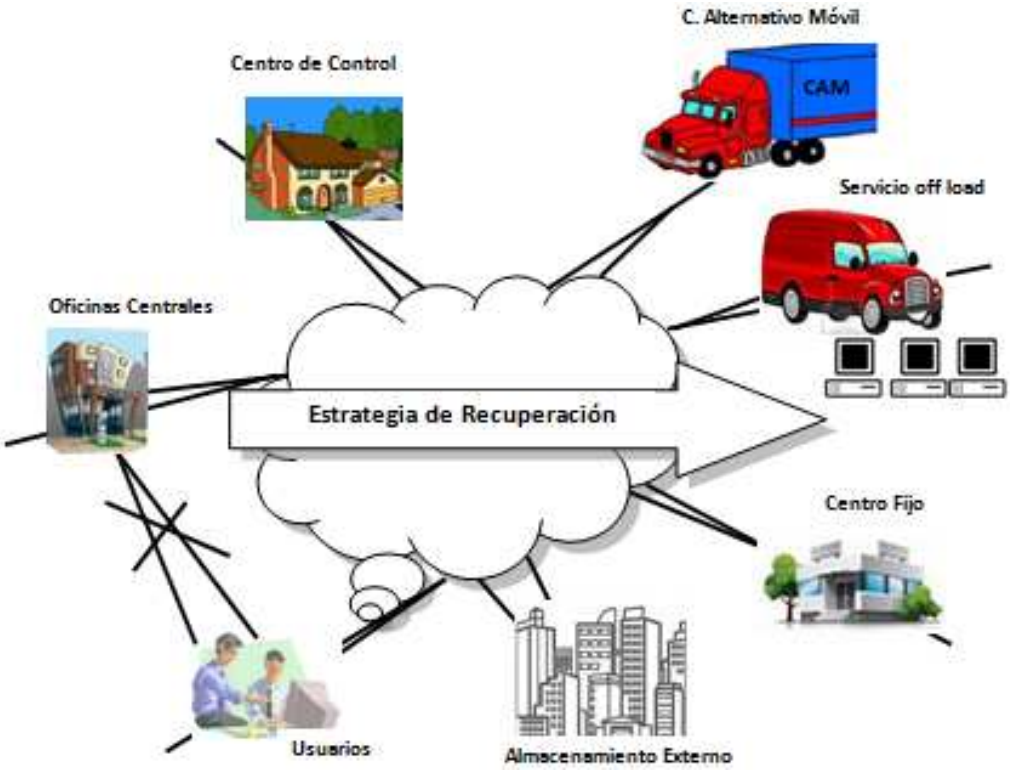


**Figura 5.11.- Estrategia de Continuidad**

En caso necesario, la dirección de las operaciones se realizará desde uno de los centros de control previamente definidos.

Concurrente con ello, se deberán conservar copias de seguridad convenientemente actualizadas en una ubicación externa y ajena a las instalaciones de la organización.

### 5.6.2 Centro de Control

El centro de control es el lugar de reunión, donde tienen lugar las actividades de valoración inicial, la coordinación y toma de decisiones. Las instalaciones del centro de control alojan al Equipo de Gestión de Incidentes y a los asesores durante las fases iniciales de respuesta y recuperación.

Al no poderse predecir la magnitud, alcance ni gravedad del incidente, deberán preverse varias ubicaciones del centro de control, acordes con las premisas de partida definidas al comenzar el proceso de planificación.

### 5.6.3 Centro Alternativo

Existen varias formas de dar respuesta a la necesidad de un centro alternativo.

En primer lugar, y dependiendo de los umbrales de recuperación que se hayan puesto como objetivos, habremos de definir un tipo de centro que responda a las necesidades de tiempo de disponibilidad pues, si bien cada día es más frecuente la presencia de aplicaciones de una gran criticidad respecto al tiempo, hay todavía muchas de ellas que admitirían una cierta demora en la recuperación después de la interrupción sin causar un impacto inadmisible.

#### 5.6.3.1 Centro frío

Es una sala vacía preparada con las condiciones ambientales necesarias para albergar equipos informáticos. Sobre todo debe tener instalación de potencia, climatización, falso suelo y una cierta estructura de comunicaciones. El *centro frío* está recomendado para empresas que por su estructura pueden estar un cierto período de tiempo sin servicios informáticos funcionando con procedimientos alternativos.

#### 5.6.3.2 Centro caliente

Es una instalación con un C.D.P. totalmente configurado a las especificaciones del cliente y disponible en pocas horas. El *centro caliente* está recomendado para organizaciones en las cuales su umbral de recuperación no supera las 24/48 horas.

#### 5.6.3.3 Centro espejo

En el caso de que las necesidades de respuesta sean inmediatas, la solución está en el llamado *centro espejo*, que consiste en dos instalaciones idénticas y actualizadas permanentemente con objeto de que una de ellas se haga cargo automáticamente del trabajo si la otra sufre una interrupción.

#### 5.6.3.4 Centro móvil

Existe otro tipo de servicio que consiste en trasladar las facilidades informáticas de respaldo al lugar determinado previamente en el Plan Contingencia. Es lo que se denomina un *centro móvil*, que 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 sólo a equipos y no a instalaciones, es el suministro de equipos de respaldo o servicio *"of load".*

Una vez decidida la fórmula del proceso alternativo, desde el punto de vista de tiempo de respuesta, habremos de decidir la fórmula para su contratación.

#### 5.6.3.5 Otra localización dentro de la organización

Cuando una organización tiene más de un centro de proceso de datos, una alternativa obvia es que un centro sirva de respaldo del otro. De todas formas, hay algunos elementos a considerar. Por ejemplo, si ambos centros están en la misma planta o en el mismo edificio, esta solución no ofrece garantías en el supuesto de que el incidente afecte al edificio. Incluso en la misma ciudad no se estaría protegido frente a desastres regionales. Sin embargo, si 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. La decisión debe estar basada en los supuestos de partida sobre los que se establece el plan de continuidad de negocio, es decir, para qué nos estamos planificando y para que NO nos estamos planificando.

Por otra parte, ¿hay suficiente espacio para el personal, suministros, mobiliario, etc., para las dos operaciones? Esto debe ser cuidadosamente estudiado, especialmente cuando se consideren largos períodos de interrupción. Se debe mantener hardware compatible en ambos centros. Incluso aunque ambas instalaciones estén en la misma organización y quizás reporten al mismo director, hay posibilidades de que las configuraciones de hardware evolucionen de forma diferente y lleguen a no ser intercambiables. Se debe hacer una revisión detallada de todo el hardware, al menos trimestralmente.

Se debe tomar una decisión sobre la compatibilidad en las necesidades de software en lo referente al entorno de proceso. Deben hacerse revisiones trimestrales para asegurar que existe el soporte necesario para todas las

aplicaciones críticas. Así mismo, 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 software, no sólo los obvios, las CPU y sistemas operativos.

### 5.6.4 Acuerdos de Ayuda Mutua

El objetivo de esta sección es familiarizarse con una estrategia para complementar el Plan de Recuperación de desastres mediante el trabajo conjunto con empresas localizadas en su misma zona geográfica, es decir, el plan de recuperación de desastres de una empresa u organización particular puede ser fortalecido mediante mecanismos de ayuda mutua.

