

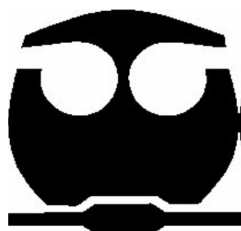


UNIVERSIDAD NACIONAL AUTÓNOMA DE
MEXICO

FACULTAD DE QUÍMICA

MANEJO DE DESASTRES Y EMERGENCIA
Y PROGRAMAS DE CONTINUIDAD DE NEGOCIO
EN LA INGENIERÍA QUÍMICA

T E S I S
QUE PARA OBTENER EL TÍTULO DE
INGENIERA QUÍMICA
P R E S E N T A
DULCE MARIA HERNANDEZ BARRERA



MÉXICO, D.F.

2012



Universidad Nacional
Autónoma de México

Dirección General de Bibliotecas de la UNAM

Biblioteca Central



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.



JURADO ASIGNADO:

PRESIDENTE: Prof. Ramón E. Domínguez Betancourt
VOCAL: Prof. Mirna Rosa Estrada Yañez
SECRETARIO: Prof. Héctor Marcelino Gómez Velasco
1er. SUPLENTE: Prof. Alejandro Zanelli Trejo
2do SUPLENTE: Prof. Héctor Israel Basave Rivera

SITIO DONDE SE DESARROLLÓ EL TEMA:
INSTITUTO NACIONAL DE CONTROL TOTAL DE PÉRDIDAS

ASESOR:

Ing. Ramón E. Domínguez Betancourt

SUSTENTANTE: Dulce María Hernández Barrera



Dedicado

A mi mamá Tereza Barrera Ayala que es el motor de mi vida y que siempre has estado a mi lado para brindarme las palabras necesarias para no rendirme cada vez que me sentía derrotada. Gracias por tu amor, comprensión y esfuerzo, por que por ti soy la mujer en la que me he convertido.



Agradecimientos

A mi madrina Rosa María Barrera Ayala que ha estado al pendiente de mí como una madre, gracias por tus consejos y apoyo durante toda mi vida de estudiante.

A mis tíos Fernando y Saúl Barrera Ayala, por que siempre compartieron sus conocimientos conmigo cuando más lo necesitaba.

A la memoria de mi tío Antonio Barrera Ayala por que gracias a ti ame las ciencias exactas.

A todos mis tíos y tías que me abrieron las puertas de su apoyo siempre que lo necesite

A mi abuelita Esperanza Ayala Aparicio y a la memoria de mi abuelito Isidro Barrera García, por que siempre vieron por mi como una hija y estuvieron a mi lado brindándome su amor y consejos.

Al amor de mi vida Ramón Pacheco Hernández, gracias por aguantarme cada final de semestre y hacer que confiará más en mí.



A mis amigos Laura, Andrés y Joao por la amistad que nos une desde hace muchos años

A mis amigos de la facultad Maribel, Baruch, Juan, Paulina y Monica por su apoyo desinteresado en cada momento de estudio y que de alguna forma cooperaron con algo de si mismos.

A mis compañeras y amigas de trabajo Isabel y Esperanza por que mantuvieron en mi la llama de la perseverancia.

A mi asesor el Ing. Ramón Domínguez Betancourt que me impulso con sus conocimientos y consejos para alcanzar mi objetivo.

A mi profesor el Ing. Alejandro Villalobos Hiriart que con su enseñanza despertó y mantuvo en mí el amor y entusiasmo a la ingeniería química.

Q. Carlos Olvera Bermúdez que me ayudo en cada momento de estudio, compartiendo su tiempo y conocimientos para poder salir adelante.

A mí amada UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO (UNAM) que me vio crecer desde que era un cachorro hasta el día de hoy que soy un puma.



ÍNDICE

INTRODUCCIÓN	1
OBJETIVOS	3
HIPOTESIS	4
CAPITULO 1 ANTECEDENTES	5
CAPITULO 2 ¿QUÉS ES RIESGO?	9
2.1 Riesgo Telúrico	10
2.1.1 Sismicidad	11
2.1.2 Tsunamis	13
2.1.3 Vulcanismo	13
2.1.4 Movimientos de laderas y suelos	14
2.2 Riesgos Hidrometeorológicos	15
2.2.1 Precipitaciones Pluviales	15
2.2.2 Inundaciones	15
2.2.3 Heladas	17
2.2.4 Huracanes	19
2.2.5 Sequías	21
2.3 Riesgos Humanos	23
2.3.1 Terrorismo	23
2.3.2 Sabotaje	26
CAPITULO 3 LEY GENERAL DE PROTECCIÓN CIVIL	28
4.1 Disposiciones Generales	28
4.2 Del Sistema Nacional	31
4.3 Del Consejo Nacional	32
4.4 De los Grupos Voluntarios	33
4.5 Del Programa Nacional	34
4.6 De las Declaratorias de Emergencia y de Desastre	34
4.7 De las Medidas de Seguridad	35



CAPÍTULO 4 ADMINISTRACIÓN DE RIESGOS	36
4.1 Administración y Planeación de Riesgos	36
4.2 Identificación de Riesgo	40
4.3 PASST (Programa de Autogestión en Seguridad y Salud en el Trabajo).....	48
4.3.1 Breve Historia	48
4.3.2 Estructura del Programa	49
4.3.3 Planeación y Diagnostico.....	48
4.3.4 Compromiso en la autogestión	52
4.3.5 Evaluación del Sistema de Administración en Seguridad y Salud en el Trabajo	54
4.3.6 Restricciones del Programa.....	60
CAPITULO 5 ANÁLISIS DE RIESGO Y EMERGENCIAS.....	62
5.1 Análisis Cualitativo	62
5.1.1 Entradas para el Análisis Cualitativo de los Riesgos	63
5.1.2 Técnicas para el Análisis Cualitativo de los Riesgos	63
5.1.3 Clasificación global del riesgo.....	66
5.2 Análisis Cuantitativo.....	66
5.2.1 Entradas para el Análisis Cualitativo de los Riesgos	67
5.2.2 Técnicas para el Análisis Cualitativo de los Riesgos	67
5.3 Planificación de la Respuesta en Riesgos	73
5.3.1 Técnicas para el Análisis Cualitativo de los Riesgos	74
5.3.2 Resultados de la Planificación de la Respuesta Frente al Riesgo.....	75
5.4 Plan de Respuesta de Emergencia.....	77
5.4.1 Implantación del Plan de emergencia.....	78
5.5 Monitores y Control de los Riesgos.....	82
5.5.1 Estrategias de Monitoreo y Control de los Riesgos	83



CAPITULO 6 PLAN DE ADMINISTRACIÓN DE INCIDENTES	85
6.1 National Incident Magement System (NIMS)	85
6.1.1 Funciones y Organización	86
6.1.2 Preparación para Funciones	88
6.1.3 Protocolos de Planeación y Comunicación	89
6.1.4 Descripción de los Recursos	92
6.1.5 Conceptos y Principios	92
6.1.6 Sistemas de Gestión de la Información	93
6.1.7 Gestión de los Recursos	94
6.1.8 Comando y Gestión de Incidentes	99
6.2 Occupational Health and Safety Assessment Series(OHSAS) 18001 ³²	104
6.2.1 Requisitos del sistema de gestión de la SST.....	104
6.2.2 Planificación y Desarrollo del sistema de gestión de la SST	106
6.2.3 Determinar la Necesidad de Controles.....	107
6.2.4 Iniciar una Auditoría.....	108
6.2.5 Realizar las revisiones de los documentos.....	109
CAPITULO 7 EL PLAN DE CONTINUIDAD DE NEGOCIO	111
7.1 Iniciación del Plan de Continuidad de Negocio	111
7.2.- Análisis del Plan de Continuidad.....	112
7.3.- Análisis de Impacto.....	113
7.3.1 Tipos de impacto Económico.....	114
7.4 Desarrollo de Estrategias de Continuidad.....	116
7.5 Entrenamiento y Pruebas de Mantenimiento de los Planes de Continuidad...	118
7.6 Gestión de la Crisis y Comunicación.....	119
7.7 British Continuity Institute (BCI)	121
7.7.1Componentes de la Empresa	122
7.7.2 Manejo de Continuidad de Negocio.....	123
7.7.3 British Standar Institute (BSI).....	125
7.8 Plan de Recuperación de Desastres	126



CAPITULO 8 CONCLUSIONES	134
REFERENCIAS.....	137

INTRODUCCIÓN

En la actualidad establecer y coordinar un conjunto de procedimientos y acciones destinadas a impedir, neutralizar y principalmente a reaccionar frente a los posibles riesgos que atenten contra el desarrollo del funcionamiento no ha sido fácil, debido al continuo crecimiento tecnológico alrededor del mundo.

Hoy en día es fundamental para las empresas poder asegurara la continuidad de un negocio, debido a los crecientes efectos causados por una globalización entre los que destacan la alta interdependencia de los mercados y la desegregación productiva.

Conforme las empresas son más dependientes de la tecnología y compiten en escenarios complejos debido a la globalización, se hacen más susceptibles a que una serie de amenazas puedan penetrar sus vulnerabilidades y causarles daño, al grado de dejarlas fuera del mercado. Las estadísticas demuestran que una empresa que deja de operar dos semanas consecutivas, sale definitivamente de operación. Los mercados y la cadena de suministros exigen hoy en día a las empresas poder demostrar que se poseen un “plan de continuidad del negocio” ante la supuesta presencia de una tragedia.

La industria química, para sobrevivir, debe estar preparada para los riesgos inherentes en su operación y establecer las estrategias apropiadas, ante los incidentes, no salga del negocio. La empresa debe asegurar a terceros que ante la ocurrencia de un evento mayor o menor, ella seguirá operando. Se necesita demostrar confianza en ser un proveedor confiable. El mercado, los consumidores, exigirán en el caso de un siniestro, que cualquier empresa de respuesta oportuna siga operando. La gestión de continuidad del negocio debe estar implementada en la empresa y en su cultura, es decir, no es un tema sólo de expertos, sino involucrada la alta dirección y todo el personal de la misma



El contenido principal del trabajo incluye objetivos, funciones y responsabilidades, criterios de activación, la autoridad para declarar y gestionar un incidente, las necesidades de recursos, lugares alternativos de trabajo, capacidades y estrategias de comunicación para persona dentro de ella y externos, así como los procesos de respuesta y recuperación. También se especifica, las operaciones de emergencia ó plan de respuesta de emergencia, el plan de prevención, plan de mitigación, plan de recuperación y plan de continuidad.

OBJETIVOS

Establecer una serie de criterios para el desarrollo de un Plan de Continuidad de Negocio aplicando la norma NFPA 1600 (National Fire Protection Association) “Manejo de Desastres y Emergencias y Programas de Continuidad de los Negocio”

Facilitar el manejo de desastres y emergencias con un programa para evaluar, desarrollar e implementar la prevención, mitigación, respuesta y recuperación en la empresa.

Brindar una serie de pasos que ayude al desarrollo de una empresa y que no caiga en el desafortunado suceso de salir de operación.

HIPÓTESIS

La adopción de la norma NFPA (National Fire Protection Association) 1600 como guía para desarrollar el plan de continuidad de un negocio en la industria química, le permitirá en forma proactiva prepararse para cualquier evento previsible que impida el proceso libre de interrupciones.

Como ventaja adicional la empresa será más competitiva al adoptar nuevos modelos de desempeño en su gestión.

CAPITULO 1

ANTECEDENTES

La rapidez con lo cual una compañía pueda reiniciar sus operaciones comerciales luego de un ataque terrorista, huracán, incendio o inundación depende de los planes de emergencia que se elaboren¹.

A partir del atentado terrorista de 11 de septiembre de 2001 a las torres gemelas, la preocupación se incremento en estar preparados. Cuando se considera que el número va aumentando en los desastres se piensa en incluir una política corporativa y estatutos que ayuden a la organización a establecer prácticas de recuperación ante un desastre como DRII (Disaster Recovery Institute International)¹.

La más importante de las 10 Prácticas Profesionales, durante el desarrollo de un proceso de continuidad de los negocios de una organización, es el aval y compromiso de la gerencia ejecutiva, identificada en la primera práctica, "Inicio y Gestión de Proyectos". Una vez que el aval de la gerencia ha sido confirmado, un representante acreditado del DRII dispondrá todo lo necesario para definir la gestión y organización del proyecto con respecto a los restantes componentes del modelo de planificación¹.

Hay pocas normas en el mundo sobre continuidad de los negocios, principalmente todavía está visto como un concepto nuevo. Debido a este faltante, en el mercado la recientemente norma publicada fue BS 25999 de origen británico en el 2006.

La norma BS 25999 contiene dos partes. La Parte 1 es el "Código de Prácticas", presentando los lineamientos y los objetivos de la norma así como explicando cuál es el alcance cubierto. La Parte 2 es la especificación los requisitos contra los cuales se certifican las organizaciones. Describe los requisitos para la



implementación, documentación y mejora del sistema. En términos sencillos, la parte 1 es el “debería” y la parte 2 es el “debe”.

El lanzamiento de la BS 25999-1, el Código de Prácticas, ciertamente revirtió la creencia usual de que no tiene ventajas respecto a otras disciplinas de la gestión. Raramente una nueva norma genera entusiasmo excesivo en el mundo de las empresas, muchas veces percibida como respetable.

Sin embargo, en el grupo de normas regulatorios que existen en el mundo, muchos hacen referencia a la gestión de la continuidad de los negocios, aunque no usen necesariamente la misma terminología. Algunas de las normas que existen son:

- ISO 17799 – Una norma de sistemas de gestión de la seguridad de la información, la que gestiona y minimiza las amenazas a la información.
- ISO 22399– lineamientos para la toma de conciencia de los incidentes y la gestión de la continuidad operativa.
- HB 221 y HB 292/293 – la norma y la guía australianas sobre la gestión de la continuidad de los negocios.
- AS/NZS 4360:2004 – compartida por Australia y Nueva Zelanda, la que en conjunto con la HB 436 proporciona lineamientos sobre la gestión de riesgos.
- SPRING TR 19– la referencia técnica de Singapur sobre la gestión de la continuidad de los negocios, la que trata principalmente los aspectos técnicos de los sistemas.
- El reporte King II sobre Gobernanza Corporativa – estos lineamientos de Sudáfrica para la gestión de riesgos, enfocan la gestión de la continuidad de los negocios desde la perspectiva de la gobernanza.



- El Civil Contingencies Act 2004 – este Acta recibió la aprobación real en 2004 en el Reino Unido, proporcionando lineamientos sobre la gestión de la continuidad de los negocios³⁶.

La NFPA (National Fire Protection Association) 1600 fue establecida como el documento de consenso, que complementa las 10 Prácticas Profesionales del DRII en las que se fundamenta el modelo de Goodyear. Al cumplir con los lineamientos y prácticas recomendadas de NFPA 1600, y el modelo del DRII, ayudó a que toda la organización comenzara a centrarse en un mismo aspecto y a utilizar una terminología común. Esto ayudó a que todos los miembros del equipo táctico comprendieran la importancia de una planificación previa interna y conjunta con socios externos, así como al desarrollo de un enfoque común para el logro de una respuesta efectiva con una rápida recuperación¹.

El origen y desarrollo de la norma NFPA 1600 comenzó en enero de 1991, el Consejo de Normas de la NFPA creó el Comité de Manejo de Desastres, que tendría a su cargo la elaboración de documentos relacionados con la preparación, respuesta y recuperación ante desastres, provocados por incidentes tecnológicos, naturales o causados por fallas humanas¹.

En la edición del año 2000, el comité introdujo un “enfoque que incluía una programación total” para el manejo de desastres/emergencias y programas sobre la continuidad de los negocios, en la revisión del documento que lo transforma de práctica recomendada a norma. El comité amplió las disposiciones con el fin de aumentar las capacidades para el manejo de desastres/emergencias y de los programas de continuidad de los negocios, de manera que el impacto de un desastre pudiera ser mitigado, protegiendo al mismo tiempo la vida y los bienes.

En año 2004, se incluyó en el Anexo A una tabla en la que se establecen referencias cruzadas entre la Agencia Federal de Gestión de Emergencias (FEMA, por sus siglas en inglés) y las prácticas profesionales del Instituto de Continuidad



de los Negocios (BCI, por sus siglas en inglés) y del Instituto Internacional de Recuperación ante Desastres (DRII, por sus siglas en inglés)¹.

La edición 2007 se amplió el marco conceptual para el manejo de desastres y emergencias para los programas de continuidad de los negocios para resumir en estos cuatro pasos: mitigación, preparación, respuesta y recuperación. De esa forma, la norma se alinea con disciplinas y prácticas relacionadas sobre gestión de riesgos, seguridad y prevención de pérdidas¹.

CAPITULO 2

¿QUÉ ES RIESGO?

En la vida no puede haber una actividad que no implique un riesgo, sin embargo, los riesgos pueden reducirse o manejarse. Los riesgos han aumentado conforme la tecnología avanza, por lo que se describirá en este capítulo de lo que es un riesgo y los diferentes escenarios que se tiene al clasificarlos. En una empresa una de las obligaciones más importantes o de función primordial es evaluar y controlar los riesgos para la salud de los trabajadores.

El riesgo es la probabilidad de que suceda un evento no deseado por la severidad o consecuencia de este, por lo que se puede expresar de la siguiente forma:

$$\text{Riesgo} = \text{Probabilidad} \times \text{Severidad}.$$

En la siguiente figura se muestran las etapas en un evento no deseado al que se denomina impacto. En estado de normalidad están las medidas de prevención y mitigación, en la de anormalidad están el de control y combate así como recuperación y restablecimiento².

Figura 2.1.-Un evento no deseado².



Las medidas de **prevención y mitigación** se basan en la identificación de los riesgos diseñando acciones o programas para reducir la probabilidad de que ocurra un impacto.

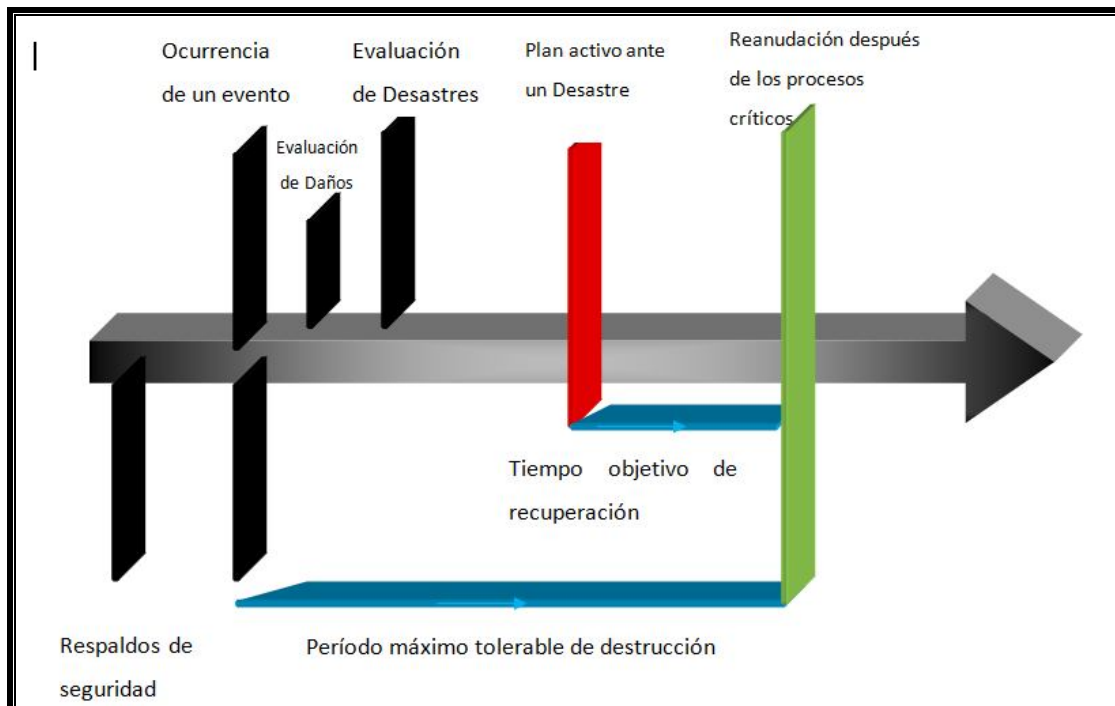
El **control y combate** se refiere a las acciones que deben tomarse inmediatamente antes, durante y después del impacto con el fin de minimizar los daños causados.



En **recuperación y restablecimiento** son acciones orientadas a la reconstrucción y mejoramiento de infraestructura y servicios dañados o destruidos.

Para poder reducir un estado de crisis es importante identificar la vulnerabilidad y la exposición, tomando parámetros cuantitativos de los bienes materiales expuestos que podamos medir por ejemplo la magnitud y la intensidad.

Figura 2.2.-Periodo Máximo de Destrucción



Fuente: Elaboración propia

En la figura 2.2 muestra el proceso que comprende desde la ocurrencia de un evento hasta su reanudación, de esta forma la magnitud es una medida de la vulnerabilidad de que suceda un riesgo y la intensidad es la medida de la fuerza con que se manifiesta el riesgo.

2.1. Riesgo Telúrico³.

En un riesgo telúrico se encuentran varios fenómenos geológicos que son aquellos que intervienen en la dinámica de los materiales interiores y exteriores de la tierra y se clasifican en: sismicidad, vulcanismo, tsunamis y movimientos de laderas y suelos.



2.1.1. Sismicidad

El fenómeno de la sismicidad está presente constantemente en la historia, es como así se ha aprendido a que un sismo no se puede predecir por que no existe un procedimiento que establezca con exactitud el lugar, día y hora en que puede ocurrir este acontecimiento.

Se conoce que los sismos se originan en lugares bien definidos en ciertas regiones con una estimación de magnitudes.

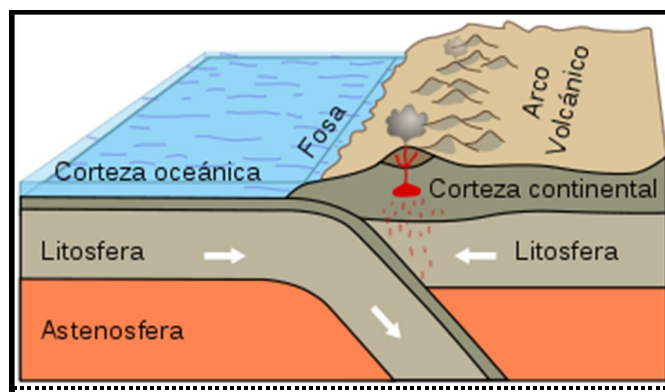
El movimiento vibratorio de la corteza terrestre de corta duración pero con diferentes intensidades se le conoce como un movimiento sísmico. El punto u origen del movimiento se le conoce como foco sísmico o hipocentro y el punto de la superficie terrestre principalmente afectado se le llama epicentro.

Estos movimientos están relacionados con dos de las capas de la corteza terrestre y son la litosfera y astenosfera.

La litosfera es una capa fuerte y rígida, está dividida en numerosos fragmentos que se mueven uno respecto de la corteza terrestre, cambiando constantemente de tamaño y forma las cuales se llaman placas.

La litosfera se encuentra superior a la astenosfera que es una capa con temperatura y presión muy similares a la de fusión del material rocoso, lo cual provoca una zona muy dúctil que permite la separación con facilidad de las placas de la litosfera induciendo los movimientos sísmicos.

Figura 2.3.-Capas exteriores de la corteza terrestre³⁷.





Existe una gran cantidad de información de todos los sismos que han sucedido alrededor del mundo pero esto no significa que han aumentado la cantidad de éstos. La población ha crecido y se ha asentado en lugares proclives a la amplificación de movimientos sísmico, empleando una incorrecta técnica de construcción, lo que a conducido a consecuencias devastadoras para las personas.

En 1935 Charles Richter desarrolló la primera escala de magnitudes utilizando registros sísmicos para calcular las dimensiones de los movimientos que relaciona la cantidad de energía liberada en las amplitudes de onda, su escala tiene aplicación para sismos superficiales y relativamente cercanos Tabla 2.1.

Tabla 2.1.-Magnitudes Richter y sus efectos⁴

MAGNITUDES RICHTER	DESCRIPCIÓN	EFFECTOS	FRECUENCIA
Menor de 2	Micro	Los microsismos no son perceptibles.	Alrededor de 8 por día
2.0-2.9	Menor	Generalmente no son perceptibles	Alrededor de 1 por día
3.0-3.9		Perceptibles a menudo, pero rara vez provocan daños.	49 por año
4.0-4.9	Ligero	Movimiento de objetos en las habitaciones que genera ruido. Sismo significativo pero con poco probable daño	6.2 por año
5.0-5.9	Moderado	Puede causar daños mayores en edificaciones débiles o mal construidas. En edificaciones bien diseñadas los daños son leves.	800 por año
6.0-6.9	Fuerte	Pueden ser destructivos en áreas pobladas, en hasta unos 160 kilómetros a la redonda.	120 por año
7.0-7.9	Mayor	Puede causar serios daños en extensas zonas.	18por año



8.0-8.9	Grande	Puede causar graves daños en zonas de varios cientos de kilómetros.	1 por año
9.0-9.9		Devastadores en zonas de varios miles de kilómetros	1 en 20 años

Los factores a contemplar donde puede haber un riesgo de un sismo van acompañados de tres factores los bienes expuestos, la vulnerabilidad y el peligro de que ocurra el fenómeno. Por lo tanto contemplar estos tres factores ayudará a que controlar que la población no se establezca en zonas muy vulnerables.

2.1.2. Tsunamis.

Los Tsunamis se generan en el fondo del océano, les precede de una retirada brusca del mar que deja al descubierto parte de la plataforma normalmente cubierta por el agua. El comportamiento que tiene es impreciso ya que si su origen es en mar abierto no se nota el cambio de nivel pero al llegar a costa su velocidad disminuye pero su altura puede aumentar hasta llegar alcanzar unos 30 metros.

2.1.3. Vulcanismo^(4y8).

Los volcanes son más fáciles de tratar ya que conocemos la ubicación exacta y es una manifestación de la energía interna de la Tierra, pero no se dispone de un calendario donde indique las actividades de erupción como la magnitud de la actividad futura. El registro de erupción del pasado sirve para ver cómo es la actividad del volcán y las magnitudes que puede alcanzar. Esto ayuda a calcular los peligros de las zonas más vulnerables y tomar acciones para tener una reducción de pérdidas humanas y materiales. La elaboración de mapas de peligro volcánico es compleja y queda en manos de técnicos especializados en el tema. Las erupciones que tienen los volcanes son emisiones de mezcla de roca fundida con material volátil al que se conoce como magma la cual va acompañada de fragmentos de agua, dióxido de carbono y azufre entre otros.

Los terrenos que han sido alcanzados por la lava no pueden volver a ser utilizados, lo que provoca una gran destrucción.



Las cenizas volcánicas son lava que ha sido pulverizada y convertida en polvo o arena por erupciones volcánicas. Durante una explosión, los fragmentos más gruesos caen rápidamente en las cercanías del volcán, sólo la ceniza más fina es arrastrada por el viento a grandes distancias que van de cientos hasta miles de kilómetros, y puede afectar áreas muy extensas y a un gran número de personas. La caída de cenizas puede provocar en las personas algunas de los siguientes efectos: el agravamiento de enfermedades pulmonares, trastornos gastrointestinales por la ingestión de agua y alimentos contaminados con flúor y posiblemente con metales pesados (arsénico, mercurio, etc.); daños oculares como conjuntivitis y abrasiones en la córnea. Las cenizas puede ser resbalosa obstruir corrientes de agua, carreteras, plantas de agua residual, todo tipo de maquinaria, y grandes cantidad de ceniza altera el suministro de energía, tráfico aéreo y el cultivo.

El viento y el tipo de erupción son los dos factores principales que controlan la dispersión de la ceniza de un volcán que entra en erupción. El tipo de erupción determinará el volumen y el tamaño de la ceniza, así como la variedad de altitudes a la cual la ceniza es propulsada o elevada.

2.1.4 Movimientos de laderas y Suelos^{5y6}

Otros fenómenos locales que pueden producir consecuencias severas son los movimientos de laderas y los desplazamientos permanentes del terreno por la presencia de fallas activas.

Los movimientos de laderas se producen por la pérdida de la capacidad de carga de suelos arenosos saturados de agua debido a la vibración producida por un sismo; los edificios sobre estos suelos pueden presentar grandes hundimientos y, en casos extremos, colapso por volteo.

Las laderas de cerros o terraplenes de suelos poco compactos y fuertes pendientes pueden sufrir deslizamientos y arrastrar las construcciones sobre ellas edificadas.

Finalmente, en ocasiones se presentan fallas geológicas superficiales que, además de llegar a producir excitación sísmica en mayor o menor grado, dejan como consecuencia desplazamientos permanentes del terreno, en sentido



horizontal y/o vertical, que llegan a producir graves daños a las construcciones ubicadas sobre la traza de la falla.

Por lo anterior, es necesario que para todas aquellas ciudades importantes o donde ya se hayan observado efectos de sitio, se realicen estudios que definan la distribución y características de los materiales superficiales, y en particular su respuesta dinámica, así como la presencia de laderas inestables o de fallas activas.

Con esta información es posible realizar estudios de microzonificación y los correspondientes mapas detallados de la distribución de peligro sísmico a escala local.

2.2. Riesgos Hidrometeorológicos ^(5y7).

En las crisis de origen hidrometeorológico están los fenómenos de inundaciones, precipitaciones pluviales, huracanes, sequía y heladas, estos fenómenos provocan la pérdida humana o material al estar expuesta constantemente en ciertas zonas. Los conocimientos que nos proporciona protección civil ayuda a contrarrestar los daños y prevenir un desastre en la población y su entorno.

2.2.1 Precipitaciones Pluviales

Una precipitación pluvial es cualquier forma de agua que cae de la atmósfera a la superficie de la tierra. Estas se pueden manifestar en forma de lluvia, llovizna, nieve y granizo.

La humedad siempre está presente en la atmósfera aunque los días están despejados, este vapor se condensa y se transforma en líquido en forma de gotas o al estado sólido como cristales de hielo.

La humedad se produce por la evaporación de océanos, mares, lagos, lagunas, ríos, arroyos y de los suelos.

Los diferentes tipos de precipitación están englobados en lluvia ciclónica que es el resultado del levantamiento de aire por una baja de presión atmosférica y la lluvia de frente cálido es la formación por una subida de masa de aire caliente por encima de una de aire frío. Esto es cuando las montañas desvían hacia arriba el viento, sobre todo aquel proveniente del mar. Otras de las causas que causan las



precipitaciones son la llegada de los frentes fríos provenientes de las zonas polares.

2.2.2 Inundaciones.

Las inundaciones vienen acompañadas de material sólido provenientes de las partes altas de la cuenca, con características diferentes ya que depende del tipo de suelo y pendiente que definirá el material de arrastre, como el tiempo de escurrimiento para ver si el proceso inesperado o lento.

Cuando una inundación es imprevista va a depender de varios factores, en primera el tipo de pendiente ya que si es de carácter montañoso está pendiente es muy prolongada y hará más rápido el descenso del agua acompañado de rompimientos de un bordo o deslaves. También se presenta en presas, ciudades donde el tipo de suelo es muy impermeable provocando una difícil manera de alertar a la población cobrando muchas vidas humanas.

Las inundaciones están muy ligadas a la geografía según la región ya que de esto va depender en donde es más vulnerable a que halla una precipitación pluvial. La precipitación se puede manifestar como lluvia, llovizna, nieve y granizo, originada por la humedad que está presente en la atmósfera aunque el cielo este despejado.

Para identificar los riesgos de inundación en una zona de interés se tienen que tomar varios aspectos, si en la zona existe un arroyo, la distancia que hay hasta la población más cercana, si las bajadas del terreno son muy prolongadas, que tipo de drenaje hay en la zona y los tipos de suelo.

Los suelos se clasifican en finos y gruesos, en la tabla 2.2 se muestra la clasificación según su diámetro.



Tabla. 2.2.- Tipos de Suelo⁵

Gruesos	Macizo Rocoso
	Roca disgregada($100 < \varnothing < 500\text{mm}$)
	Gravas($3.5 < \varnothing < 100\text{mm}$)
	Arena gruesa($2.4 < \varnothing < 3.5\text{mm}$)
	Arena mediana($1.22 < \varnothing < 2.4\text{mm}$)
	Arena fina($0.075 < \varnothing < 1.22\text{mm}$)
	Arena limosa
Finos	Arena arcillosa
	Limo arenoso
	Arcilla arenosa
	Limo
	Arcilla

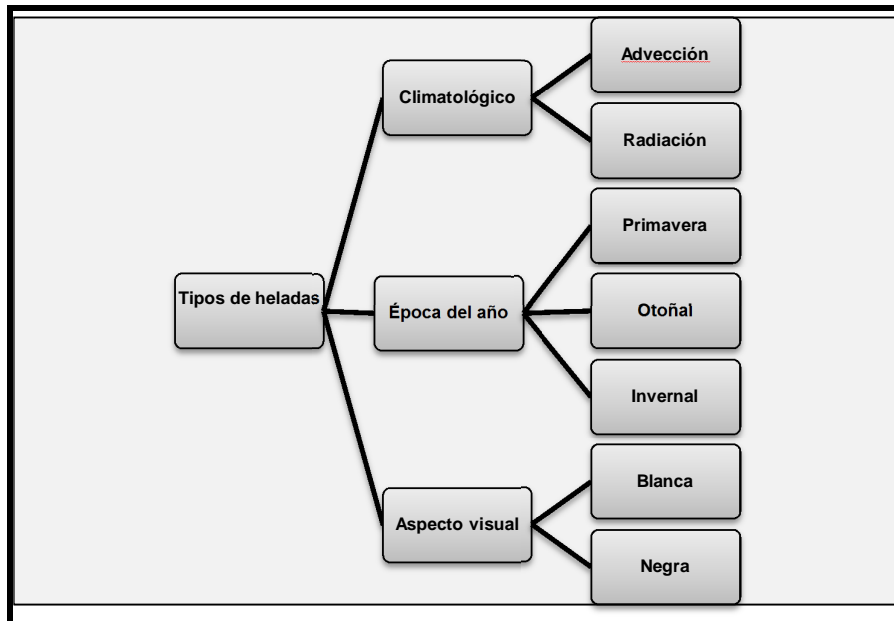
Esta tabla nos ayuda a tener una mejor clasificación de cómo es el suelo de interés para poder hacer una valoración más amplia y saber si es vulnerable a una posible inundación. Como en el caso de tener un suelo fino va a ser mas vulnerable a que se inunde.