Es difícil poder cubrir todos los riesgos a los que está expuesta una empresa u organización, ya que demanda costos muy altos y por ende difíciles de poder ser asumidos; ante esta limitante de alcanzar la seguridad total de la empresa u organización no queda más que elevar su nivel de seguridad haciendo uso del apoyo externo que pueda recibir.

El apoyo externo generalmente es enfocado específicamente a nivel de servicios públicos de socorro a los cuáles obviamente debe acudirse en toda circunstancia de riesgo, pero seguramente existe otro apoyo más inmediato y posiblemente más eficaz que no se ha tenido en cuenta y los constituye las empresas del vecindario que a lo mejor teniendo similitud de riesgo con la empresa dispondrá de protecciones compatibles y podrá brindarle valiosa ayuda en el control de una emergencia, esto podrá lograrse mediante el establecimiento de una plan de ayuda mutua.

El plan de ayuda mutua potencializa la seguridad brindada por las protecciones individuales disponibles por cada empresa en una comunidad industrial, revirtiendo en mayor capacidad para enfrentar con éxito una eventual emergencia y se fundamenta en el establecimiento de un acuerdo formal entre las empresas de un mismo sector geográfico para facilitarse ayuda técnica y humana en el evento de una emergencia que sobrepase o amenace con sobrepasar la capacidad de protección de la empresa u organización.

Los principios en los que se fundamenta el Plan de Ayuda Mutua son:

- Establecimiento de un convenio formal de ayuda mutua entre las empresas, suscrito a nivel gerencial y/o como compromiso de asociación.
- Delimitación clara de los recursos humanos y materiales para atención de emergencias que cada empresa está dispuesta a facilitar para el servicio de los demás sin deterioro de las condiciones mismas de seguridad.
- Compromiso de compensación económica o reintegro de los materiales o equipos consumidos o deteriorados ene l control de una emergencia por una empresa en beneficio de la otra.

#### 5.6.4.1 Estructura orgánica del plan.

Constituye la base de interacción del grupo de empresas y el planeamiento del Plan de Ayuda Mutua, se fundamenta en la conformación de Comités de Trabajo Interdisciplinarios en los campos: técnico, de comunicaciones, de relaciones públicas, de evacuación y de apoyo logístico: con objetivos y funciones plenamente definidas y coordinadas por un Consejo Directivo.

**Notas importantes**

- El plan de ayuda mutua debe ser perfectamente asimilado por todas las empresas que participan.
- Todas las empresas deben establecer canales de comunicación directa y confiable entre sí y con el centro de operaciones del comité local de emergencias.
- El plan de ayuda mutua debe velar también por las condiciones de protección industrial o seguridad física del sector.
- Los miembros de las brigadas de emergencia de cada una de las empresas deben recibir entrenamiento especial para enfrentarse a los riesgos especiales que puedan hallar en otras instalaciones amparadas por los acuerdos de ayuda mutua.

**Acuerdos con los proveedores de equipos**

No todos los proveedores se comprometerán por escrito a suministrar *backup* de su instalación. "Lo mejor posible" es una frase usada normalmente para describir verbalmente hasta dónde iría el proveedor para suministrar *backup* de emergencia en su centro de proceso de datos. Hay muchas situaciones en lo que "lo mejor posible" ha sido insuficiente. Sin embargo es cada vez más frecuente que los proveedores de equipos ofrezcan servicios de respaldo, por lo que al igual que en los casos anteriores, estos acuerdos deben estar reflejados de forma clara en un contrato específico para este servicio firmado por ambas partes.

### 5.6.5 Comunicaciones Alternativas

En función de la magnitud y alcance del incidente, puede ocurrir que la solución de respaldo requiera el uso de un centro alternativo remoto. Es ese caso, los usuarios críticos que no puedan ser ubicados en dicho centro alternativo deberían poder conectarse a él, por lo que será necesario disponer de una red de comunicaciones alternativas que permitan esa conexión.

### 5.6.6 Procedimientos de Backup

El departamento de Sistemas de la Información proporciona un servicio centralizado para ayudar al resto de departamentos en el proceso de protección de la información mediante la obtención de copias de seguridad, sin embargo, cada departamento debe de ser individualmente responsable de la identificación y protección de todos los registros vitales para una recuperación satisfactoria de la información contenida en equipos departamentales. Para una protección más efectiva, las copias de seguridad deberán almacenarse en un centro externo.

Para una mayor eficiencia en los procesos de copias de seguridad, los propietarios de la información definirán los ciclos de copiado y períodos de retención de dichas copias.

### 5.6.7 Centro de Almacenamiento Externo

Este es uno de los puntos más importantes en la elaboración del plan. Es imprescindible tener las copias de salvaguardia fuera del área de riesgo del C.D.P.

La solución de tener un armario ignífugo en el sótano del edificio o en cualquier otra planta no es admisible. En primer lugar, el armario ignífugo solamente protege contra el incendio y, aún así, durante un tiempo limitado, (usualmente un máximo de 120 minutos). A partir de ahí, la elevación de la temperatura en el interior, producirá el deterioro de los soportes, comúnmente fabricados en plástico. Pero además, el armario ignífugo no protege frente a muchos otros posibles incidentes, como la inundación o cualquier otro que afecte a la accesibilidad del edificio.

Debemos, por tanto, seleccionar el almacenamiento externo en el cual vamos a guardar la información. Existen dos soluciones, la solución propia y la contratación de una empresa de servicios.

#### 5.6.7.1 Solución propia

Es la solución más accesible e inmediata, sin embargo, no se suelen mantener las condiciones de seguridad mínimas exigibles, sobre todo por dejadez y costes. Es una solución cara, si se requiere realizar con un mínimo de garantía, debido a la necesidad de ocupación de un espacio dedicado y acondicionado a la gestión de almacenamiento externo. Si se sumasen estos costes internos, se vería que es una solución cara.

Aparte de todos los inconvenientes, está el más grave, la dejadez. El realizarlo uno mismo hace relajarse en los salvados, en los envíos, y sobre todo en el control de la información almacenada, con lo que se crean archivos vegetativos, y lo que es más grave, muchas veces no se sabe si la información salvada y almacenada es completa.

Si se plantea realizar este servicio de una forma interna a continuación se recomienda una serie de consejos para tener una cámara de almacenamiento en condiciones.

- **Accesibilidad**
  Las 24 horas del día, los 365 días del año.
- **Resistencia al fuego**
  La resistencia al fuego de los muros, paredes, o paneles exteriores de la cámara de seguridad, debe ser de 120 minutos (RF-120), como mínimo.
- **Temperatura controlada**
  Aunque la temperatura en la cual los soportes magnéticos empezarían a sufrir consecuencias irreparables es de 55 grados Celsius, por degradación y mantenimiento se hace necesario mantener la temperatura de 20 grados.
  Ello obliga a sistemas de de acondicionamiento de aire redundantes, con toma de aire fresco externo, con energía eléctrica alternativa y dotados de sensores de alarma y de activación de actuaciones de emergencia, por ejemplo llamadas telefónicas automáticas a personas de servicio de mantenimiento.
- **Humedad controlada**
  Los soportes magnéticos se deterioran a partir de una humedad relativa del aire superior al 85%, pero para un mantenimiento continuo se recomienda una humedad relativa del 50%.

Ello obliga a un control de humedad por el sistema de acondicionamiento de aire descrito anteriormente, dotado también de sensores y activación de alarma.

- **Resistencia al aplastamiento**
  La cámara debe ser capaz de aguantar el derrumbe de las estructuras superiores, con lo cual su construcción resulta cara y compleja.

#### 5.6.7.2 Solución Externa

Existe una gran variedad de oferta en el mercado para este tipo de servicio.

Desde empresas dedicadas exclusivamente al almacenamiento de soportes informáticos hasta las que incluyen este servicio dentro de una gama más variada, como las empresas de gestión de archivos en papel o las de seguridad con actividades de transporte y depósito de valores.

Pero sea cual sea el suministrador seleccionado, por lo que se refiere al servicio de almacenamiento de copias de seguridad, se debe exigir una serie de requisitos adicionales:

Con respecto a las instalaciones:

- Almacén vigilado y conectado a una central de alarmas 24 horas, 365 días al año y dotado con sistemas de seguridad pasiva.
- Sala de almacenamiento de soportes presurizada, evitando así la entrada de polvo, y exenta de campos magnéticos.
- Sistema de extinción de incendios mediante gas inerte.
- Control automatizado de parámetros de: temperatura, humedad, pureza de aire, accesos,…, etc.
- Sistemas de alimentación redundantes.

Con respecto al transporte:

- Vehículos sin distintivos visibles con aire acondicionado para que las condiciones ambientales del transporte sean lo más similares que sea posible a las de la base.
- Transporte en maletines o contenedores.
- Transporte con comunicación con la base (radio, teléfono, buscapersonas, etc.).

Con respecto al servicio:

- Disponibilidad de la información 24 horas del día, 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 y/o posibilidad de peticiones de urgencia con un tiempo de respuesta aceptable (2/3 horas).
- Una cobertura de seguro adecuada.
- Conceptos de facturación claros y cerrados, incluidas la tarifas para servicios de emergencia en horario normal, nocturno, fines de semana, fiestas, etc.

- Confidencialidad de los datos almacenados, ya sea si están almacenados dentro de maletas o contenedores independientes, o directamente en las estanterías o armarios de la base (etiquetas con código de barras, números clave, etc.). es decir, que si, a pesar de las medidas anti-intrusión, alguien consiguiera entrar, no pueda conocer a quién corresponden los soportes.

### 5.6.8 Equipos de recuperación

Los equipos de recuperación son grupos de personas que en encargan de una serie de actividades para conseguir un proceso de recuperación efectivo. Cada equipo está constituido por un jefe, un suplente y un grupo de personas asignadas a él. Un equipo puede constar de una sola persona, y una persona puede pertenecer a más de un equipo, dependiendo de las circunstancias.

Como parte de la estrategia general, es esencial que las responsabilidades principales sean asignadas al equipo adecuado. Las responsabilidades ambiguas o indefinidas suelen generar dificultades, no solamente en la planificación sino, lo que s peor, en las actividades de recuperación.

Por lo general, las responsabilidades de recuperación van en paralelo con las actividades del día a día. Sin embargo, la asignación de responsabilidades puede depender del lugar donde se realice la recuperación, la logística y el tiempo.

En función del tamaño de la organización, y con objeto de clarificar las distintas funciones, se han definido varios equipos a modo de orientación, aunque una misma persona pueda tener varias responsabilidades y pueda realizar varias tareas en uno o varios equipos. El número y funciones de cada equipo deberá ajustarse a las necesidades específicas de la organización.

### 5.6.9 Composición de los Equipos

**Equipo de Gestión de Incidentes**

Este equipo debe estar formado por los jefes de equipo de los equipos restantes, y estar dirigido por una persona con suficiente nivel jerárquico dentro de la estructura de la organización. Sus principales funciones son:

- Planificar y controlar actividades.
- Decidir la ubicación del centro de control.
- Realizar los informes de situación.
- Evaluar los daños.

A lo largo del año se deben planificar reuniones periódicas por parte de este equipo para revisar el plan, y organizar las pruebas.

**Equipo de Operaciones informáticas**

Este equipo será responsable de la rápida y efectiva reimplantación de las instalaciones informáticas después del desastre. Cuando se pide el servicio de recuperación, el suministrador de los servicios de respaldo pondrá a disposición del usuario un conjunto de técnicos que serán capaces de responder a la petición del servicio.

Sus funciones básicas serán:

- Instalación de la solución de recuperación.
- Aviso a la empresa de servicios de respaldo.
- Petición de las copias de seguridad.
- Prueba de la máquina de respaldo.
- Restauración de las comunicaciones locales.
- Restauración de las comunicaciones remotas.
- Obtención de soportes magnéticos nuevos para *backup*, material pre impreso y suministros.
- Recuperación de las copias de seguridad del sistema operativo, programas y datos.
- Restauración del sistema operativo, software de aplicaciones y datos.
- Realizar las pruebas de comprobación de la calidad de las aplicaciones restauradas.

**Equipo de Administración**

La responsabilidad de este equipo es la provisión de recursos a los demás equipos y también:

- La asignación y administración de una caja para gastos de menor cuantía.
- Coordinar la seguridad del edificio con Dirección.
- Relaciones con los servicios públicos.
- Notificación a las compañías de seguros adecuados y relaciones con los peritos.
- Relaciones con el personal y tratamiento de los problemas que se les puedan presentar.
- Relación con los medios de comunicación y edición de notas de prensa.

**Equipo de atención a usuarios**

Si ha de haber cualquier cambio en la secuencia predeterminada de la restauración de la organización, debe ser decidido por este equipo. Este equipo mantendrá informados a todos los demás departamentos usuarios, del progreso realizado, mediante la publicación regular de boletines informativos, actuando como intermediario entre los departamentos usuarios y el proceso de recuperación.

**Equipo de inmuebles**

Este equipo será responsable de la reconstrucción y reacondicionamiento de la sala. Esta tarea puede incluir la coordinación de un cierto número de subcontratistas y suministradores.

Este equipo puede transformarse en un Comité de Dirección para la sustitución de las instalaciones informáticas, incluyendo la construcción de un nuevo edificio, instalación de aire acondicionado y equipos informáticos.

**Equipo de servicios generales**

Este equipo será responsable del soporte de cualquier servicio auxiliar que pueda ser necesario para la completa recuperación de todas las áreas afectadas.

Esta tarea puede incluir la coordinación de un cierto número de subcontratistas y suministradores.

### 5.6.10 Funciones de los Equipos

Cada actividad de este plan está identificada por un número de suceso único y por el equipo responsable de realizarla. Durante una crisis, cada equipo recibirá una lista de acciones a realizar y reportar al coordinador de la Continuidad de Negocio.

### 5.6.11 Plan de Acción

La sección de activación del Plan, documenta la evaluación inicial y actividades de puesta en marcha de equipos y toma de decisiones efectuadas por el Equipo de Gestión de incidentes. Estos procedimientos de activación del plan incluyen la ejecución de los procedimientos apropiados de respuesta ante emergencias, desarrollando el plan de acción y movilizando al personal apropiado.