2.2.3. Heladas

Cuando sucede una helada es cuando la temperatura de la superficie de la tierra desciende a los 0°C en un período de 12 horas. Existen dos fenómenos que ocasionan las heladas uno es las radiación durante la noche de la tierra a la atmósfera que causa la perdida de calor y la otra es una masa de aire frío.

La helada es la disminución de la temperatura del aire a un valor igual o inferior al punto de congelación del agua. Se presentan particularmente en las noches de invierno por una fuerte pérdida radiactiva. Esto sucede de la siguiente forma: una fracción de la energía desprendida por el sol es absorbida por la troposfera (capa de la atmosfera más cercana a la tierra), otra es dirigida al exterior al ser difundida desde la atmósfera. Cuando una región de la superficie terrestre desprende más energía que la que recibe, ocurre un enfriamiento al que llamamos helada.

Las heladas se pueden agrupar de la siguiente forma:

Figura 2.4.- Tipo de heladas⁵

Las de origen *climatológico* por **advección** se forman cuando llegan grandes masas de aire frío, que se pueden presentar en el día o en la noche.

Las *heladas por radiación* ocurren por la pérdida de calor del suelo durante la noche, durante el día el suelo se calienta y en las noches pierde calor por la radiación. Las zonas más propensas a que suceda este fenómeno son valles y cuencas por la acumulación de aire frío que desciende durante la noche. Conforme a las estaciones del año las *heladas primaverales* afectan principalmente a los cultivos cuando llega el primer brote de ramas o pocos días de nacimiento presentando un descenso de temperatura.

Las *heladas otoñales* o tempranas son provenientes de masas de aire del polo norte que dañan la formación o maduración de frutos provocando un golpe brutal para la agricultura.

Las *heladas invernales* llegan a ser las más dañinas ya que el descenso de la temperatura con los frentes fríos, dañan notablemente al ser humano y la agricultura, provocando una gran pérdida económica.

La *helada blanca* se origina cuando estas masas de aire son húmedas. Para que se presente esta helada es indispensable que el aire cercano al follaje y las flores tengan temperaturas iguales o menores que 0°C, de esta manera, el aire alcanza



la temperatura del punto de rocío, ya que con ello existe condensación y de inmediato el vapor de agua del aire pasa al estado sólido para formar hielo.

La **helada negra** se desarrolla cuando el aire tiene poco vapor de agua y la temperatura del punto de rocío es inferior a 0° C; de modo que existe escasa condensación y nula formación de hielo sobre la planta. Sin embargo, los cultivos son dañados y al día siguiente las plantas presentan una coloración negruzca, por la congelación de la savia de las plantas o del agua de sus tejidos.

2.2.4. Huracanes

Los huracanes cuyo origen es en los trópicos, son formados por calor y humedad que transfiere el océano al aire. Los principales factores de la formación de los huracanes son los siguientes:

- * Cambio de rapidez de los vientos
- * Una distribución vertical de humedad y temperatura que permita la formación de la nubes
- * Concentración de la rotación ciclónica en la tropósfera.

Los huracanes están dentro de los sistemas más destructivos de los fenómenos meteorológicos. Los huracanes tropicales se caracterizan por una circulación cerrada de sus vientos y se divide en fases de acuerdo a su velocidad de su viento máximo.

- * Depresión Tropical: menor a 63 km/h.
- * Tormenta Tropical: entre 63 y 118 km/h.
- * Huracán: mayor a 118 km/h.

Los riesgos de los huracanes tropicales cambian en tierra firme y superficie marina. Los principales riesgos en océanos que presentan las actividades humanas ante la presencia de un huracán son instalaciones petroleras, barcos y tráfico aéreo. En tierra se ven amenazadas las ciudades, pueblos, carreteras, cultivos entre muchas más actividades que competen al hombre.

La lluvia es un aspecto característico de los huracanes, este permanece en el centro del huracán después de la llegada a tierra, si el huracán permanece más tiempo en tierra se espera un incremento de lluvia. En algunas ocasiones los



ciclones tropicales producen lluvias muy intensas pero otros pueden pasar rápidamente sin causar precipitaciones severas, también presentan vientos, muy intensos cerca del centro del huracán.

La escala de huracanes de Saffir-Simpson es una escala que clasifica los huracanes tropicales según la intensidad del viento, desarrollada en 1969 por el ingeniero civil Herbert Saffir y el director del Centro Nacional de Huracanes de Estados Unidos, Bob Simpson.

La escala original fue desarrollada por Saffir mientras pertenecía a una comisión de las Naciones Unidas. En el desarrollo de su estudio, Saffir se percató de que no había una escala apropiada para describir los efectos de los huracanes. Apreciando la utilidad de la escala sismológica de Richter para describir terremotos, inventó una escala de cinco niveles, basada en la velocidad del viento, que describía los posibles daños en edificios. Saffir cedió la escala al Centro Nacional de Huracanes de Estados Unidos; posteriormente Simpson añadiría a la escala los efectos del oleaje e inundaciones.

Además, a medida que un huracán tropical se organiza, pasa por dos categorías iniciales. Éstas no están contenidas dentro de la escala de Huracanes de Saffir Simpson, pero clasifican a un huracán tropical en formación y se utilizan como categorías adicionales a la misma como depresión tropical que es un sistema organizado de nubes y tormenta eléctrica con una circulación cerrada y definida y la otra es tormenta tropical que es un sistema organizado de fuertes tormentas eléctricas con una circulación bien definida que muestra la distintiva forma ciclónica.



Tabla 2.3.-Categoría de Huracanes

Categoría	Velocidad de viento (Km/h)	Marea (m)	Nivel de Daño
1	119-153	1.2-1.5	Sin daños en las estructuras de los edificios. Daños básicamente en casas flotantes no amarradas, arbustos y árboles. Inundaciones en zonas costeras y daños de poco alcance en puertos
2	154-177	1.8-2.4	Daños en tejados, puertas y ventanas. Importantes daños en la vegetación, casas móviles, etc. Inundaciones en puertos así como ruptura de pequeños amarre
3	178-209	2.7-3.7	Daños estructurales en edificios pequeños. Destrucción de casas móviles. Las inundaciones destruyen edificaciones pequeñas en zonas costeras y objetos a la deriva pueden causar daños en edificios mayores. Posibilidad de inundaciones tierra adentro.
4	210-249	4.0-5.5	Daños generalizados en estructuras protectoras, desplome de tejados en edificios pequeños. Alta erosión de bancales y playas. Inundaciones en terrenos interiores.
5	>250	>5.55	Destrucción de tejados completa en algunos edificios. Las inundaciones pueden llegar a las plantas bajas de los edificios cercanos a la costa. Puede ser requerida la evacuación masiva de áreas residenciales.

2.2.5. Sequías

Una sequía es un lapso que tiene como característica una prolongada falta de humedad que producen una gran pérdida económica y favorecen la migración hacia otras zonas de trabajo. Las sequías afectan grandes extensiones de terreno de cultivo y cabezas de ganado, disminuyendo la disponibilidad de agua para la producción industrial y de uso doméstico.

La forma en que se presentan las sequías es de una forma lenta provocando que los daños sean de poco apoco con una duración de meses hasta años. Las medidas de prevención para afrontar las sequías están orientadas, por un lado, a políticas de uso eficiente del agua en los hogares, agricultura ganadería y en la industria y por otro lado aumentar la infraestructura hidráulica para almacenar agua y conducirla adecuadamente a su destino.



No es fácil identificar cuando se está presentando una sequía ya que su proceso es paulatino y hay que verificar la intensidad con la que se está presentando. En una distribución temporal y espacial de la precipitación en forma de lluvia, nieve, y granizo ayuda a ver si se presentara una sequía, relacionado con cambios en las presiones atmosféricas, alteraciones en la circulación de los vientos a escala planetaria, modificaciones en la cantidad de luz reflejada en la superficie, cambios en la temperatura de la superficie de los océanos e incrementos en las concentraciones de bióxido de carbono en la atmósfera.

Las medidas de mitigación se dividen en dos grandes ramas: las estructurales y las no estructurales.

Las medidas estructurales son las grandes construcciones de obras de ingeniería que ayudan a controlar, almacenar, extraer y distribuir el agua. Dentro de estas obras se encuentran las construcciones de presas, tanques de almacenamiento, sistemas de abastecimiento de agua potable, perforación de pozos y canales.

Dentro de las que mencionamos las de mayor importancia son las presas. Su diseño va en función de la hidrología y topografía del lugar, así como de las actividades humanas cercanas a esta obra como la ganadería, agricultura y la industrial.

Otras obras de ingeniería de igual importancia son el tratamiento de aguas negras, la construcción de drenaje sanitario y pluvial. En general todas las obras de ingeniería para mitigar las sequías son costosas pero solas no son suficientes para enfrentar las sequias, más bien son complemento.

Las medidas no estructurales son de acciones que se adoptan antes y después de la sequía que son: socioeconómicas, legales, de planeación. Se refieren específicamente a reglamentos del uso del agua. Como ejemplos de estas son:

- * Limitar la dotación de agua
- * Implantar programas de emergencia para disminuir el impacto económico
- * Cultura en la población de cuidar el agua (clases en las escuelas del uso del agua, repartir folletos en mercados, calle, centros de trabajo.)



2.3. Riesgos Humanos.

En los riesgos humanos cabe mencionar el terrorismo y el sabotaje se describirá de las características de cada uno.

2.3.1. Terrorismo.

Aquel ataque a las torres gemelas en Nueva York, EUA y a otros puntos el 11 de septiembre de 2001 introdujeron el término terrorismo como parte del vocabulario cotidiano; sin embargo no sólo estos ataques son ocasionados por grupos religiosos descontentos, de igual forma el narcotráfico es autor de estos crímenes que azotan al mundo hoy en día. Dicho acontecimiento que puso a los ojos del mundo en EUA ha sido antecedido por eventos similares en España, Alemania, México, Iraq y la mayoría de los países del mundo. Las víctimas cada vez son más, los civiles son el blanco predilecto para los terroristas, se inician guerras y mueren más inocentes, naciones enteras se ven destrozadas, líderes políticos amenazados, el mundo desencadena destrucción.

Entonces podemos preguntarnos ¿Qué es el terrorismo? A fin de combatir un mal es necesarios determinar su naturaleza por lo que aclarar estos puntos es importante mencionar que este fenómeno que se ha convertido en un mal para todo el mundo. El terrorismo es un tema del que todos hablan pero pocos acertadamente podrían definir cómo surgió, en pocas palabras, no es tarea fácil. Por tanto podemos hablar de diferentes definiciones de terrorismo. De acuerdo con que el terrorismo está vinculado al uso de la violencia o la amenaza con el fin de crear una atmósfera de miedo, terror y alarma para ayudar a alcanzar objetivos específicos.¹⁰

Las causas que explican el terrorismo son múltiples, las fórmulas que permiten a un grupo de personas considerar correcto su uso a pesar de su profunda inmoralidad son abundantes. La diferencia tecnológica, económica, militar entre unos países u organizaciones y otros obliga a que el terrorismo sea una respuesta, y que la comprensión a esa violencia encuentre apoyo en una amplia base social. Casi todos los grupos terroristas generan, de no existir previamente,



ese apoyo, que rápidamente elabora los criterios intelectuales que justifican los atentados.

El problema no es nuevo, pero conviene plantearse el porqué de la globalización del fenómeno terrorista. La globalización ayuda a todos los elementos que concurren en la actividad terrorista. Facilita los contactos, por medios electrónicos o personales y la transmisión de ideas, métodos, procedimientos, modelos.

La pobreza, la falta de entendimiento en la concepción del mundo, el fanatismo en la aplicación de las ideas justifica el asesinato y las víctimas acaban siendo culpables por su modo de vida, por su religión, por sus ideas, por sus profesiones. Lo peor de los argumentos del terrorismo es culpabilizar a otro como justificación del uso de la violencia⁹.

Orígenes¹¹

El carácter extra normal de la violencia terrorista se debe a que ésta se desarrolla no en un combate o en medio de una manifestación popular, sino en escenarios improbables de violencia, tales como el hogar, los centros comerciales, las tranquilas calles de una ciudad, etcétera, e incluso en no pocos casos se produce contra personas “inocentes” que no están directamente ligadas al mundo político ni son culpables de la causa de la violencia. El terrorismo, como señala Alex Schmid, “es el equivalente de crímenes de guerra en tiempos de paz”.

El terrorismo, así definido, no es un fenómeno nuevo en el mundo político. Tiene antecedentes muy antiguos. Uno de los primeros ejemplos es el de los sicarios palestinos, una secta religiosa judía que actuó durante la lucha de los zelotes contra el imperio romano (años 66 a 73 DC). Su modo de actuar era el asesinato de judíos moderados que contemporizaban con los romanos, para lo cual utilizaban pequeños cuchillos denominados VLFDULL que escondían entre sus ropas.

El mensaje era que todos los que buscaran entenderse con los romanos correrían igual suerte. El resultado final, como sabemos, fue catastrófico, ya que la respuesta romana significó el Los zelotes no fueron la única secta religiosa que recurrió al terrorismo para imponer sus ideas. Los llamados asesinos conformaron otro de estos grupos. Su lucha deriva del enfrentamiento entre ismailíes (una



secta chiita) y sunitas. Los ismailíes creían que era necesario purificar al Islam, según ellos sumido en la corrupción para preparar el arribo del Mahdi, el sucesor del Profeta. Superados por los ejércitos sunitas, recurrieron al terrorismo asesinando a sus rivales y dejándose capturar para convertirse en mártires. Una muestra de las delicias del paraíso al que arribarían con su martirio les era proporcionada por la ingestión del *hashish*¹².

Es por ello que los grupos terroristas han tenido una gran motivación ideológica, religiosa o patriótica. Algo que cada vez se manifiesta como menos relevante, aunque se sigue utilizando como reclamo ante los medios y para obtener respaldo popular.

Situación actual

A lo largo de varios años se está tratando de describir el proceso de cómo atacar a una red de terrorismo: identificar la red, desarticularla, prevenir su reconfiguración, y evitar su reproducción, así como los medios involucrados en el mismo.

Una red es un enemigo, al cual no es posible aplicar el tradicional tratamiento de los centros de gravedad ni el ataque al punto más débil. Aunque en esencia vivimos en un conflicto parecido a una guerra, es esencialmente asimétrico, y los Estados han de perder su papel principal para pasar a ser componentes de otra red, si queremos tener alguna opción de ganar esta guerra. La historia reciente ha demostrado que nuestro enemigo vive perfectamente mimetizado y embebido en un entorno que le apoya, y cuando creemos haber cortado una de las cabezas de la red, aparecen nuevas cabezas en sitios distintos, distantes y no necesariamente conexos.

Es indudable que, como reacción a este problema, se está produciendo, una intensa cooperación entre los países que se sienten más directamente amenazados, lo que podría determinar un nuevo orden mundial, caracterizado por la colaboración estrecha entre los sujetos más importantes del panorama estratégico internacional.

Para identificar la red y su capacidad de acción, es fundamental contar con los medios de inteligencia necesarios. Pero a diferencia con un conflicto tradicional,



donde la inteligencia es proporcionada por múltiples fuentes de inteligencia de medios humanos y electrónicos en un campo de batalla, centralizadas, controladas y accesibles, es por ello que el combate contra la red implica revisar el concepto clásico. El campo de batalla es ahora la mitad del planeta, y de forma evidente será preciso disponer de medios de inteligencia donde la red se desenvuelva, y estos medios, principalmente humanos (aunque necesariamente apoyados por la electrónica y las comunicaciones) han de estar integrados en el entorno en que vivan, y contar con componentes autóctonos.

El costo asociado es elevado, como lo es el tiempo necesario, y por lo tanto será imprescindible reforzar los acuerdos existentes entre las naciones para compartir información y desarrollar la elaboración de evaluaciones de situación e informes de alerta rápida, sobre la base de la más amplia gama de fuentes posible.

2.3.2. Sabotaje¹⁴.

La palabra Sabotaje proviene del francés, "sabots", en esta lengua, significa zueco y la palabra sabotaje viene a raíz de la acción que realizaron trabajadores franceses que trabajaban en una harinera. En pleno conflicto laboral usaron sus zuecos para que hábilmente, como requiere el arte del sabotaje, no pudieran funcionar los molinos para moler el trigo usándolos de cuñas. Este acto ingenioso, seguramente no fue el primer acto para parar la producción pero si el que dio nombre tan magnífica labor en el arte del sabotaje.

En guerra, la palabra sabotaje se utiliza para describir la actividad de un individuo o para agrupar (no asociado con militar) los partidos en la guerra, particularmente cuando las acciones dan lugar a la destrucción o a dañar de una facilidad productiva o vital, tal como equipo, fábricas, presas, servicios públicos, plantas del almacenaje o logístico rutas.