El aspecto más importante de la continuidad del negocio es la inmediata notificación al responsable apropiado de cualquier suceso que pueda causar una interrupción en las operaciones, con independencia de su dimensión. El enemigo a batir durante una situación de crisis es el paso del tiempo, por ello, las acciones a realizar deben estar perfectamente definidas así como los responsables de llevarlas a cabo y el momento de realizarlas.

Un pequeño fallo de una máquina cuya reparación lleva normalmente unas cuantas horas, puede transformarse en una serie de sucesos que pueden causar interrupciones prolongadas en los servicios, en el sistema y en los usuarios. Por tanto, todo el mundo debe ser consciente de que los desastres pueden evolucionar, además de ocurrir.

Incluso el suceso más insignificante que pueda causar una interrupción en el funcionamiento normal, debe ser comunicados al coordinador del Plan de Continuidad de Negocio o a su suplente.

Tan pronto como reciba la notificación de un incidente, el coordinador del Plan tomará acción según se especifica en la lista de actividades de la gestión del mismo, desencadenando la puesta en marcha de los distintos procedimientos de actuación.

A efectos de fijar la metodología utilizada, estos procedimientos se han clasificado en tres grandes familias, cada una con una denominación genérica.

- *Procedimientos de emergencia.* Son actuaciones inmediatas al incidente que tratan de proteger la integridad de las personas (si está amenazada), atajar la progresión del incidente y pararlo en la medida de lo posible, realizando la correspondiente evaluación de daños.
- *Procedimientos de respuesta.* Son actuaciones de cada departamento o servicio que tienden a sustituir los procedimientos habituales de trabajo por otros alternativos que, aunque no reproduzcan totalmente las funcionalidades de cada departamento o servicio, permiten atender las necesidades más inmediatas y críticas de los mismos.
- *Procedimientos de recuperación.* Normalmente referidos a actividades de los sistemas de información, como son los procedimientos que permiten volver a utilizar datos, aplicaciones, sistemas operativos, etc.

**Definiciones de Desastre**

Para establecer el nivel de plan a seguir en supuesto de un desastre, se observarán las directrices siguientes teniendo en cuenta su gravedad en función del período de interrupción previsto.

Las categorías son las siguientes:

- Desastre menor
- Desastre mayor
- Desastre catastrófico

**Desastre menor**

Se puede definir como desastre menor aquel que *provoca* una *parada que no sobrepase las cuatro horas.* Aunque los márgenes de tiempo deberán ser definidos de acuerdo con las características de la organización.

**Desastre mayor**

Se puede definir como desastre mayor aquel que provoca *una parada de más de cuatro horas y que no sobre pase un día.*

El daño aquí puede ser ligeramente mayor que en el caso anterior, por ejemplo, el causado por la inundación de la sala o rotura del aire acondicionado.

**Desastre catastrófico**

Cuando el servicio vaya a estar fuera de servicio *más de un día y que no sobre pase una semana,* se puede calificar como desastre catastrófico.

### 5.6.12 Activación de Procedimientos de Emergencia

#### 5.6.12.1 Notificación de primera alerta

Dependiendo de la naturaleza del incidente, del día y de la hora, la notificación puede venir de muy diferentes orígenes. La respuesta inicial estará basada en los procedimientos de respuesta de la organización y las prácticas operativas estándar.

Si usted es testigo o es informado de un incidente dentro de la instalación…

1. Ejecute todas las acciones de emergencia apropiadas.
2. Dé parte a seguridad.
3. Informar al equipo de Gestión de Incidentes.
4. El jefe del equipo de Gestión de incidentes decidirá las acciones a tomar, pudiendo convocar al resto de los miembros del equipo para poner en marcha el Plan de Contingencia o permanecer en alerta hasta recibir instrucciones.

*En caso de evacuación del edificio o falla de suministros…*

1. El jefe o suplente de cada equipo de recuperación ejecutará todas las acciones de respuesta de emergencia requeridas.
2. El jefe o suplente de cada equipo de recuperación, deberá presentarse en el Centro de Control tan pronto como la situación lo permita con:
    - Copia de Plan de Contingencia.
    - Tarjeta de identificación personal.
    - Teléfono móvil.

Si la comunicación se produce fuera de horas de trabajo o por escalado del problema, el receptor de la comunicación…

1. Tomará nota de la información cuando le sea notificada la situación e emergencia.
2. Si es jefe o suplente de un equipo de recuperación, se presentará en el Centro de Control tan pronto como la situación lo permita con:
    - Copia del Plan de Contingencia.
    - Tarjeta de identificación personal.
    - Teléfono móvil.

#### 6.6.12.2 Escalado de problemas

Un aspecto crítico en la recuperación de desastres es la inmediata notificación al personal apropiado, para que las operaciones de detención de la emergencia, o el activado del Plan de Acción, sean iniciadas lo antes posible.

Los objetivos de esta actividad son:

- Determinar QUIÉN debe ejecutar la acción.
- Determinar el TIEMPO MÁXIMO permitido para la ejecución de la acción.
- En caso de no tener éxito en la acción, determinar QUIËN debe ser avisado a continuación para hacerse cargo del problema y de su resolución.
- Si el tiempo pasa y las acciones de resolución del problema no tienen éxito, determinar en qué nivel de gravedad se encuentra la organización, por medio de un sistema de graduación de alertas.

Resumiendo, la Guía de Escalado del Problema pretende evitar que una emergencia menor pueda llegar a convertirse en un desastre:

- Tardando demasiado tiempo en solucionarla.
- No informando a niveles superiores, para que aporten su experiencia, autoridad, o medios extraordinarios, en la solución.

### 5.6.13 Responsabilidad

Una emergencia debe ser tratada en su origen por:

- Personal designado para ello en el Plan de Acción.
- Personal no designado pero entrenado, o informado de los procedimientos de notificación.
- Si no hay nadie de los anteriores, cualquier persona que se encuentre con el problema.

### 5.6.14 Acciones A Ejecutar

Esta persona deberá:

- Detenerlo y solucionarlo si es su responsabilidad.
- Si no es su responsabilidad, intentar detenerlo y solucionarlo si lo cree posible y no puede causar daños mayores o correr riesgos innecesarios.
- Informar A LA MAYOR BREVEDAD, al personal implicado en el Plan de Acción, y si no lo conoce, a sus superiores o departamento de seguridad.

### 5.6.15 Tiempo

En la detección del problema y la activación de medidas resolutorias son piezas fundamentales:

- El conocimiento y el entrenamiento en las acciones a realizar.
- El tiempo MÁXIMO a invertir en ellas.
- En las guías de escalado que se acompañan, se ha asignado un tiempo máximo de realización para cada tarea. Este tiempo, deberá ser objeto de revisión continua a los largo de la vida del Plan de acción y se modificará como consecuencia del entrenamiento, de las pruebas y de la inclusión/ supresión/ modificación de acciones.

### 5.6.16 Notificaciones

Uno de los aspectos peor resueltos de los planes de contingencia, está referido a la notificación:

- A QUIÉN notificar.
- CUÁNDO notificar.
- CÓMO notificar.
- DÓNDE y CUÁNDO celebrar la primera reunión.