Los actos del sabotaje no tienen siempre un objetivo primario de infligir muertes. Clasifican a los saboteadores generalmente como enemigos, y como espías puede ser obligado a procesamiento y penas criminales en vez de detención como a prisionero de guerra. Es común para un gobierno en energía durante guerra o los partidarios de la política de la guerra de utilizar el término libremente



contra los opositores de la guerra. El sabotaje sutil también ha estado apoyado por otras razones, incluyendo procurar guardar y obtener capacidades nucleares¹

Algunos criminales han enganchado a actos del sabotaje por razones de extorsión. Cuando los trabajadores contrariados dañan o destruyen el equipo o interfieren con el funcionamiento liso de un lugar de trabajo, se llama sabotaje del lugar de trabajo. Esto puede estar como parte de una actividad organizada del grupo, o de la acción de un o algún trabajadores en respuesta a agravios personales.

Ciertos grupos dan vuelta a la destrucción de la característica para parar inmediatamente la destrucción ambiental o hacer discusiones visibles contra las formas de tecnología moderna consideradas como perjudiciales a la tierra y a sus habitantes. FBI y otras agencias de la aplicación de ley utilizan el término eco-terrorista cuando está aplicado al daño de la característica. Los autores discuten que puesto que la característica no puede sentir terror, el daño a los bienes esté descrito más exactamente como sabotaje. Los opositores, por el contrario, precisan que los dueños de característica y los operadores pueden sentir de hecho terror.

¹ Sheila MacVicar; Ashley Velie con el Amy Guttman. "LOS E.E.U.U. Trabajo al programa de Irán Nuke del sabotaje", Noticias del CBS, 2007-May-23. Recuperado encendido 2007-05-23

CAPITULO 3

LEY DE PROTECCIÓN CIVIL¹⁵

La ley de protección civil es de orden público e interés social y se contempla en este capítulo para establecer las bases en materia de protección civil, entre la Federación, las Entidades Federativas así como Municipios, con el propósito esencial promover la prevención y trabajo independiente.

3.1. Disposiciones Generales

“La Ley de Orden Público” tiene por objeto establecer las bases de la coordinación en materia de protección civil, entre la Federación, las Entidades Federativas y los Municipios.

El Sistema Nacional de Protección Civil se integra con las normas, instancias, instrumentos, políticas, servicios y acciones previstos en la mencionada Ley con el fin de cumplir los objetivos.

Para comprender mejor esta ley se definen los siguientes términos:

a. *Sistema Nacional.*

Se refiere Al Sistema Nacional de Protección Civil.

b. *Consejo Nacional.*

Se refiere Al Consejo Nacional de Protección Civil.

c. *Programa Nacional.*

Se refiere Al Programa Nacional de Protección Civil.

d. *Protección Civil.*

Es el conjunto de disposiciones, medidas y acciones destinadas a la prevención, auxilio y recuperación de la población ante un desastre natural o provocado.

e. *Prevención.*

Conjunto de acciones y mecanismos a reducir riesgos, así como evitar o disminuir los efectos del impacto destructivo de los fenómenos perturbadores sobre la vida y bienes de la población.



f. *Auxilio.*

Acciones para salvaguardar la vida de las personas, sus bienes y el medio ambiente, ante la presencia de un agente destructivo.

g. *Recuperación.*

Proceso orientado a la reconstrucción y mejoramiento del sistema afectado así como a la reducción del riesgo y la magnitud de los desastres futuros.

h. *Apoyo.*

Conjunto de actividades administrativas para el sustento de la prevención, auxilio y recuperación de la población ante situaciones de desastre.

i. *Grupos Voluntarios.*

Son instituciones, organizaciones y asociaciones que cuentan con el personal con conocimientos, experiencia y equipo necesarios para prestar sus servicios en acciones de protección civil de manera desinteresada y comprometida.

j. *Agentes Destructivos.*

Fenómenos de carácter geológico, hidrometeorológico, químicotecnológico, sanitario-ecológico y socio-organizativo que pueden producir riesgo, emergencia o desastre. También se les denomina fenómenos perturbadores.

k. *Fenómeno Geológico.*

Calamidad que tiene como causa las acciones y movimientos violentos de la corteza terrestre, como los sismos, terremotos, las erupciones volcánicas, los tsunamis o maremotos también conocida como movimientos de tierra.

l. *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.



m. 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.

n. Fenómeno Sanitario-Ecológico.

Calamidad que se genera por la acción patógena de agentes biológicos que atacan a la población, animales y cosechas, causando su muerte o la alteración de su salud. Las epidemias o plagas constituyen un desastre. En esta clasificación también se ubica la contaminación del aire, agua, suelo y alimentos.

o. 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.

p. Riesgo.

Probabilidad de que se produzca un daño, originado por un fenómeno perturbador.

q. Emergencia.

Situación anormal que puede causar un daño a la sociedad y propiciar un riesgo excesivo para la seguridad e integridad de la población.

r. Desastre.

Se define como el estado en que la población de una o más entidades federativas, sufre severos daños por el impacto de una calamidad devastadora, enfrentando la pérdida de sus miembros, infraestructura o entorno, de tal manera que la estructura social se desajusta y se impide el cumplimiento de las actividades esenciales de la sociedad, afectando el funcionamiento de los sistemas de subsistencia.

s. Zona de desastre.

Espacio territorial que sufre en su estructura social, impidiéndose el cumplimiento normal de las actividades de la comunidad.



t. Damnificado.

Persona cuyos bienes, entorno o medios de subsistencia registran daños provocados directa o indirectamente por un fenómeno.

u. Evacuado/albergado.

Persona que ante la posibilidad de la ocurrencia de un desastre, es retirado por la autoridad de su lugar de alojamiento usual, para instalarla en un refugio temporal, a fin de garantizar tanto su seguridad como la satisfacción de sus necesidades básicas.

El poder ejecutivo federal dictara los lineamientos generales para conducir los labores de protección civil con el fin de lograr la participación de los diferentes sectores y grupos de la sociedad.

La Secretaria de Gobernación debe Incluir un presupuesto de egresos de la Federación en el Fondo de Desastres estableciendo los montos para dicha operación.

Los medios de comunicación masiva con ayuda de las autoridades orientaran a la población difundiendo oportunamente y verazmente la información emitiendo si hay una situación de emergencia o de desastre, donde actuaran los 3 poderes para sumarse a las acciones de protección civil de forma coordinada y eficaz.

3.2. Del Sistema Nacional.

El Sistema Nacional de Protección Civil es un conjunto de estructuras para el procedimiento y funcionamiento de las dependencias del sector publico contra los peligros que presenten a la población ante un desastre.

El objetivo del Sistema Nacional es proteger a la sociedad ante la eventualidad de un desastre, provocado por agentes naturales o humanos, a través de acciones que reduzcan la pérdida de vidas, propiedad y entorno ayudando a su rápida recuperación.

El Sistema Nacional se encuentra integrado por el Presidente de la República, por el Consejo Nacional, Organismos e Instituciones de la Administración



Publica Federal, por el Centro Nacional de Desastres grupos voluntarios, vecinales, nogubernamentales y por el sistema de protección civil de las entidades federativas del Distrito Federal y municipios.

La coordinación ejecutiva del Sistema Nacional recaerá en la Secretaría de Gobernación, la cual tiene la atribución de:

- a. Integrar, coordinar y supervisar el Sistema Nacional para garantizar la prevención, auxilio y recuperación de la población y su entorno ante una situación de desastre.
- b. Proponer políticas y estrategias para el desarrollo de programas internos de protección civil.
- c. Crear procedimientos de carácter técnico operativo de logística para prevenir y atender un desastre
- d. Asesorar a los gobiernos de entidades federativas y municipales.
- e. Preparar redes de detección, monitoreo de medición de riesgos.
- f. Emitir declaraciones de emergencia y desastre.
- g. Solicitar recursos para la prevención y atención de desastre.

En una situación de emergencia, el auxilio a la población debe constituirse en una función prioritaria, con al finalidad de iniciar las actividades de auxilio en caso de emergencia. La primera instancia de actuación especializada, corresponde a la autoridad municipal o delegación que conozca de la situación, si resulta insuficiente, se procederá a informar a las instancias federales correspondientes.

En las actividades de desastre y recuperación se dará prioridad a los grupos sociales vulnerables de escasos recursos económicos.

3.3. Del Consejo Nacional.

El Consejo Nacional es un órgano consultivo en materia de planeación de la protección civil.

Está integrado por el Presidente de la República, Secretaria de Gobernación, Relaciones Exteriores, Defensa Nacional, Marina, Hacienda y Crédito Publico.

Sus atribuciones del Consejo Nacional son:



-
- a. Órgano de consulta y coordinación de acciones del Gobierno Federal para integrar las actividades de los diversos participantes e interesados en la materia.
 - b. Fomentar la participación de todos los sectores de la sociedad, en ejecución de los programas de protección civil.
 - c. Convocar, coordinar y armonizar, la participación de protección civil.
 - d. Fijar por conducto de la Secretaria de Relaciones Exteriores, los criterios para el cumplimiento de los acuerdos internacionales en materia de protección civil, así como las modalidades de cooperación con otros países.
 - e. Promover una educación nacional de protección civil.

El Secretario de Gobernación será el Secretario Ejecutivo del consejo Nacional y el Secretario Técnico será el Coordinador General de Protección Civil.

El secretario ejecutivo tiene como deber presentar un informe del avance de programa nacional de Protección Civil, concertar con los poderes Legislativo y Judicial el cumplimiento del Programa Nacional, proporcionar a la población la información generada de protección civil.

El Secretario Técnico tiene como deber suplir en caso de ausencia al Secretario Ejecutivo, elaborar el calendario de sesiones del consejo nacional, formular el orden del día de cada sesión, convocar por escrito a los miembros del Consejo Nacional y demás funciones que le sean encomendadas.

3.4. De los Grupos Voluntarios.

La ley reconoce a como grupo voluntario a las instituciones, organizaciones y asociaciones municipales, estatales y nacionales que obtengan su registro en la Secretaria de Gobernación.

Los derechos y obligaciones de los grupos voluntarios son los siguientes:

- a. Disponer del reconocimiento oficial una vez registrados y sea publicado en el Diario Oficial de la Federación.
- b. Recibir reconocimiento por acciones realizadas en beneficio de la población.



-
- c. Cooperar en difusión de planes de protección civil.
 - d. Comunicar en caso probable de un riesgo.
 - e. Coordinarse bajo mando de autoridades en caso de riesgo.
 - f. Abstenerse de solicitar o recibir contraprestación alguna de las personas q quienes hayan ayudado.
 - g. Utilizar solo vehículos debidamente registrados y cuenten con las características de las Normas Oficiales Mexicanas.
 - h. Las personas que deseen desempeñar labores de rescate y auxilio deberán integrarse a los ya registrados para recibir la capacitación adecuada.

3.5. Del Programa Nacional.

El Programa de Nacional es el conjunto de objetivos políticas, estrategias, líneas de acción y metas para cumplir con el objetivo del Sistema Nacional.

Cuando se identifique riesgos específicos que puedan afectar a la población o se trate de personas minusválidas, de tercera edad y menores de edad se elaborara programas especiales de protección civil.

3.6. De las Declaratorias de Emergencia y De Desastre.

En esta ley el presupuesto de egresos de la federación se hará uso de los recursos financieros a la prevención y atención de desastres atendiendo al de mayor prioridad.

Una vez que se presente la solicitud de un desastre natural las autoridades tendrán un plazo de 12 días naturales para publicarlo en le Diario Oficial de la Federación.

La retención injustificada de recursos por parte de servidores públicos se les sancionara de acuerdo a la ley federal de responsabilidades administrativas de los servidores públicos.

Los recursos para prevención de desastres será administrado en un fideicomiso preventivo a cargo de la Secretaría de Gobernación.



3.7. De las Medidas de Seguridad.

Las unidades Estatales o Municipales aplicaran las medidas de seguridad, cuando se identifique o delimite una zona de riesgo, teniendo acciones preventivas para la movilización de la población a refugios temporales para evitar que siga causando un riesgo.

Cuando se aplique alguna de las medidas de seguridad se indicara su temporalidad para saber en que momento se retiran.

CAPITULO 4

ADMINISTRACION DE RIESGOS

La situación ambiental de las ciudades está directamente relacionada con los problemas que conlleva el acelerado proceso de urbanización, producto de desequilibrios de orden social y económico a través de la historia.

Los riesgos para el ser humano se fueron incrementando en la medida que se desarrollaba la tecnología. Este proceso comienza en forma notoria a partir de los años treinta y se acentúa en la década de los cincuenta que es marcado por el crecimiento de la población y los avances tecnológicos.

La clave del éxito en una empresa consiste en no ignorar los riesgos, estar pendiente de ellos, analizarlos y controlarlos de manera efectiva.

Todas las empresas requieren un enfoque formal de administración de riesgo, pero ésta debe convertirse en un proceso sistemático aplicado de manera disciplinada para obtener el máximo beneficio, de ahí que se pueda definir como:

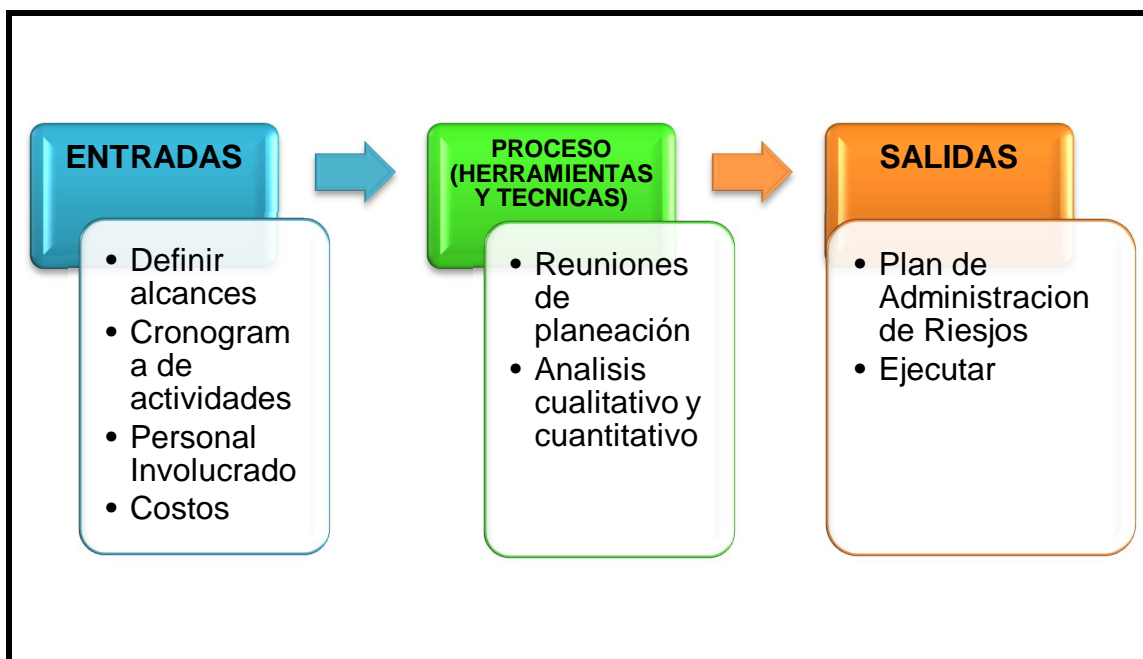
La administración de riesgos es el proceso sistemático de planear, identificar, analizar, responder y controlar los riesgos de una empresa.

Este proceso trata de maximizar la probabilidad de ocurrencia de sucesos positivos y minimizar la de sucesos adversos.

La administración moderna de la seguridad se fundamenta y emplea como sus herramientas los instrumentos clásicos de la administración, por lo que es conveniente comenzar por revisar el Proceso Administrativo.

4.1 Administración y Planeación de Riesgos ¹⁶

En la elaboración de una correcta planeación, en términos generales se constituye por un conjunto de etapas y tareas a cumplir, que genéricamente se concretan en los siguientes rubros:

Figura.- 4.1 Proceso de la planeación de un riesgo.

Fuente: Elaboración propia

En la figura 4.1 tenemos el proceso de planeación de un riesgo por lo que definamos cada una de sus partes:

Entradas

1. Definir los alcances para cada área de trabajo que proporcione una clara percepción de las posibilidades asociadas con el riesgo al que se va enfrentar con sus entregables a cada departamento, con el fin de definir la importancia de la administración de los diferentes riesgos a los que se enfrentaran.
2. La estructura de la organización a menudo restringe la disponibilidad de los términos bajo los cuales los recursos se hacen disponibles para enfrentar el riesgo. Las estructuras organizacionales se pueden caracterizar por una jerarquía donde el empleado tiene un superior claro. Esta estructura deberá definir la forma en que se informara y evaluara las contingencias de los riesgos.



3. Para enfrentar cualquier riesgo se deberá tener un buen líder en la empresa por lo que distinguir entre *liderar* y *gestionar*, enfatizando al mismo tiempo la necesidad de ambos: el uno sin el otro está propenso a producir malos resultados. Señala que gestionar tiene que ver principalmente con “producir consistentemente los resultados claves que, mientras que liderar implica motivar a las personas de una visión del futuro como las estrategias para producir los cambios que sean necesarios para lograr la misión:
- * Alinear a las personas: comunicar la visión por medio de palabras y hechos a todos aquellos cuya cooperación puede ser necesaria para lograr la visión.
 - * Motivar e inspirar: ayudar a las personas a energizarse con el objeto de superar las barreras políticas, burocráticas y de recursos y lograr el cambio.