## 5.7 Procedimientos de respuesta

El propósito de la fase de respuesta ante emergencias es desarrollar e implementar procedimientos para responder y estabilizar la situación después de un incidente y administrar el centro de operaciones de emergencia a ser utilizado como “centro de mando”.

Para cumplir con este propósito es necesario que:

- Identifique componentes de los procedimientos de respuesta a emergencia.
- Especifique los procedimientos de respuesta a emergencia.
- Identifique requerimientos de control y autoridad.
- Procedimientos de control y autoridad.
- Respuesta a emergencia y recuperación de heridos.
- Seguridad y recuperación.

Los procedimientos de respuesta pueden ser activados muy rápidamente, pero usualmente son solo medidas de emergencia y, por lo general, no son suficientes para las operaciones del negocio a más largo plazo. Por ejemplo, un procedimiento común de respuesta es desviar las llamadas de los clientes esenciales a un ligar alternativo, para dar una respuesta por el altercado.

## 5.8 Concientización y Entrenamiento para BCP

Toda organización que quiera posicionarse en el mercado y estar preparada a cambios en su entorno, requiere de un constante proceso de evolución. Este proceso genera en la mayoría de los casos, cambios al interior de la organización. Siempre que se generan estos cambios existe un porcentaje de resistencia al cambio relacionado con el personal que interviene en dicho proceso.

Es necesario que la organización prepare a su personal ante la presencia de un cambio, logrando minimizar esa resistencia y obteniendo mejor disposición ante situaciones de este tipo creando una cultura de aceptación ante un evento que perturbe su labor.

Son estos algunos motivos por los cuales se presenta en la gestión de continuidad de negocio una fase en la cual se trata la concientización y el entrenamiento del BCP y su relación con la implementación, mantenimiento, gestión y ejecución del mismo. Este proceso de conciencia es necesario que se realice en toda la organización logrando aumentar la resistencia ante los riesgos.

Para lograr una concientización y entrenamiento es necesario:

- Definir objetivos de concientización y entrenamiento.
- Desarrollar e implementar varios tipos de programas de entrenamiento.
- Desarrollar programas de concientización.
- Identificar otras oportunidades de educación

## 5.9 Mantenimiento y Ejercicio del BCP

Una vez que se han realizado, desarrollado e implementado estrategias de y/o planes, con el objetivo de su utilización ante una situación de interrupción de actividades y las cuales contribuirán al proceso de normalización ante una situación de crisis, es necesario realizar pruebas para determinar la eficacia con la que puede continuar el negocio ante la presencia de una posible interrupción. Así mismo se puede evaluar el equipo y personal a cargo de cada actividad crítica.

Los propósitos de realizar el ejercicio son: 1. Evaluar y permitir el continuo mejoramiento del BCP en la organización logrando una recuperación prioritaria de las actividades críticas de acuerdo con los objetivos de puntos de recuperación asegurando un nivel mínimo de continuidad de negocio. 2. Permite evaluar y mejorar la capacidad de competencia ante la gestión de crisis.

Con la realización del ejercicio se pueden determinar varios aspectos, entre los cuales se encuentran:

- Identificar el nivel de madurez del BCP de la organización.
- Verificación y validación que la continuidad de negocio y la gestión de crisis y estrategias son variables, efectivas, actualizadas y ajustadas al proceso.
- Verificación y validación que los miembros y personal se familiarizan con el entendimiento de roles, responsabilidades y autoridades en la operación de la continuidad de negocio y proceso de administración de crisis.
- La formación de conciencia involucrando individuos usando la continuidad de negocio y los planes de gestión de crisis.
- El ensayo y familiarización de los miembros del equipo y personal con sus roles, responsabilidad y autoridad en la operación de continuidad de negocio y planes de gestión de crisis.
- Probar la organización e infraestructura de la gestión de continuidad de negocio y planes de gestión de crisis.
- El ensayo de la disponibilidad y traslado del personal.

- Verificación y validación que el BCP refleja las actuales prioridades del negocio.
- Documentar resultados.
- Incrementar la cultura de los procedimientos de conciencia.
- La oportunidad de identificar defectos y mejorías de la organización del BCP, administración de crisis y planes de continuidad de negocio.
- Documentación y evaluación del ejercicio.

Para lograr estos resultados es necesario seguir un proceso en la elaboración de una prueba. Principalmente es necesario establecer directores de cada área de organización, luego se planificarán los escenarios en los cuales se van a llevar a cabo las pruebas. Estas pruebas deben tener un grupo de administración, logística, recursos, listas de verificación, estructura. Posteriormente al haber planificado se harán las consideraciones del programa, se documentará el ejercicio junto con la información de los participantes, se procederá a la realización del ejercicio luego se evaluará y se hará un análisis de los resultados con el objetivo de tenerlos en cuenta en pruebas posteriores junto con sus recomendaciones.

### 5.9.1 Mantenimiento

El proceso de gestión de continuidad de negocio no finaliza con la realización del documento en el cual se plasman estrategias y se asignan roles o equipos de trabajo a las áreas organizacionales; es quizás el proceso de mantenimiento del plan un punto importante si se quiere hacer uso de este considerando que el negocio continúa y está en constante cambio.´

El propósito de este proceso de mantenimiento es asegurar que la gestión de continuidad del negocio incluyendo la gestión de crisis permanezca efectivo, con el objetivo de ser capaz de lograr la recuperación de actividades de misión crítica y sus dependencias dentro de los objetivos de tiempo de recuperación y los objetivos de punto de recuperación asegurando una continuidad de sus servicios y productos.

Con la realización del mantenimiento del BCP podremos obtener:

- Pruebas definidas y documentadas para la gestión y gobierno pro activo del programa de mantenimiento y monitoreo del BCM respecto a actividades de misión critica y sus dependencias.
- Detalles de todos los cambios de estrategias del BCP y planes de continuidad de negocio documentados con toda la historia de estrategias y detalles de control de versiones.
- Verificación y validación de políticas, estrategias y planes BCP.
- Identificación e inclusión de cambios en los sistemas y proceso de la organización.
- Identificación e inclusión de cambios en legislación y regulación para la industria.
- Verificación y validación de análisis de impacto y de riesgos basados en las estrategias y planes BCP.

Los resultados que se obtendrán con el proceso de mantenimiento son de gran utilidad para la organización, reviniendo que los documentos realizados queden obsoletos con el paso de los años. Para realizarlo es necesario tener una clara definición y documentación del programa de mantenimiento y monitoreo, incluyendo políticas, marcos y procesos así como la estrategia de negocio operacional.

Para la realización de cualquier plan es necesario tener en cuenta la legislación existente, para tener una base y cumplir con la normatividad que se exige.

El proceso de mantenimiento requiere de un subconjunto de procesos auditoria ejercicio y aseguramiento que permiten su fortalecimiento, capacidad de continuidad y soporte a la gestión de continuidad de negocio en su aplicación a la organización cuando lo requiera.

### 5.9.2 Auditoría

Luego de haber realizado los procesos de ejercicio y mantenimiento sigue un proceso de auditoría que se hace necesaria en cualquier proceso al interior de la organización. El propósito de la auditoria en la gestión de continuidad de negocio es revisar los estándares del BCP identificando defectos y dificultades, proporcionando recomendaciones de acuerdo a estándares predefinidos.