Proceso (Herramientas y Técnicas)

La *comunicación* implica el intercambio de información. El emisor es el responsable de que la información sea clara, sin ambigüedades y completa, de modo tal que el receptor la pueda recibir correctamente. El receptor es responsable de asegurarse de que la información se reciba en su totalidad y de que se entienda correctamente. La comunicación tiene muchas dimensiones:

1. Escrita y oral, oída y hablada.
2. Formal (reportes, entrevistas, etc.) e informal (memorandos,
3. conversaciones).
4. Verticales (hacia arriba y hacia abajo en la organización) y horizontales (con nuestros compañeros y colegas en la organización).

La planificación es de mayor importancia para un análisis de riesgo, ya que implica realizar algo que no se ha hecho antes. La cantidad de planificación realizada debe ser conmensurada con el alcance y la utilidad de la información desarrollada. Algunos procesos de planificación tienen claras dependencias, como el que ejecuten varias alternativas de respuesta esencialmente en el mismo orden. Las



actividades deben definirse antes de que se puedan programar o costear. Estos procesos centrales de planificación pueden ser iterados varias veces durante cualquier fase de un análisis como:

1. Desarrollar una base escrita de los alcances esperados como base para las futuras decisiones en respuesta ante un riesgo.
2. Subdividir los principales componentes más manejables y más pequeños.
3. Identificar las actividades específicas que se deben ejecutar con mayor prioridad.
4. Analizar las secuencias de las actividades de respuesta y los requerimientos de recursos para crear el programa.
5. Decidir cómo abordar y planificar la gestión de riesgos.
6. Determinar qué recursos (personas, equipos, materiales) y en qué cantidades de cada uno, se deben utilizar para desarrollar las actividades.
7. Desarrollar una aproximación (estimación) de los costos de los recursos requeridos para completar las.
8. Asignar la estimación global de costos a paquetes de trabajo individuales.
9. Realizar un análisis cualitativo de los riesgos y condiciones a fin de priorizar sus efectos.
10. Análisis Cuantitativo del Riesgo que consiste en medir la probabilidad e impacto de los riesgos y estimar sus implicancias.
11. Desarrollar los procedimientos y técnicas para aumentar las oportunidades y reducir las amenazas de riesgo.
12. Determinar qué se debe adquirir, cuánto se debe comprar y cuándo.

Una metodología de planificación es cualquier enfoque estructurado que se utiliza para guiar al equipo durante el desarrollo. La mayoría de las metodologías de planificación hace uso de una combinación de herramientas “duras”, tales como el software de gestión de proyectos, y herramientas “blandas” tales como las reuniones de puesta en marcha.



Salidas

La ejecución del plan del análisis de riesgo es el principal proceso para verificar que dicha administración funcionará adecuadamente. En este proceso, el gerente de la organización y el equipo de gestión deben coordinar y dirigir las distintas interfaces técnicas y organizacionales que existan. Es precisamente, el proceso que está más directamente afectado ya que en este paso se ve directamente la aplicación más directa de dicha administración, para llevar a cabo la ejecución del plan.

Se debe monitorear continuamente el desempeño del plan de análisis de riesgo con respecto a la línea base, de modo tal que se puedan tomar las acciones correctivas sobre la base del rendimiento y desempeño real con relación al plan de administración de riesgos.

Para respaldar este análisis, se debe llevar a cabo predicciones periódicas de los resultados finales de costo.

A menudo, será necesario el juicio experto con el fin de evaluar las entradas para este proceso. Dicha experticia puede ser proporcionada por cualquier grupo o individuo con conocimiento o entrenamiento especializado, y se puede obtener de muchas fuentes, que incluyen:

- * Otras unidades dentro de la organización ejecutante.
- * Consultores
- * Accionistas, incluidos los clientes.
- * Asociaciones profesionales y técnicas

4.2 Identificación del Riesgo¹⁶

La identificación de los riesgos implica determinar que eventos y con cuales características podrían afectar.

Entre los participantes de la identificación de los riesgos, generalmente se incluyen:

- * El equipo de gestión de riesgos
- * Los expertos en temas particulares de otras partes de la compañía



- * Clientes
- * Usuarios finales
- * Gerentes de la empresa
- * Accionistas y expertos externos.

A menudo, se pueden desarrollar e incluso implementar respuestas simples y efectivas frente al riesgo, tan pronto como éste sea identificado.

Entradas para la Identificación de los Riesgos

La identificación de los riesgos requiere de la comprensión de la misión, alcance y objetivos para el responsable de la empresa. Se deberán revisar los resultados de los demás procesos de forma tal de identificar posibles riesgos durante todo el proceso de identificación. Estos pueden incluir, pero sin limitarse a ello:

- * Descripción del proceso de operación.
- * Programa y estimaciones de costos en medida de recuperación.
- * Plan de recursos disponibles.
- * Listas de supuestos y restricciones a tomar para la recuperación.

Los riesgos que pueden afectar al proyecto y pueden identificarse y organizarse en categorías de riesgos.

Las categorías de riesgos deben ser definidas y deben reflejar fuentes comunes de riesgo para la industria o área de aplicación. Las categorías incluyen además de los mencionados en el capítulo 3 son los siguientes:

- * Riesgos técnicos, de calidad o de rendimiento o desempeño, como por ejemplo la dependencia en tecnología compleja o no probada, metas de rendimiento irreales, cambios a la tecnología utilizada o a las normas de la industria durante el proyecto.
- * Riesgos de la gestión como por ejemplo la mala asignación de tiempo y recursos, calidad inadecuada del proceso productivo, incorrecto uso de las disciplinas de gestión de la empresa.
- * Riesgos organizacionales como son: los objetivos de costo, tiempos, falta de prioridad de los procesos de operación en respuesta ante un riesgo, falta



o interrupción del financiamiento y conflictos de recursos con otros procesos que se llevan a cabo en la organización.

- * Riesgos externos como por ejemplo temas laborales, cambio de las prioridades del dueño, riesgo del país y el clima. Los riesgos de fuerza mayor como son los terremotos, las inundaciones y sabotaje (mencionadas en el Capítulo 2), requieren generalmente de acciones de recuperación contra desastres en vez de una gestión de riesgo.

La información sobre riesgos anteriores que pueda obtenerse de las siguientes fuentes:

- * Archivos de riesgos anteriores que es una o más de las organizaciones involucradas en la organización que pueden mantener registros de resultados de respuestas previas, que se puedan utilizar para identificar riesgos. Estos pueden ser informes finales o planes de respuesta al riesgo. Además, pueden incluirse las lecciones organizadas aprendidas que describan los problemas y sus resoluciones, o bien pueden estar disponibles por medio de la experiencia de los trabajadores u otras personas ajenas a la organización.
- * Información publicada basada en datos comerciales, estudios académicos y otros estudios publicados que puedan estar disponibles para muchas áreas de aplicación.

Herramientas y Técnicas para la Identificación de los Riesgos

La revisión de documentación por lo general, los equipos asignados en la administración realizan a etapa inicial una revisión estructura de los planes y supuestos del proyecto en la identificación, tanto a niveles de alcance detallado como del plan final, archivos de documentos anteriores y otra información de tipo similar.

Las Técnicas de recopilación de información son utilizadas en la identificación de riesgos, se pueden incluir entrevistas y análisis de fortalezas, debilidades, oportunidades y amenazas (FODA).



Entre otras técnicas están los siguientes:

- ★ Lluvia de ideas: Esta es quizás la técnica de identificación de riesgos más frecuentemente empleada. El objetivo es obtener una lista amplia de los riesgos que pueden ser abordados más tarde en los procesos de análisis cualitativo y cuantitativo. El Brainstorming es realizado, generalmente, por el equipo asignado para este método basado en la lluvia de ideas, aunque esta técnica también puede ser ejecutada por un grupo multidisciplinario de expertos. Bajo el liderazgo de un facilitador, estas personas generan ideas acerca del riesgo. Se identifican a gran escala las fuentes de riesgos, y se dejan planteadas para que todos la revisen durante la reunión.
- ★ Técnica de Delphi. Esta técnica es una manera de lograr el consenso de los expertos respecto de un tema como puede ser el riesgo en la empresa o industria. Se identifican los expertos en riesgos de la empresa, para que participen en forma anónima. Un facilitador utiliza un cuestionario para solicitar ideas acerca de los riesgos importantes. Se presentan las respuestas y, luego, son hechas llegar ante los expertos seleccionados para mayores comentarios. En unas cuantas iteraciones de este proceso, se puede llegar a un consenso. La técnica Delphi ayudar a reducir el sesgo de la información y evita que cualquier persona tenga influencia indebida en la consecuencia¹⁸.
- ★ Entrevistas. Es posible identificar los riesgos mediante entrevistas con expertos en asuntos específicos o por expertos temáticos. La persona responsable de la identificación de los riesgos identifica a los individuos responsables, les resume el plan y les entrega información como puede ser el listado de supuestos. Las entrevistas identifican los riesgos de la empresa sobre la base de su experiencia u otras fuentes que estos puedan encontrar útiles.
- ★ El análisis FODA: Tiene como objetivo el identificar y analizar las Fuerzas y Debilidades de la Institución u Organización, así como también las Oportunidades y Amenazas. Se utilizará para desarrollar un plan que tome



en consideración muchos y diferentes factores internos y externos para así maximizar el potencial de las fuerzas y oportunidades minimizando así el impacto de las debilidades y amenazas. Se debe de utilizar al desarrollar un plan estratégico, o al planear una solución específica a un problema. Una vez que se ha analizado el ambiente externo (por ejemplo: la cultura, la economía, datos demográficos, etc.)³⁸.

Tabla 4.1.- Matriz FODA³⁸

Análisis	Fortalezas	Debilidades
Interno	<ul style="list-style-type: none"> * Capacidades fundamentales en áreas claves. * Recursos financieros adecuados. * Buena imagen de los compradores. * Ser un reconocido líder en el mercado. * Estrategias de las áreas funcionales bien ideadas. * Acceso a economías de escala. * Propiedad de la tecnología. * Ventajas en costos. * Mejores campañas de publicidad. * Habilidades para la innovación de productos. 	<ul style="list-style-type: none"> * No hay una dirección estratégica clara. * Instalaciones obsoletas. * Falta de oportunidad y talento gerencial. * Seguimiento deficiente al implantar la estrategia. * Atraso en investigación y desarrollo. * Débil imagen en el mercado. * Débil red de distribución. * Incapacidad de financiar los cambios necesarios en la estrategia.
	Oportunidades	Amenazas
Externo	<ul style="list-style-type: none"> * Atender a grupos adicionales de clientes. * Ingresar en nuevos mercados o segmentos. * Expandir la línea de productos para satisfacer una gama mayor de necesidades de los clientes. * Diversificarse en productos relacionados. * Eliminación de barreras comerciales en mercados foráneos atractivos. 	<ul style="list-style-type: none"> * Entrada de competidores foráneos con costos menores. * Incremento en las ventas y productos sustitutos. * Crecimiento más lento en el mercado. * Cambios adversos en los tipos de cambio y políticas comerciales de gobiernos extranjeros. * Requisitos



	<ul style="list-style-type: none">* Complacencia entre las compañías rivales.* Crecimiento más rápido en el mercado	reglamentarios costosos. <ul style="list-style-type: none">* Vulnerabilidad a la recesión y ciclo empresarial.* Creciente poder de negociación de clientes o proveedores..
--	--	---

Lo importante de este análisis es pensar en lo que es necesario buscar para identificar y medir los puntos fuertes y débiles, las oportunidades y las amenazas del proyecto, cuestiones claves que son compiladas y analizadas gráficamente.

Análisis Interno: Para el diagnóstico interno será necesario conocer las fuerzas al interior que intervienen para facilitar el logro de los objetivos, y sus limitaciones que impiden el alcance de las metas de una manera eficiente y efectiva. En el primer caso estaremos hablando de las fortalezas y en el segundo de las debilidades. Como ejemplos podemos mencionar: Recursos humanos con los que se cuenta, recursos materiales, recursos financieros, recursos tecnológicos.

Análisis Externo: Es analizar las condiciones de oportunidades y amenazas de su entorno; identificadas como las oportunidades; así como las tendencias del contexto que en cualquier momento pueden ser perjudiciales y que constituyen las amenazas, con estos dos elementos se podrá integrar el diagnóstico externo. En los ámbitos que se pueden hacer es de carácter político, legal, social o tecnológico.

- * Otra forma de identificar es hacer listas de verificación, basándose en la información histórica y en el conocimiento que se ha acumulado de proyectos previos similares o de otras fuentes de información. Una de las ventajas de utilizar una lista de verificación es que la identificación del riesgo es rápida y sencilla. Una desventaja sería que es imposible construir una lista exhaustiva de los riesgos y, el usuario puede efectivamente limitarse a las categorías que aparecen en el listado. Se debe procurar



explorar en aquellos casos que no aparezcan en una lista de verificación estándar si se considera que estos son relevantes al proyecto en cuestión. La lista debe tener todos los tipos de riesgos posibles para la empresa. Es importante que se revise la lista de verificación como si fuera una etapa formal de cada procedimiento de cierre de proyecto, a objetivo de mejorar el listado de riesgos potenciales, para mejorar la descripción de los riesgos.

- * Análisis de los supuestos. Cada plan de respuesta se concibe y desarrolla sobre la base de un conjunto de hipótesis, escenarios o supuestos. El análisis de los supuestos es una técnica que explora la validez de los mismos.
- * Técnicas de diagramación. Las técnicas de diagramación pueden incluir:
- * Diagramas de causa-y-efecto (también conocidas como diagramas *Ishikawa* o *de espina de pescado*) son útiles para la identificación de las causas de los riesgos. El Diagrama de Causa y Efecto es un gráfico con la siguiente información:
 1. El problema que se pretende diagnosticar
 2. Las causas que posiblemente producen la situación que se estudia.
 3. Un eje horizontal conocido como espina central o línea principal.

El tema central que se estudia se ubica en uno de los extremos del eje horizontal. Este tema se sugiere encerrar con un rectángulo. Es frecuente que este rectángulo se dibuje en el extremo derecho de la espina central.

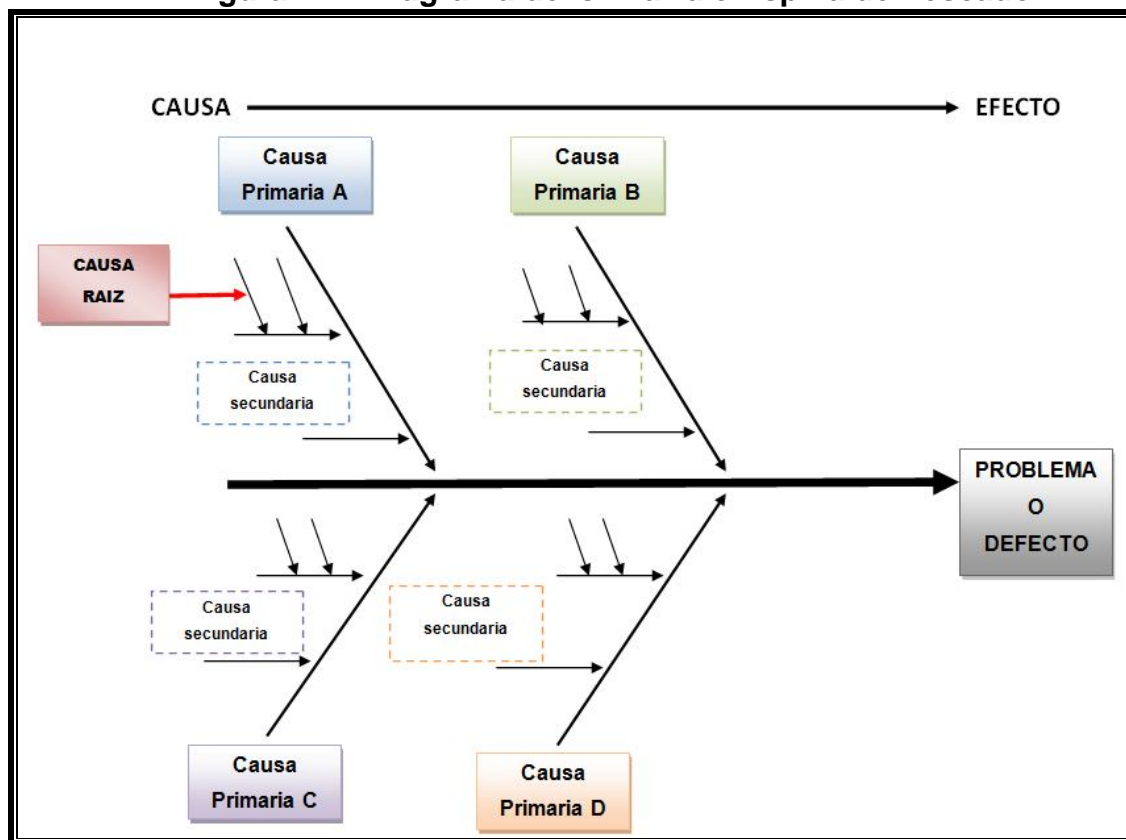
Líneas o flechas inclinadas que llegan al eje principal. Estas representan los grupos de causas primarias en que se clasifican las posibles causas del problema en estudio.

A las flechas inclinadas o de causas primarias llegan otras de menor tamaño que representan las causas que afectan a cada una de las causas primarias. Estas se conocen como causas secundarias.