La auditoria revisara varios aspectos en la organización algunos de ellos son:

- Resistencia (aplicación de planes y estrategias en crisis).
- Políticas, estrategias, marcos y planes continúa bajo presión de acuerdo a estrategias, prioridades y objetivos.
- Políticas, estrategias, marcos y planes continúa bajo presión de acuerdo a las directrices de buenas prácticas.
- El BCP es competente de acuerdo al propósito.
- Los planes y soluciones son efectivos y actualizados de acuerdo al propósito.
- Implementa sus programas.
- Documenta el control, procesos y procedimientos operando efectivamente.

En la realización de la auditoría como en cualquier proceso existen componentes como son: definición y documentación del programa de auditoría, auditar el plan de auditoría, buscar expertos internos y externos, aplicar los estándares de auditoría, actualizar estrategias del BCP, tener en las normas de requerimientos, legislación, directrices de buenas prácticas, estándares, realizar programas de conciencia y formación, actualizar análisis de impacto, estrategias y planes a ser auditados.

Para poder obtener estos resultados el proceso de auditoría debe seguir métodos y/o técnicas que optimicen este proceso. Algunas técnicas y/o metodologías que se nombran son: Auto evaluación, auditoría forense, cumplimiento de auditoría, diligencia auditoria, viabilidad de auditoría, control de auditoría, mejor valor auditado. Con el seguimiento de estas técnicas y la ayuda de los responsables, el proceso de auditoría podrá cumplir su propósito y así dar un informe para la organización en el cual se presenten los resultados de los procesos auditados.

Luego de haber realizado el proceso de auditoría la organización tendrá definido y documentado este proceso y se preparara para realizar un plan de acción y un programa de monitoreo.

# 6. Sistema de Comando de Incidentes

El sistema de comando de incidentes (**ICS**) es un modelo de gestión desarrollado para comando, control y coordinación de la respuesta a una situación de emergencia y su objetivo es estabilizar el incidente y proteger la vida, las propiedades y el ambiente.

La compleja gestión de un incidente y la creciente necesidad de acciones de varios grupos de actuación hacen indispensable que exista un único sistema de gestión que sirva de guía para todos. Los principios del **ICS** permiten que diferentes grupos desarrollen actividades conjuntas con elementos comunes: comando unificado, planes de acción, terminología, administración, recursos humanos y materiales, flexibilidad organizacional, conceptos de seguridad, procedimientos estandarizados, etc.

La flexibilidad del **ICS** permite ampliar o restringir la gestión de acuerdo con las diferentes necesidades, lo que posibilita lograr un sistema eficiente.

El sistema fue probado y validado en respuesta a todos los tipos de incidentes y situaciones de no-emergencia, como por ejemplo: emergencias con productos peligrosos, accidentes con un gran número de víctimas, eventos planificados (celebraciones, desfiles militares, conciertos, etc.), catástrofes, incendios, misiones de búsqueda y salvamento, programas de vacunación masiva, etc.

El SCI fue desarrollado en la década de los setenta en respuesta a una seria de grandes incendios forestales en el sur de California (E.U. A.). El daño a las propiedades ascendió a millones y muchas personas murieron o resultaron heridas. En este periodo se reunieron las autoridades del municipio, organismos estatales y federales involucradas en la lucha contra incendios, para formar el Firescope (Firefighting resources of California organized for Potential Emergencies-Recursos contra incendios de California organizados para emergencias potenciales). Esta unidad identificó problemas que pueden suscitarse cuando participan en una misma misión distintos grupos, como:

- Falta de estandarización de la terminología utilizada.
- Falta de capacidad de ampliar y restringir la estructura de gestión del incidente.
- Ausencia de estandarización e integración en los medios de comunicación.
- Ausencia de planes de acción consolidados.

Los esfuerzos para resolver estas dificultades conllevaron al desarrollo del modelo original de ICS para gestión de incidentes, sin embargo, el sistema inicialmente concebido para combatir incendio forestales, evolucionó hasta llegar a ser un sistema aplicable a cualquier tipo de emergencia, sea o no incendio.
Un gran éxito del ICS es producto de la aplicación directa de:

- Una estructura organizacional común.
- Principios de gestión estandarizados.

El uso del ICS es ordenado por el Sistema Nacional de Gestión de Incidentes (National Incident Management System, NIMS). El NIMS proporciona un enfoque proactivo y sistemático que guía a los departamentos y a las agencias de gobierno, del sector privado y de organizaciones son gubernamentales para que trabajen de manera integral cuando se preparen para, eviten,

respondan a, se recuperen de y mitiguen los efectos de los incidentes, sin importar la causa, el tamaño, la ubicación o la complejidad, con el fin de reducir la pérdida de vidas y de propiedades, así como el daño al medio ambiente.

Sin el ICS, las respuestas a los incidentes generalmente dan como resultado:

- Falta de responsabilidad, incluyendo cadenas de comando y supervisión poco claras.
- Mala comunicación debida tanto a los usos ineficientes de los sistemas de comunicaciones disponibles como a los códigos y la terminología problemáticos.
- No existe una estructura de administración común flexible, prediseñada que permita que los comandantes deleguen responsabilidades y administren las cargas de trabajo de una manera eficiente.
- No existen métodos predefinidos para integrar los requisitos entre agencias en la estructura de administración y en el proceso de planeación de una manera efectiva.

Utilizar el ICS nos permite evitar debilidades en todos los tipos de respuestas a incidentes. Al usar las mejores prácticas de administración, el ICS ayuda a garantizar:

- La seguridad del personal de respuesta, el cuerpo docente, los trabajadores y otros.
- El éxito de los objetivos de la respuesta.
- El uso eficiente de los recursos.

## 6.1 Organización del ICS

En todo incidente o evento, se deberán ejecutar ciertas actividades y acciones de administración. Siempre se realizarán actividades administrativas, inclusive de manera inconsciente, independientemente del alcance del accidente, aún con sólo dos o tres personas involucradas en la operación.

La organización del ICS está formada por cinco sectores funcionales:

- Comando
- Operaciones
- Planificación
- Logística
- Finanzas

El siguiente diagrama indica la relación entre estos sectores:

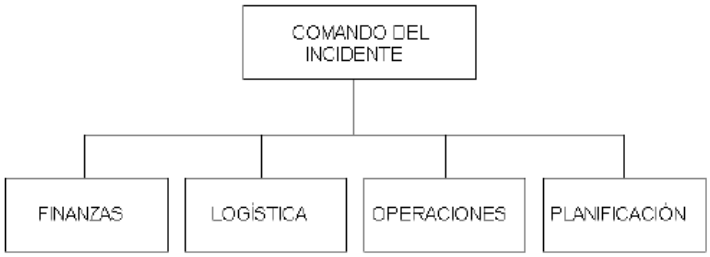


**Figura 6.1.- Diagrama de Sistema de Comando de Incidentes**

Estos cinco componentes principales son la base del desarrollo de la organización de ICS. Estos se aplican durante una pequeña emergencia o un incidente de gran escala.

Estos incidentes de pequeña escala, una sola persona, el comandante del incidente (CI), puede administrar todos los componentes. Los accidentes de gran escala, en cambio, requieren que cada componente o sector tenga un responsable administrativo que responda al CI. Por ello, cada uno de estos sectores primarios de ICS, con excepción del comando de incidentes, se puede dividir en funciones secundarias según la necesidad.

La organización del ICS se puede ampliar o restringir para satisfacer las necesidades del incidente pero todos los incidentes independientemente de su dimensión o complejidad, deberán nombrar un comandante del incidente, en un ICS básico cuando CI debe alejarse del puesto de comando (PC) para realizar una operación o supervisión en el lugar del incidente, el cargo de CI deberá transferirse a otra persona.

## 6.2 Funciones del comando

La función de comando está dirigida por el comandante del incidente (CI), que es la persona técnicamente calificada para asumir la responsabilidad y gestión global del incidente. Las principales responsabilidades del CI incluyen:

- Ejecutar la actividad de comando y establecer el lugar del puesto de comando.
- Proteger las vidas, propiedades y el ambiente.
- Controlar los recursos humanos y materiales.
- Establecer y mantener contacto con otros grupos de actuación e instituciones.

En relación con la administración del incidente.

- Recopilar y analizar los datos sobre el incidente.
- Estructurar el plan de alerta y desarrollar acciones prioritarias.
- Aprobar las solicitudes de recursos adicionales.
- Mantener contacto con los coordinadores del sector.
- Establecer el comando.
- Establecer el sistema de seguridad.
- Evaluar las prioridades del incidente.
- Determinar los objetivos operacionales.
- Desarrollar e implementar el plan de acción del incidente.
- Desarrollar una estructura organizacional apropiada.
- Nombrar y supervisar a los coordinadores de los diversos sectores.
- Mantener el control global de la situación.
- Administrar los recursos del incidente.
- Coordinar las actividades de emergencia.
- Coordinar las actividades de los otros grupos.
- Autorizar a los medios en la divulgación de información.
- Controlar los costos implicados.

Un CI eficaz debe ser seguro, decidido, positivo, objetivo, tranquilo y tener raciocinio rápido. Para dirigir todas las responsabilidades que demanda esta función, el CI también debe ser flexible, adaptable y realista en relación con sus propias limitaciones. Además, el CI debe saber cuándo y a quién delegar funciones, en caso necesario durante el desarrollo de las actividades en el incidente.

Inicialmente, la primera persona calificada para llegar al lugar del incidente, deberá asumir el papel de comandante del incidente y establecer el control de la situación hasta la llegada del CI nombrado, quien pasará a tener el control total del incidente.

A medida que los incidentes evolucionan o se hacen más complejos con la participación de autoridades de diferentes jurisdicciones o acciones conjuntas de varios grupos de respuesta, se podrá asignar un CI más calificado. En el cambio de comando, el CI que deja el cargo debe dar instrucciones detalladas al nuevo CI y notificar el cambio de cargo a todo el personal involucrado.

### 6.2.1 Asesoría del comando

Para un incidente de gran escala o complejo, se establecen algunos supuestos de asesoría para auxiliar al comandante del incidente en el cumplimiento de las responsabilidades directamente asociadas con la administración del incidente. Los asesores dirigen funciones claves, lo que permite que el CI tenga más libertad para concentrarse en la administración global del incidente. El personal de asesoría no forma parte de la organización establecida, es decir, de la función de comando.

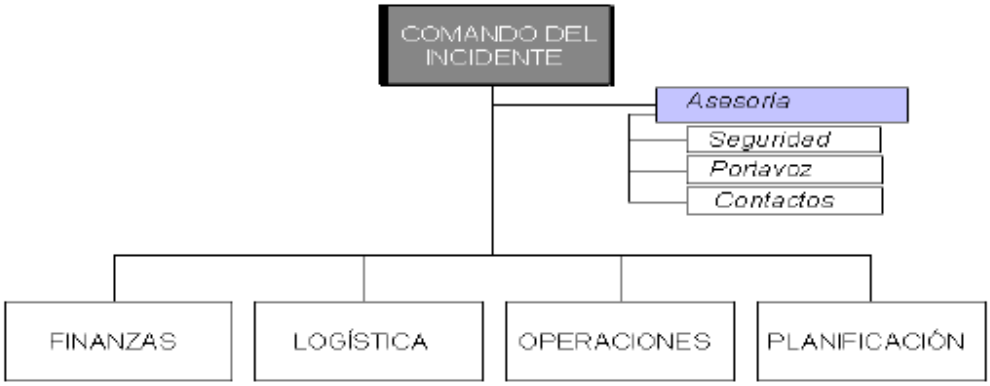


**Figura 6.2.- Diagrama de Asesoría del Comando de Incidentes**

**Seguridad**

Título: Supervisor de Seguridad

Objetivo: Garantizar la seguridad general de las operaciones y monitorear las medidas de seguridad en las que participan los equipos, las víctimas y el público en general.

Funciones:

- Actuar bajo la orientación del CI.
- Utilizar su autoridad, en casos de emergencias, para interrumpir cualquier actividad considerada insegura, cuando sea necesario adoptar una medida inmediata.
- Identificar, monitorear y evaluar situaciones de riesgo relacionadas con el incidente.
- Responsabilizarse por la seguridad de los integrantes de los equipos de respuesta.
- Determinar el aislamiento del área involucrada en el incidente.
- Documentar todas las ocurrencias sospechosas.
- Mantener registros formales.

**Portavoz**

Título: Portavoz

Objetivo: Gestionar la divulgación de la información sobre el desempeño de las operaciones a las autoridades y la prensa, bajo la estricta coordinación del CI.

Funciones:

- Actuar bajo la orientación del CI.
- Responsabilizarse por transmitir información a la prensa y otros organismos involucrados en las operaciones.
- Establecer un único centro de información sobre el incidente, siempre que sea posible.
- Organizar el lugar de trabajo, materiales, teléfono y personal necesario.
- Obtener la autorización del CI para divulgar la información.
- Mantener registros formales.

**Contactos**

Título: Contactos oficiales.

Objetivo: Efectuar, de ser necesario, contactos con organismos oficiales, otros equipos de atención y profesionales especializados.

Funciones:

- Actuar bajo la orientación del CI.
- Prever contactos con organismos oficiales, como el cuerpo de bomberos, defensa civil, policía militar, etc.
- Identificar y localizar al representante de un organismo específico, de ser necesario.
- Prever contactos con profesionales y servicios especializados.
- Mantener una lista de nombres, teléfonos y direcciones de personas y entidades claves.
- Mantener registros formales.

El CI tomará la decisión de ampliar o restringir la estructura de la organización del ICS con base en tres puntos principales:

1. Seguridad de la vida: La principal prioridad del CI debe ser la seguridad de la vida de todos los involucrados.

2. Estabilidad del incidente: El CI es responsable de determinar la estrategia que permitirá:

- Minimizar el efecto que podrá causar el incidente.
- Maximizar el esfuerzo en relación con la rapidez de respuesta y el uso eficaz de los recursos.

El tamaño y complejidad de la estructura del ICS que desarrolla el CI se debe basar más bien en la complejidad del incidente (nivel de dificultad en la respuesta) y no en el tamaño (área geográfica o cantidad de recursos).