El Diagrama de Causa y Efecto también conocido como espina de pescado o Ishikawa debe llevar información complementaria que lo identifique. La

información que se registra con mayor frecuencia es la siguiente: título, fecha de realización, área de la empresa, integrantes del equipo de estudio.

Figura 4.2.- Diagrama de Ishikawa o Espina de Pescado²⁰



Resultados de la Identificación de los Riesgos

Riesgos. Un riesgo es un evento o condición incierta que, de llegar a ocurrir, tiene un efecto negativo en un objetivo de la empresa.

Gatilladores. Los gatilladores, o algunas veces denominados síntomas del riesgo o signos de advertencia, son indicaciones de que se ha producido un accidente o bien de que está a punto de ocurrir. Por ejemplo, el no cumplimiento una señal de advertencia temprana de un riesgo importante.



Entradas a otros procesos. La identificación de los riesgos puede identificar una necesidad de mayor acción en otra área. Por ejemplo, la de no tener detalles suficientes como para permitir la adecuada identificación de los riesgos, o bien puede que el programa no esté completo o que no sea completamente lógico.

4.3 PASST (Programa de Autogestión en Seguridad y Salud en el Trabajo)²¹

4.3.1 Breve Historia

El Programa de Autogestión en Seguridad y Salud en el Trabajo tuvo su origen en el año de 1995 en los denominados “Programas Preventivos”, los cuales se aplicaban en centros de trabajo con cien o más trabajadores de la industria maquiladora de exportación de las entidades federativas de la frontera norte del país, así como de Jalisco y el Distrito Federal, con el propósito de promover la implementación de programas preventivos en los centros de trabajo y, de esta manera, también atender los compromisos derivados del Acuerdo de Cooperación Laboral de América del Norte, ACLAN.

El 21 de enero de 1997, se publicó en el Diario Oficial de la Federación el Reglamento Federal de Seguridad, Higiene y Medio Ambiente de Trabajo, el cual señala en el artículo 12 que “La Secretaría llevará a cabo programas de asesoría y orientación para el debido cumplimiento de la normatividad laboral en materia de seguridad e higiene en el trabajo, en los que se establecerán los mecanismos de apoyo para facilitar dicho cumplimiento, así como simplificar la acreditación del mismo, tomando en cuenta la actividad, escala económica, procesos de trabajo, grado de riesgo y ubicación geográfica de los centros de trabajo, a través de compromisos voluntarios con aquellas empresas o establecimientos que así se lo soliciten, para lo cual se auxiliará de la Comisión Consultiva Nacional de Seguridad e Higiene en el Trabajo”.

En 2002, se emiten los lineamientos generales para el “Programa de Autogestión en Seguridad y Salud en el Trabajo”, con objeto de propiciar y fortalecer el manejo



de la seguridad y salud en el trabajo, a través de la participación activa de todos los trabajadores de los centros de trabajo, además de incluir para su atención, los señalamientos antes citados.

Bajo estos lineamientos, se acuña el otorgamiento del reconocimiento de “Empresa Segura” en sus tres niveles:

1. Por el cumplimiento de la normatividad en seguridad y salud en el trabajo.
2. Por las acciones de mejora continua en la seguridad y salud en el trabajo.
3. Por sus logros en la administración de la seguridad y salud en el trabajo.

4.3.2 Estructura del Programa

El objetivo es promover que las empresas instauren y operen Sistemas de Administración en Seguridad y Salud en el Trabajo, con base en estándares nacionales e internacionales, y con sustento en la reglamentación vigente en la materia, a fin de favorecer el funcionamiento de centros laborales seguros e higiénicos.

El Programa de Autogestión en Seguridad y Salud en el Trabajo constituye una acción promocional de la Secretaría del Trabajo y Previsión Social para favorecer la autogestión de los centros de trabajo en la seguridad y salud en el trabajo. El Programa de Autogestión en Seguridad y Salud en el Trabajo está abierto a cualquier tipo de centro de trabajo, con prioridad para aquellas actividades económicas con alta accidentabilidad, siniestralidad o riesgo.

Los procesos de evaluación, dictamen y otorgamiento de reconocimientos son transparentes, al concurrir en forma simultánea personal de las áreas de seguridad y salud en el trabajo y de inspección federal del trabajo, tanto a nivel regional como central.

La Secretaría del Trabajo y Previsión Social difundirá los resultados del Programa de Autogestión en Seguridad y Salud en el Trabajo, los reconocimientos otorgados



a los centros de trabajo, así como las mejores prácticas en la instrumentación de Sistemas de Administración en Seguridad y Salud en el Trabajo

4.3.3 Planeación y Diagnostico

Las autoridades federales del trabajo deberán realizar un análisis sobre el universo de empresas y trabajadores en el ámbito de su competencia, considerando el tamaño de los centros de trabajo. Asimismo, efectuarán un diagnóstico sobre los accidentes de trabajo, las enfermedades laborales, las incapacidades permanentes, las defunciones y los días subsidiados, por división, grupo y actividad económica, que hayan ocurrido en su circunscripción.

Igualmente, deberán evaluar la evolución de la tasa de incidencia de accidentes de trabajo por cada cien trabajadores; la tasa de enfermedades profesionales por cada diez mil trabajadores; la tasa de incapacidades permanentes por cada cien casos, y la de mortalidad por accidentes y enfermedades de trabajo por cada diez mil trabajadores, dentro de su entidad federativa.

Por último, con base en dicha información, las delegaciones federales del trabajo seleccionarán los centros de trabajo, de acuerdo con las actividades económicas o ramas industriales de mayor accidentabilidad, siniestralidad o riesgo en la entidad federativa para considerar su promoción e incorporación al Programa de Autogestión en Seguridad y Salud en el Trabajo.

La Dirección General de Seguridad y Salud en el Trabajo hará del conocimiento de las delegaciones federales del trabajo, por conducto de la Unidad de Delegaciones Federales del Trabajo, aquellas actividades económicas o ramas industriales que determine la Comisión Consultiva Nacional de Seguridad e Higiene en el Trabajo con carácter prioritario a nivel nacional, a fin de promover su incorporación al Programa de Autogestión en Seguridad y Salud en el Trabajo. Los centros de trabajo que cuenten con diversas áreas o procesos industriales de alto riesgo, podrán incorporar al programa de manera gradual las diversas naves, departamentos, áreas, secciones o procesos que los conforman, a las que en lo



sucesivo se les denominará como áreas, considerando inicialmente aquellas con mayor accidentabilidad, siniestralidad o riesgo.

Salud en el Trabajo se sustenta en un proceso de formación de los integrantes de los servicios preventivos de seguridad y salud en el trabajo y de las comisiones de seguridad e higiene, así como de los trabajadores.

La formación de recursos humanos será de manera grupal, por lo que deberá evitarse en lo posible la realización de acciones individuales por centro de trabajo, con el fin de racionalizar y optimizar los recursos que se destinan para tales fines.

Dentro de la organización se llevará la actividad de talleres de administración en seguridad. Esta actividad se deberá desprender de los eventos de difusión con los niveles directivos y gerenciales de los centros de trabajo.

El taller de administración en seguridad y salud en el trabajo se deberá impartir a los integrantes de los servicios preventivos de seguridad y salud en el trabajo y a los líderes del proyecto en la instauración y seguimiento del Sistema de Administración en Seguridad.

A solicitud de los centros de trabajo se incluirá a los contratistas que desarrollen labores relacionadas con la actividad principal dentro de las instalaciones del propio centro de trabajo.

Los centros de trabajo deberán comprometerse a la formación e involucramiento de todos los mandos y supervisores, o puestos afines, así como de los trabajadores, con el apoyo de los servicios preventivos de seguridad y salud en el trabajo.

Además de los talleres de la administración en seguridad se deberá impartir talleres en comisiones de seguridad. Este taller se deberá impartir a los integrantes de las comisiones de seguridad e higiene de los centros de trabajo y de los contratistas que desarrollen labores relacionadas con la actividad principal dentro de las instalaciones del propio centro de trabajo.



Tendrá la finalidad de incorporar a los integrantes de estos organismos al proceso de autogestión, como un mecanismo de evaluación del cumplimiento de la normatividad. El taller para comisiones de seguridad e higiene se deberá impartir dentro de los treinta días naturales siguientes al desarrollo del taller de administración en seguridad y salud en el trabajo.

Estos talleres deberán tener una duración total mínima de 24 horas y deberán impartirse durante la jornada laboral.

4.3.4 Compromiso en la autogestión.

Los centros de trabajo que deseen incorporarse al Programa de Autogestión en Seguridad y Salud en el Trabajo deberán elaborar el Compromiso Voluntario, en forma posterior a la realización del taller de administración en seguridad y salud en el trabajo, de acuerdo con los criterios y lineamientos del programa.

Los centros de trabajo deberán elaborar y presentar ante la delegación federal del trabajo que corresponda los siguientes documentos:

1. Diagnóstico de Administración en Seguridad y Salud en el Trabajo
2. Programa de Seguridad y Salud en el Trabajo
3. Compromiso Voluntario.

1.-Diagnóstico de Administración en Seguridad y Salud en el Trabajo, estará integrado por las siguientes evaluaciones:

- * La evaluación de la administración de la seguridad y salud en el trabajo se realizará mediante la aplicación de la “Guía de Asesoría para la Instauración de Seguridad y Salud en el Trabajo”, para identificar las debilidades, áreas de oportunidad y fortalezas de la gestión en esta materia.



- * La evaluación del cumplimiento de la normatividad en seguridad y salud en el trabajo se efectuará a través de la “Guía para la Evaluación del Cumplimiento de la Normatividad en Seguridad y Salud en el Trabajo”. Su aplicación se deberá realizar por área del centro de trabajo, con el objeto de identificar y ubicar con precisión las debilidades en la observancia de las normas de seguridad y salud en el trabajo.
- * La evaluación de los accidentes y enfermedades de trabajo se realizará con base en la información del centro de trabajo y de los contratistas que desarrollen labores relacionadas con la actividad principal dentro de las instalaciones del propio centro de trabajo. Dicha información deberá contener por cada área del centro de trabajo: accidentes de trabajo; enfermedades laborales; incapacidades permanentes; defunciones, y días subsidiados. Asimismo, la tasa de accidentes de trabajo por cada cien trabajadores; la tasa de enfermedades laborales por cada diez mil trabajadores; la tasa de incapacidades permanentes por cada cien casos, y la tasa de defunciones por cada diez mil trabajadores. En el caso de los centros de trabajo que se encuentren sujetos de aseguramiento del régimen obligatorio del seguro social, se deberá acompañar copia de la última Determinación de la Prima en el Seguro de Riesgos de Trabajo, derivada de la Revisión Anual de la Siniestralidad, y la Relación de riesgos de trabajo terminados presentada al Instituto Mexicano del Seguro Social, sellados por dicha institución. Para los que no sean sujetos de aseguramiento del régimen obligatorio del seguro social, deberán acompañar copia del reporte instaurado para el seguimiento de los accidentes y enfermedades de trabajo, validado por la comisión de seguridad e higiene.

2.- Programa de Seguridad y Salud en el Trabajo

Dicho programa proveerá los elementos para la mejora continua del Sistema y el cumplimiento de la normatividad en la materia.



El Programa de Seguridad y Salud en el Trabajo podrá formularse por escrito o en medios electrónicos. Su contenido habrá de estar sustentado en los resultados obtenidos a partir del Diagnóstico de Administración en Seguridad y Salud en el Trabajo.

Dicho programa deberá contener al menos las actividades para el cumplimiento de la normatividad en la materia; las fechas de inicio y término programadas para cada una de ellas, así como el responsable de su ejecución.

Para su seguimiento y control, el programa deberá contar con indicadores de resultados que faciliten la toma de decisiones para actuar de manera inmediata y oportuna en la prevención de los accidentes y enfermedades de trabajo.

3.-Compromiso Voluntario.

El Compromiso Voluntario es el documento mediante el cual los centros de trabajo formalizarán su registro en el Programa de Autogestión en Seguridad y Salud en el Trabajo. Deberá ser firmado por los representantes legales de los empleadores y de los trabajadores.

Cuando en un centro de trabajo no exista sindicato, se deberá nombrar por consenso a los representantes de los trabajadores.

Tratándose de empresas contratistas que desarrollen labores relacionadas con la actividad principal del centro de trabajo dentro de las instalaciones de éste último, el compromiso deberá constar del Compromiso Voluntario o en el contrato que se suscriba entre el centro de trabajo y la empresa contratista.

4.3.5 Evaluación del Sistema de Administración en Seguridad y Salud en el Trabajo.

La evaluación se realizará a través de revisiones iniciales e integrales.

Dichas evaluaciones se deberán llevar a cabo por parte de un asesor en seguridad y salud en el trabajo y de un inspector federal del trabajo de la delegación federal



del trabajo que corresponda, bajo la coordinación del delegado federal del trabajo al que se encuentren adscritos.

En las evaluaciones deberán participar por parte de los centros de trabajo, los representantes legales del empleador y de los trabajadores, los integrantes de los servicios preventivos de seguridad y salud en el trabajo y los integrantes de la comisión de seguridad e higiene.

Los resultados de dichas evaluaciones se deberán registrar en minutas de evaluación inicial o integral, según corresponda, las cuales deberán ser firmadas al margen y al calce por los representantes legales del empleador y de los trabajadores; los integrantes de los servicios preventivos de seguridad y salud en el trabajo; los integrantes de la comisión de seguridad e higiene, así como por el asesor de seguridad y salud en el trabajo y el inspector federal del trabajo de la delegación federal del trabajo que corresponda.

Los hallazgos que resulten con motivo de las evaluaciones iniciales e integrales deberán incorporarse al Programa de Seguridad y Salud en el Trabajo.

Evaluaciones iniciales.

Las evaluaciones iniciales deberán realizarse dentro de los 180 días naturales siguientes a la fecha de autorización del Compromiso Voluntario, y tendrán por objeto validar:

- a. La normatividad en seguridad y salud en el trabajo que aplica de manera general y para cada área del centro de trabajo.
- b. La distribución de las áreas del centro de trabajo para la aplicación de la “Guía para la Evaluación del Cumplimiento de la Normatividad en Seguridad y Salud en el Trabajo”.
- c. El sistema de información sobre accidentes y enfermedades de trabajo con que deberá contar el centro de trabajo para conocer los resultados con motivo de la instauración de su Sistema de Administración en Seguridad y Salud en el Trabajo.



- d. Al concluir la evaluación inicial, el asesor de seguridad y salud en el trabajo y el inspector federal del trabajo deberán elaborar la “Minuta de Evaluación Inicial”, con los resultados de su intervención. Dicha minuta deberá ser revisada por el jefe o jefes inmediatos de dichos servidores públicos.

Evaluaciones integrales.

Las evaluaciones integrales se deberán realizar a los centros de trabajo a partir de la evaluación inicial, a petición del centro de trabajo o dentro del año siguiente a la fecha del levantamiento de la minuta que corresponda a la evaluación inicial o a la evaluación integral inmediata anterior. Esta actividad tendrá el propósito de evaluar:

1. El funcionamiento de los Sistemas de Administración en Seguridad y Salud en el Trabajo;
2. El cumplimiento de la normatividad en seguridad y salud en el trabajo;
3. El avance en el Programa de Seguridad y Salud en el Trabajo, y
4. La prevención de los accidentes de trabajo y sus consecuencias.

Los centros de trabajo con Sistemas de Administración en Seguridad y Salud en el Trabajo alineados al PASST y validados por la STPS, deberán enviar a la delegación federal del trabajo que corresponda la documentación que para tal fin se señale en el convenio de concertación correspondiente.

Reconocimiento de “Empresa Segura”

Aquellos centros de trabajo que reciban la revalidación del reconocimiento del tercer nivel de “Empresa Segura” por segunda ocasión o subsecuentemente, deberán enviar a la delegación federal del trabajo cada cinco años, contados a partir de la fecha del otorgamiento de dicho reconocimiento.

Las delegaciones federales del trabajo deberán dar seguimiento a los resultados de los centros de trabajo que hayan obtenido el reconocimiento de “Empresa Segura” en su tercer nivel.



En caso de que dichos resultados no se ubiquen dentro de los criterios antes mencionados, estos lineamientos, las delegaciones federales del trabajo promoverán reuniones con los servicios preventivos de seguridad y salud en el trabajo y las comisiones de seguridad e higiene, a efecto de analizar y determinar las áreas de oportunidad que presenten los Sistemas.

Al término de cada periodo de vigencia del reconocimiento de “Empresa Segura”, las delegaciones federales del trabajo deberán proceder a la evaluación integral del centro de trabajo.

En la siguiente etapa de reconocimiento de “Empresa Segura” se otorgará en cuatro niveles, divididos en dos etapas.

En la primera etapa se contemplan los reconocimientos de “Empresa Segura” en sus tres primeros niveles. El propósito último de ésta etapa será lograr que los centros de trabajo obtengan el reconocimiento de “Empresa Segura” en su tercer nivel.

El reconocimiento de “Empresa Segura” en su tercer nivel deberá revalidarse por vez primera, a los tres años contados a partir de la fecha de su otorgamiento y, posteriormente, cada cinco años, siempre y cuando el centro de trabajo obtenga resultados satisfactorios en la gestión de la seguridad y salud en el trabajo, el cumplimiento de la normatividad, el avance en su Programa de Seguridad y Salud en el Trabajo, así como en la prevención de los accidentes de trabajo y sus consecuencias.

En la segunda etapa se promoverá que los centros de trabajo con reconocimiento de “Empresa Segura” en su tercer nivel o revalidación de éste, participen en la promoción, asesoría y asistencia técnica del PASST, al promover la incorporación de sus clientes, proveedores u otros centros de trabajo en dicho programa.

En estos casos, al término de la vigencia del reconocimiento de “Empresa Segura” en su tercer nivel o revalidación de éste, y cuando los centros de trabajo cumplan con los criterios del Programa y se les otorgará el que corresponde al cuarto nivel, cuyos periodos de revalidación se apejarán a los del tercer nivel.



NIVELES DE EMPRESA SEGURA

Nivel	Denominación del nivel
1	Por el cumplimiento de la normatividad en seguridad y salud en el trabajo.
2	Por las acciones de mejora continua en la seguridad y salud en el trabajo.
3	Por sus logros en la administración de la seguridad y salud en el trabajo.
Revalidación del tercer nivel:	Por la eficaz administración de la seguridad y salud en el trabajo.
4	Por su liderazgo en la seguridad y salud en el trabajo.

Los centros de trabajo que obtengan el reconocimiento de “Empresa Segura” en su tercer nivel o la revalidación de éste, podrán solicitar la Acreditación de su Sistema de Administración y Seguridad en el Trabajo, con base en el “Acuerdo por el que se establecen los requisitos para obtener la Acreditación del Sistema de Administración y Seguridad en el Trabajo.

Primer nivel.- Por el cumplimiento de la normatividad en seguridad y salud en el trabajo.

Elemento	Calificación/Criterio
Funcionamiento del Sistema de Administración en Seguridad y Salud en el Trabajo.	30%
Cumplimiento de la normatividad en seguridad y salud en el trabajo.	80%
Avances del Programa de Seguridad y Salud en el Trabajo.	90%
Accidentes de trabajo.	Los centros de trabajo deberán presentar una tasa de accidentes de trabajo por debajo de la que registraron cuando se incorporaron al Programa Este criterio se aplicará cuando los registros iniciales se hayan ubicado por arriba de los promedios generales nacional y de la actividad económica que tienen registrada ante el Instituto Mexicano del Seguro Social. En caso contrario, la tasa de accidentes de trabajo deberá ubicarse por debajo del promedio general de la actividad económica que tienen registrada ante el



	Instituto Mexicano del Seguro Social.
Incapacidades permanentes y defunciones por accidentes de trabajo.	Los casos de incapacidades permanentes por cada cien casos y las defunciones por cada diez mil trabajadores deberán ubicarse por debajo de los que registró cuando se incorporó al Programa.
Días subsidiados por accidentes de trabajo.	Los días subsidiados por accidentes de trabajo deberán ubicarse por debajo de los que registró cuando se incorporó al Programa.

Segundo nivel.- Por las acciones de mejora continua en la seguridad y salud en el trabajo.

Elemento	Calificación/Criterio
Funcionamiento del Sistema de Administración en Seguridad y Salud en el Trabajo.	70%
Cumplimiento de la normatividad en seguridad y salud en el trabajo.	85%
Avances del Programa de Seguridad y Salud en el Trabajo.	90%



Accidentes de trabajo.	Los centros de trabajo deberán presentar una tasa de accidentes de trabajo por debajo de la que registraron cuando se incorporaron al Programa de Autogestión en Seguridad y Salud en el Trabajo.
Incapacidades permanentes y defunciones por accidentes de trabajo.	Los casos de incapacidades permanentes por cada cien casos y las defunciones por cada diez mil trabajadores deberán ubicarse por debajo de los que correspondan a la actividad económica que tienen registrada ante el Instituto Mexicano del Seguro Social
Días subsidiados por accidentes de trabajo.	Los días subsidiados por accidentes de trabajo deberán ubicarse por debajo de los que correspondan a la actividad económica que tienen registrada ante el Instituto Mexicano del Seguro Social

Tercer nivel.- Por sus logros en la administración de la seguridad y salud en el trabajo.

Elemento	Calificación/Criterio
Funcionamiento del Sistema de Administración en Seguridad y Salud en el Trabajo.	90%
Cumplimiento de la normatividad en seguridad y salud en el trabajo.	90%
Avances del Programa de Seguridad y Salud en el Trabajo.	90%



Accidentes de trabajo.	Los centros de trabajo deberán presentar una tasa de accidentes de trabajo por debajo de los promedios generales nacional y de la actividad económica que tienen registrada ante el Instituto Mexicano del Seguro Social.
Incapacidades permanentes y defunciones por accidentes de trabajo.	Los centros de trabajo no deberán presentar incapacidades permanentes ni defunciones por accidentes de trabajo en el período evaluado.
Días subsidiados por accidentes de trabajo.	Los días subsidiados por accidentes de trabajo deberán ubicarse por debajo de los promedios generales nacional y de la actividad económica que tienen registrada ante el Instituto Mexicano del Seguro Social.

4.3.6 Restricciones del Programa

A los centros de trabajo que tengas recipientes sujetos a presión y calderas no se otorgará reconocimiento alguno, si los centros de trabajo tienen pendiente la autorización provisional o de continuidad de vigencia de recipientes sujetos a presión o calderas.

Los centros de trabajo que tengan recipientes sujetos a presión o calderas sin la autorización provisional correspondiente, deberán comprometer su regularización, a través del Programa de Seguridad y Salud en el Trabajo. La programación para su cumplimiento no deberá exceder el periodo de un año a partir de la fecha de elaboración de su Compromiso Voluntario.

Las Direcciones Generales de Seguridad y Salud en el Trabajo y de Inspección Federal del Trabajo podrán otorgar un plazo distinto al antes referido, cuando el número de recipientes sujetos a presión y calderas pertenecientes a un centro de trabajo imposibiliten su regularización en un plazo de un año.

Las delegaciones federales del trabajo deberán promover que los centros de trabajo que tengan recipientes sujetos a presión o calderas con la autorización provisional correspondiente, soliciten a éstas o a la autoridad estatal competente, la autorización definitiva mediante las inspecciones convenientes, o bien, a través de unidades de verificación. Dichas solicitudes deberán presentarse dentro de los



180 días naturales siguientes a la fecha de autorización de su Compromiso Voluntario.

CAPITULO 5

ANÁLISIS DE RIESGOS Y EMERGENCIAS

En sentido amplio, análisis del riesgo implica cualquier método, cualitativo o cuantitativo, para evaluar el impacto del riesgo en la toma de decisiones. Existen numerosas técnicas al respecto, y el objetivo es ayudar a quien debe tomar una decisión a seleccionar un curso de acción, una vez que se comprenden mejor los resultados posibles que pueden ocurrir.

Una vez que se reconoce una situación riesgosa, el paso siguiente es *cuantificar el riesgo* que involucra esa situación de incertidumbre.

Cuantificar el riesgo significa determinar todos los valores posibles que una variable riesgosa puede tomar y determinar la probabilidad relativa de cada uno de esos valores.

5.1 Análisis Cualitativo

El análisis cualitativo del riesgo es el proceso por el cual se evalúa el impacto y la probabilidad de los riesgos identificados. Este proceso prioriza los riesgos de acuerdo a su efecto potencial en los objetivos del proyecto. El análisis cualitativo de los riesgos es una forma de determinar la importancia de abordar los riesgos específicos y de guiar las respuestas al riesgo. La criticidad puntual de las acciones relacionadas con los riesgos puede magnificar la importancia de un riesgo. La verificación de la calidad de la información disponible ayuda, también, a modificar la evaluación del riesgo.

Las tendencias en los resultados cuando se repiten los análisis cualitativos, pueden indicar a necesidad de más o menos acción de gestión del riesgo. El uso de estas herramientas ayuda a corregir los sesgos que suele haber en un plan de proyecto. Este análisis debe ser revisado durante el ciclo de vida para estar al día de los cambios en sus riesgos¹⁶.



5.1.1 Entradas para el Análisis Cualitativo de los Riesgos¹⁶

1. Registro de Riesgo: Se evalúan los riesgos descubiertos durante el proceso de identificación de riesgos en conjunto con sus impactos potenciales.
2. Avances en el Análisis. La incertidumbre de un riesgo suele depender del avance del análisis a través de su ciclo de vida. En la parte inicial, muchos riesgos aún no han aparecido. Pero como puede haber cambios que aumenta la probabilidad de que se descubran otros riesgos.
3. Precisión de la información. La precisión describe el grado hasta donde se conoce y se entiende el riesgo. Esta mide el grado de información disponible, y la confiabilidad de los datos. Se debe evaluar además la fuente de información que se utilizó para identificar el riesgo.

5.1.2 Técnicas para el Análisis Cualitativo de los Riesgos¹⁶

Se puede describir la probabilidad y las consecuencias de los riesgos en términos cualitativos como por ejemplo: muy alto, alto, moderado, bajo y muy bajo.

La *probabilidad del riesgo* es la posibilidad de que ocurra un accidente. Las *consecuencias del riesgo se traducen* en la probabilidad y consecuencias de un evento no deseado. Estas dos dimensiones del riesgo se aplican a eventos de riesgos específicos, no a todo el proyecto. El análisis de los riesgos utilizando la probabilidad y las consecuencias ayuda a identificar aquellos riesgos que deben ser controlados o manejados de manera agresiva.

Se puede construir una matriz que asigne una ponderación a los riesgos (muy baja, baja, moderada, alta y muy alta) a los riesgos o condiciones, sobre la base de combinar las escalas de probabilidad e impacto. Los riesgos con alta probabilidad y alto impacto, están propensos a requerir un mayor análisis, incluida la cuantificación y una gestión agresiva del riesgo. La ponderación de los riesgos se lleva a cabo utilizando una matriz y las escalas de riesgos para cada uno de estos eventos o condiciones.

La evaluación de la probabilidad del riesgo puede ser difícil dado que se utiliza el juicio experto, a menudo sin el beneficio de la información histórica. Se podría utilizar



una escala ordinal, que represente valores de probabilidad relativa desde muy probable a casi cierto. De modo alternativo, se podrían asignar probabilidades específicas, utilizando una escala general.

El impacto puede ser ordinal o cardinal, dependiendo de la cultura de la organización que realice el análisis. Las escalas ordinales son simplemente valores ordenados por rangos, como por ejemplo: muy bajo, bajo, moderado, alto y muy alto. Las escalas cardinales asignan valores a estos impactos. Se usan valores generalmente lineales pero suelen ser en realidad no lineales, lo que refleja el deseo de la organización de evitar los riesgos de alto impacto.

La tabla 5.1 es un ejemplo de evaluación de los impactos de los riesgos por medio del objetivo. Esta ilustra su utilización de, ya sea, la metodología ordinal y cardinal. Estos descriptores escalados de impacto relativo deben ser preparados por la organización.

Tabla 5.1 Impacto del Riesgo¹⁶

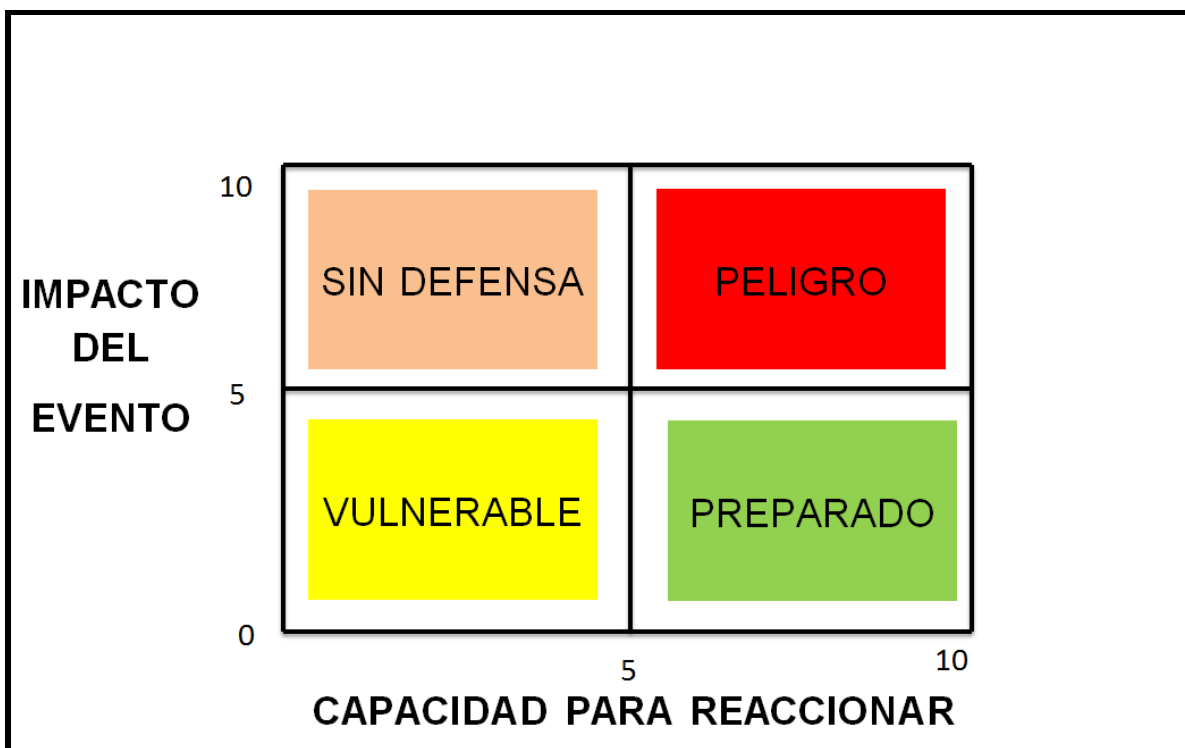
Impacto del Riesgo (Escala Ordinal y Escala no Lineal)					
Impacto(ordinal) Riesgo(cardinal)	Muy Bajo 0.05	Bajo 0.10	Moderado 0.20	Alto 0.40	Muy Alto 0.80
Costo	Aumento de costos < 1%	Aumento de costos 1-5%	Aumento de costos 6-10%	Aumento de costos 11-20%	Aumento de costos > 20%
Tecnológicos	< 2	3-5	6-15	16-30	>30
Políticos	< 5	3-10	11-20	21-40	> 40

La figura 5.2 es una matriz del impacto con la capacidad de reacción de la empresa. Esta figura ilustra la tendencia a cuantificar en que lado de la matriz se encuentra dependiendo de la identificación de los pilares de la organización, como de las



amenazas que tiene. Por ejemplo si el impacto es de 4 y la capacidad de reaccionar es de 9 la organización esta preparada para enfrentar ese evento, pero si el impacto que puede sufrir en una amenaza es de 10 y con una capacidad de reacción de 2 estamos en serios problemas ya que la organización estará sin defensa alguna.

Figura 5.1 Matriz de impacto y capacidad de reacción



Los supuestos probados deben ser evaluados con respecto a dos criterios: la estabilidad del supuesto y las consecuencias del impacto.

El análisis cualitativo de los riesgos requiere de información concreta o específica. La clasificación de la precisión de la información es una técnica que permite evaluar la utilidad de dicha información para la gestión de los riesgos. Esto implica:

- * Nivel de comprensión del riesgo.
- * Información disponible acerca del riesgo.
- * Calidad de los datos.
- * Confiabilidad e integridad de la información



El uso de información de baja precisión provoca que no se entienda bien un riesgo y puede conducir a un análisis cualitativo del riesgo de poca utilidad para el gerente de la empresa. Si fuera inaceptable la clasificación de la precisión de la información, debe recopilar mejores datos¹⁷.

5.1.3 Clasificación global del riesgo

La clasificación del riesgo indica que posición global de riesgo es útil para asignar personal u otros recursos, para tomar una decisión de análisis costo- beneficio.

Se pueden priorizar los riesgos y condiciones por medio de criterios como: alto, moderado y bajo. También pueden ser agrupados por aquellos que requieren una respuesta de corto, mediano o largo plazo. Otra forma de evaluación es estudiar separadamente la funcionalidad y la calidad. Los riesgos significativos deben tener una descripción de la base para la probabilidad e impacto evaluados.

Los riesgos clasificados como altos o moderados serían los primeros candidatos a mayores análisis, incluidos su análisis cuantitativo y las acciones de gestión del riesgo. En la medida que se repita el análisis, puede hacerse notar una tendencia de los resultados, y puede hacer que la respuesta al riesgo sea más urgente e importante²⁰.

5.2 Análisis Cuantitativo

El proceso del análisis cuantitativo de los riesgos está orientado a analizar numéricamente la probabilidad de cada uno de los accidentes y sus consecuencias para la empresa, como así también el grado de riesgo al global. Este proceso utiliza las decisiones Monte Carlo y el análisis de decisiones para:

- * Determinar la probabilidad de lograr un objetivo específico.
- * Cuantificar la exposición al riesgo y determinar el tamaño de las reservas de contingencia de costo y programa que puedan ser necesarias.
- * Identificar los riesgos que requieran mayor atención, cuantificando su contribución relativa al riesgo.



-
- * Identificar las metas realistas y alcanzables de costo, programa o alcance

5.2.1 Entradas para el Análisis Cuantitativo de los Riesgos¹⁶

Una vez que se tiene la planeación (como se mencionó en el capítulo anterior) se toma la información histórica de situaciones similares a partir de fuentes propias o industriales.