Los recursos humanos y materiales disponibles se deberán administrar racionalmente, es decir, usar sólo los recursos estrictamente requeridos para una determinada tarea y dejar los demás disponibles para cuando sean necesarios.

3. Preservación del ambiente: El CI se responsabiliza por minimizar el daño a la propiedad y al ambiente mientras se alcanzan los objetivos del plan de acción.

## 6.3 Sector Finanzas

Por lo general, el sector de finanzas sólo se establece durante incidentes o eventos de gran escala. Se encarga del suministro y administración de todos los recursos financieros relacionados con el incidente, así como de proporcionar al comandante una planificación financiera y administrar toda la documentación fiscal exigida por la ley.

- Actúa bajo la orientación del CI.
- Selecciona y nombra a los jefes de cada equipo del sector.
- Supervisa las acciones de cada equipo del sector.
- Mantiene los registros formales.

## 6.4 Sector Logística

El sector de logística se responsabiliza por el suministro de los recursos materiales necesarios para las actividades durante el incidente. Incluye las responsabilidades por el transporte, alimentación, alojamiento, control, disponibilidad y mantenimiento de los equipos usados. El coordinador del sector de logística también se responsabiliza por instalar y mantener el funcionamiento de un sistema de comunicación adecuado para cada situación.

- Actúa bajo la orientación del CI.

- Proporciona condiciones adecuadas de actuación para los diversos equipos en relación con el material necesario.
- Selecciona y nombra a los jefes de cada equipo dentro del sector.
- Supervisa las acciones de cada equipo dentro del sector.
- Crea la infraestructura necesaria para la logística.
- Efectúa las solicitudes de adquisición al CI de artículos no disponibles.
- Coordina con el personal encargado de organizar equipos, alimentación, medicamentos, transporte y alojamientos.
- Prevé las necesidades de materiales para los equipos.
- Mantiene registros formales.

## 6.5 Sector de Operaciones

El sector de operaciones se responsabiliza por realizar las actividades descritas en el plan de acción. El coordinador del sector de operaciones administra todas las actividades del sector y tiene la responsabilidad primaria de recibir, desarrollar e implementar el plan de acción.

El coordinador del sector de operaciones se reporta directamente al CI y determina la estructura organizacional y los recursos necesarios dentro del sector. Las responsabilidades principales del coordinador son:

- Dirigir y coordinar todas las operaciones y garantizar la seguridad de todos los involucrados.
- Asistir al CI en el desarrollo de las metas y en la elaboración del plan de acción del incidente.
- Implementar el plan de acción.
- Solicitar recursos al comandante del incidente (CI).
- Mantener al CI informado sobre el desarrollo de las actividades dentro del sector.
- Actuar bajo la orientación del CI.
- Actuar conjuntamente con el sector de planificación.
- Supervisar y ejecutar todas las operaciones técnicas necesarias para realizar las operaciones de respuesta.
- Coordinar y planificar la ejecución de las tareas.
- Orientar los pedidos de recursos adicionales al CI.
- Seleccionar y nombrar a los jefes de cada equipo dentro del sector.
- Someter cada tarea a la aprobación del CI.
- Supervisar las operaciones.
- Mantener registros formales.

## 6.6 Sector de Planificación

En eventos de menor escala, el comandante del incidente se responsabiliza por efectuar la planificación pero en incidentes de gran escala, el CI establece el sector de planificación.

La función del sector de planificación es recopilar, evaluar y diseminar la información necesaria para la preparación del plan de acción y cualquier otro tipo de información que podrá ser útil durante el evento.

El coordinador del sector de planificación colabora efectivamente con el CI en la elaboración del plan de acción del incidente. Es responsable de prever el probable curso del incidente y preparar planes alternativos para los posibles cambios del plan de acción principal.

Las principales responsabilidades del coordinador son:

- Actuar bajo la orientación del CI.
- Actuar conjuntamente con los coordinadores de los demás sectores.
- Solicitar recursos adicionales al CI.
- Seleccionar y nombrar a los jefes de cada equipo dentro de sector.
- Supervisar las acciones de los equipos dentro del sector.
- Organizar la gestión de la documentación e información.
- Mantener registros formales

# Conclusiones

- ✓ No es necesario realizar todas las fases del Plan de Continuidad de Negocio (BCP), ya que éstas serán realizadas dependiendo la necesidad y actividad de la organización.
- ✓ Uno de los puntos iniciales y más importantes para realizar el BCP es conocer y entender detalladamente el negocio o actividad al que se dedica la organización, para así obtener como resultado un Plan óptimo.
- ✓ El desarrollo del BCP tiene en cuenta el análisis de todos los recursos (humanos, económicos, tecnológicos, infraestructura, legales, etc.).
- ✓ Hay que tomar en cuenta que una amenaza nunca va a desaparecer, siempre estará presente en todos los procesos de una organización. Sin embargo, día a día se desarrollan técnicas que permiten, en poco tiempo, mitigar el impacto que generan estas amenazas.
- ✓ Uno de los primeros pasos para llevar a cabo la implementación de un BCP es la definición de equipos así como los coordinadores de los mismos, cada uno con sus responsabilidades y roles relacionados con cada fase del BCP
- ✓ La fase de evaluación de riesgos, permite a la organización identificar, analizar y evaluar amenazas internas y externas que representan riesgos principalmente a las actividades críticas de la organización.
- ✓ El impacto que genera una interrupción debe ser cualificado y cuantificado permitiendo que la empresa esté preparada económica y operacionalmente brindando estabilidad a su negocio.
- ✓ Para estar seguros de la funcionalidad de un Plan es necesario que se desarrollen pruebas, mantenimiento y actualizaciones.

- ✓ Es importante la actualización del BCP cuando se presentan cambios en la organización; además esta actualización debe hacerse una vez al año.

# Referencias


1. Administración de Riesgo, FAC-UNAM, 2009
2. Análisis de Incertidumbre y Riesgo, Ley Borrás, Roberto. Comunidad Morelos, México. 2004
3. BCP: Es momento de asegurar la continuidad de negocio, KPMG.
4. Cómo hacer un BIA, la base fundamental de BCP, Carvajal, Armando. Globalteksecurity
5. Con los ejercicios de recuperación ante desastres no se alcanza la línea de llegada. Artículo, Forrester. 2011
6. DRP y BCP: Continuidad Operativa, Security Advisor. 2010
7. El Plan de Continuidad de Negocio, Gaspar Martínez, Juan
8. Guía de Administración de Riesgo, Departamento Administrativo de la Función Pública, Rep. De Colombia.
9. Introducción al Sistema de Comando de Incidentes (ICS100), Curso FEMA, 2010
10. La guía fundamental para la recuperación de desastres: Cómo garantizar la continuidad en equipos Informáticos y actividades comerciales.
11. Ley General de Protección Civil, México. 2012
12. Métodos de Análisis de Riesgos, seminarios de Ingeniería Química, UNAM.
13. Norma NFPA-1600 “Planes de Emergencia/ Desastres y Continuidad de Negocios”. 2010
14. Plan de Contingencia y Emergencias, SNPAD, República de Colombia.
15. Sistema de Comando de Incidentes, Instituto Internacional de Administración de Riesgo.
16. Taller de Administración de Riesgos, Domínguez Betancourt, Ramón