Los resultados más sobresalientes son la logística, las estimaciones de tiempos, el listado de costo con sus respectivas estimaciones de la empresa.

5.2.2 Técnicas para el Análisis Cuantitativo de los Riesgos¹⁶

Las técnicas para el análisis cuantitativo son varias por lo que se hablara de las siguientes:

- * Entrevista
- * Análisis de sensibilidad
- * Análisis de árbol de decisiones
- * Simulación.

Entrevista

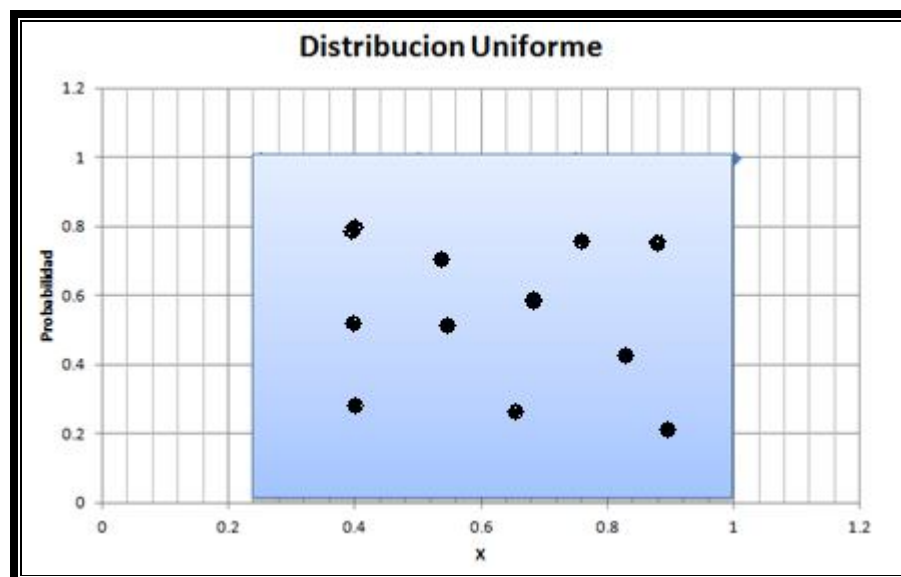
Una primera etapa en la cuantificación de los riesgos puede ser una entrevista con los accionistas de la empresa y los expertos en materias particulares. La información necesaria depende del tipo de distribuciones probabilísticas que se emplearán. Por ejemplo, se recopilaría información sobre escenarios optimistas (bajo), pesimistas (alto) y sobre los escenarios más probables en caso de utilizar distribuciones triangulares; o bien sobre la media y la desviación estándar en el caso de distribuciones normales o normales logarítmicas.

En el análisis cuantitativo de riesgos se suelen emplear distribuciones probabilísticas continuas. Las distribuciones representan tanto la probabilidad como las consecuencias. Entre los tipos de distribución comunes se incluyen: uniforme, triangular, beta y logarítmica normal.

★ *Distribución Uniforme*²²

La distribución Uniforme es el modelo continuo más simple. Corresponde al caso de una variable aleatoria que sólo puede tomar valores comprendidos entre dos extremos a y b , de manera que todos los intervalos de una misma longitud tienen la misma probabilidad. También puede expresarse como el modelo probabilístico correspondiente a tomar un número al azar dentro de un intervalo $(0.2- 1)$. De la anterior definición se desprende que la función de densidad debe tomar el mismo valor para todos los puntos dentro del intervalo $(0.2- 1)$ (y cero fuera del intervalo).

Figura 5.2.- Distribución uniforme



Fuente: Elaboración Propia

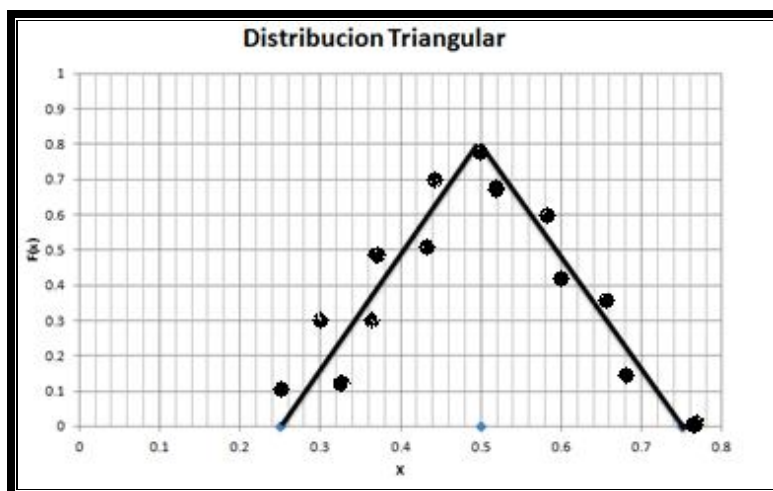
★ *Distribución triangular.*

Se define por tres parámetros: el mínimo a (0.24), el máximo b (0.74), y el valor más probable c (0.8). Variando la posición del valor más probable con relación a los extremos, la distribución puede ser simétrica o no²².

La distribución triangular con función de densidad de probabilidad es útil como una aproximación inicial en situaciones en que no es posible obtener datos confiables o en situaciones en que se disponen de pocos de ellos. Esta distribución se emplea en economía, donde el interés de estudio se refiere al análisis de la duración de

proyectos económicos usando las siguientes estimaciones: optimista, pesimista y más probable.²³

Figura 5.3.- Distribución triangular

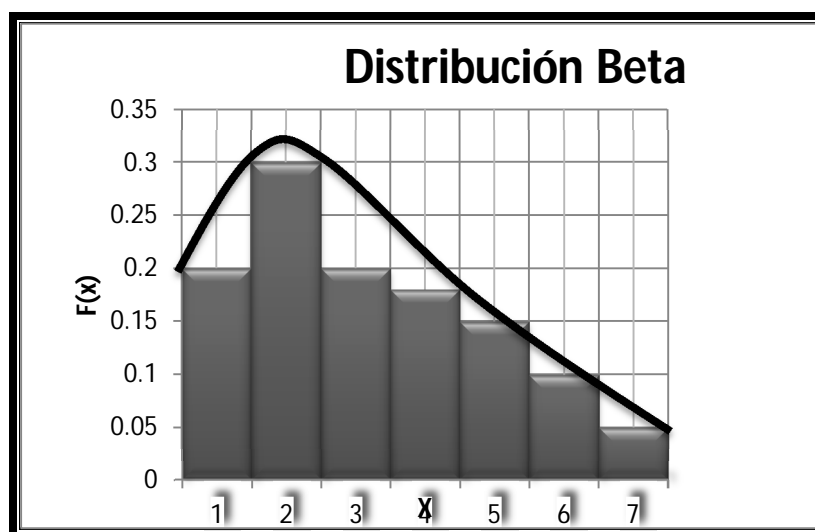


Fuente: Elaboración Propia

★ *Distribución Beta*

Esta distribución tiene un sesgo hacia aquellos eventos de alto impacto. A diferencia de la distribución triangular que requiere 3 valores en beta es necesario contar con más datos para evaluar si se ajusta a este tipo de distribución². Ver figura 5.5

Figura 5.4.- Distribución Beta



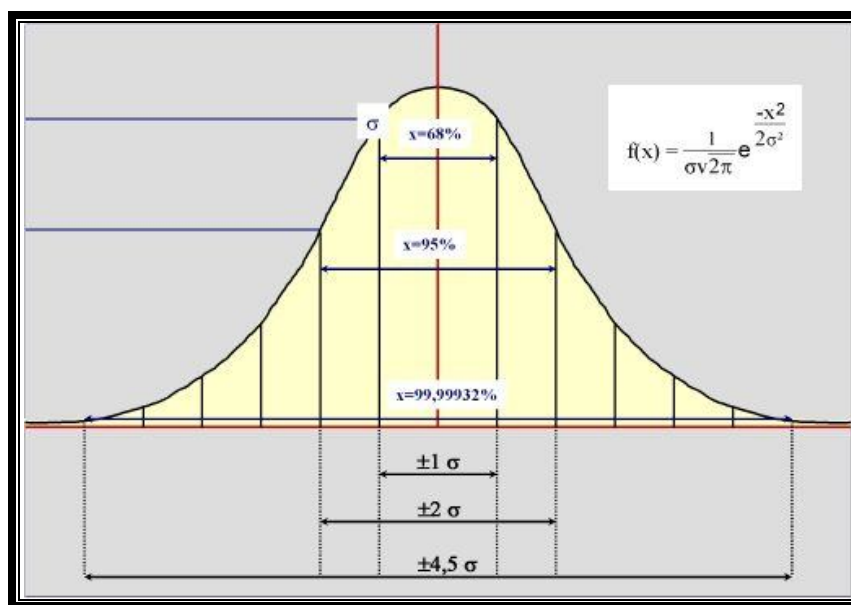
Fuente: Elaboración Propia

* *Logarítmica normal*

La distribución teórica mejor estudiada es la distribución normal, también llamada distribución gaussiana. Su importancia se debe fundamentalmente a la frecuencia con la que distintas variables asociadas a fenómenos naturales y cotidianos siguen, aproximadamente, esta distribución²⁴.

- El punto más alto corresponde al valor con mayor probabilidad de ocurrencia
- La distribución normal es simétrica
- El área bajo la curva es igual a 1
- La desviación estándar (σ) es la medida de la dispersión de los datos respecto a la media

Figura 5.5.- Campana de Gauss²⁴



Análisis de sensibilidad.

El análisis de sensibilidad ayuda a determinar cuáles riesgos tienen el mayor impacto potencial en la empresa. Este análisis revisa el grado con el cual la incertidumbre de cada elemento afecta el objetivo que se está revisando.



El primer paso para reconocer la incertidumbre es examinar como el cambio en una variable afecta un resultado. Esto permite identificar las variables más críticas o construir escenarios posibles que permitan analizar el comportamiento de un resultado bajo diferentes supuestos. El análisis de sensibilidad permite medir el cambio en un resultado, dado un cambio en un conjunto de variables, tanto en términos relativos como en términos absolutos¹. En dicho análisis deben tomar en cuenta los siguientes aspectos:

- a. Reconocer que el cambio en el resultado depende de cómo se haya construido el modelo y de los valores iniciales de las variables por analizar.
- b. Que los cambios en las variables deben ser iguales para todas de manera que se puedan comparar los resultados.
- c. Reconocer la posibilidad de que las relaciones entre las variables y los resultados no sean lineales.
- d. Al analizar la sensibilidad de las variables hay que hacerlo de una en una si se desea determinar cuales de las variables son las más críticas.

Análisis de árbol de decisiones².

El árbol de decisión es un diagrama que describe una determinada decisión y las implicancias de elegir una u otra de las alternativas disponibles. La solución del árbol indica cuál de las soluciones arroja el mayor valor esperado para el encargado de la toma de decisiones. Se cuantifican todas las implicancias, costos, recompensas inciertas y las decisiones subsecuentes.

En resumen, los árboles de decisión proveen un método efectivo para la toma de decisiones debido a que:

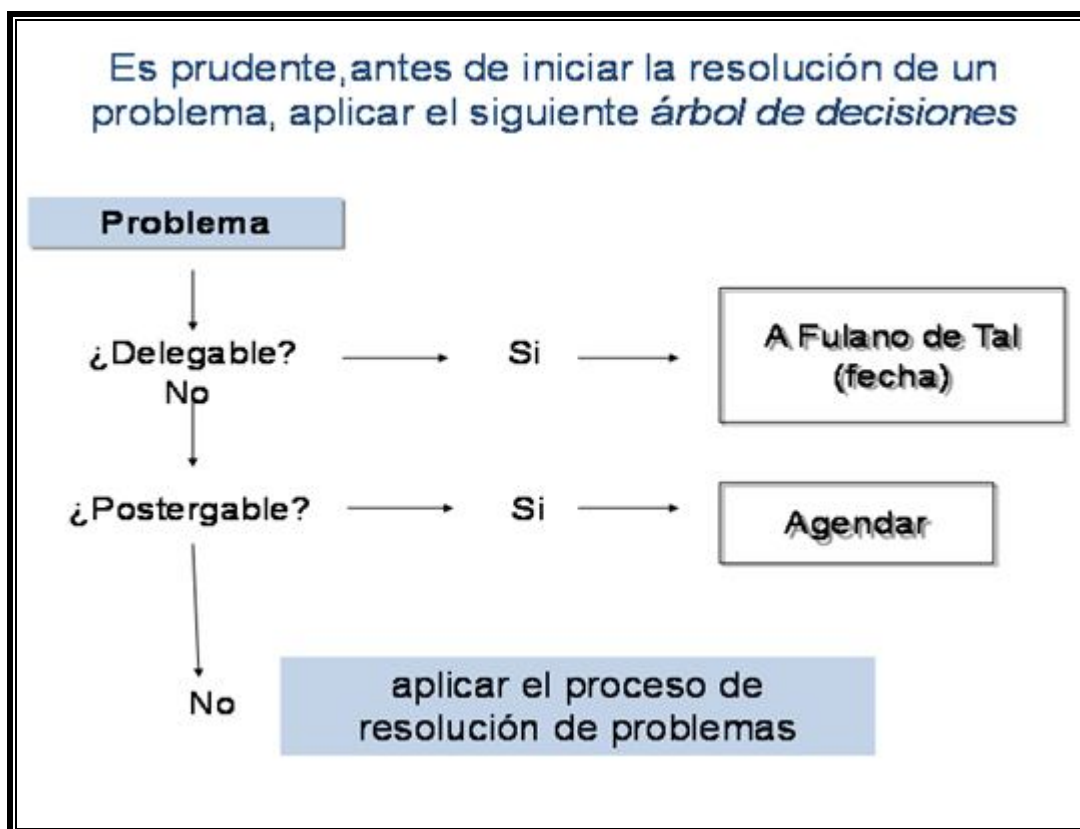
- * Claramente plantean el problema para que todas las opciones sean analizadas.
- * Permiten analizar totalmente las posibles consecuencias de tomar una decisión.

¹ Análisis de Sensibilidad, Ignacio Vélez Pareja. Politécnico Gran colombiano Bogota.2003



- * Proveen un esquema para cuantificar el costo de un resultado y la probabilidad de que suceda.
- * Nos ayuda a realizar las mejores decisiones sobre la base de la información existente y de las mejores suposiciones.

Figura 5.5.-Diagrama de árbol de decisiones



Simulación.

La simulación de un proyecto utiliza un modelo que traduce las incertidumbres especificadas a un nivel de detalle en su impacto potencial en los objetivos que se expresan a nivel del proyecto total. Las simulaciones de proyectos son realizadas, por lo general, utilizando la técnica de Monte Carlo.

El método Monte Carlo, simula los resultados que puede asumir el valor esperado de una variable a través de la asignación aleatoria de un valor a cada variable independiente que lo afecta. Ejemplo.



A cada una de estas variables independientes se le asigna una distribución de probabilidad. Supongamos un proyecto donde se quiere evaluar la rentabilidad de un hotel a construir. La rentabilidad de este hotel se medirá por su valor actual neto. Entre las variables que influyen sobre la rentabilidad del proyecto se pueden mencionar: la tasa de interés, la tasa de impuestos, los costos variables, la inversión. La simulación Monte Carlo puede incluir todas las combinaciones posibles de las variables que afectan los resultados del proyecto.

En primer lugar, se elige cual es la distribución de probabilidad de cada variable que afecta los objetivos. Este análisis ayuda a definir distribución de probabilidad de cada variable. Se debe realizar para todas aquellas variables que influyen en la rentabilidad de los objetivos. El análisis se adaptará al comportamiento que se ajuste más al modelo que se planteo. (Uniforme, triangular, beta, etc.)

La computadora asignará valores aleatorios a todas las variables que afectan al problema plantado en forma simultánea. De esta forma, se podrán correr miles de escenarios, y cada uno se obtendrá un indicador de rentabilidad.

Con el uso del riesgo cuantitativo, es posible calcular la probabilidad de lograr los objetivos con conformidad con el actual plan y con el conocimiento que en el momento se tenga de los riesgos que enfrenta la empresa.

En la medida que se repite el análisis, puede hacerse notoria una tendencia de los resultados²⁵.

5.3 Planificación de la Respuesta al Riesgos

La planificación de la respuesta al riesgo es el proceso por el cual se estudian los riesgos cualitativa y cuantitativamente y se determinan las acciones para mejorar las oportunidades de evitar el accidente o riesgo a la producción de la empresa. Esto incluye la identificación y asignación de individuos o partes para que asuman su responsabilidad para cada respuesta al riesgo que se encuentre. Este proceso asegura que los riesgos identificados sean adecuadamente abordados. La efectividad de la planificación de la respuesta determinará directamente si el grado de disminución del riesgo.



La planificación de la respuesta frente al riesgo debe ser adecuada a la gravedad del riesgo, costo-efectiva en la consecución del desafío, puntual para ser exitoso, realista dentro del contexto, convenida por todas las partes involucradas, y estar a cargo de personas responsables.

En el proceso de identificación de los riesgos, se pueden identificar las acciones que respondan a riesgos individuales o categorías de riesgos. El nivel de riesgo que es aceptable para la organización influirá en la planificación de la respuesta al riesgo.

Son varios los riesgos que pueden ser provocados por una causa común. Esta situación puede revelar oportunidades para mitigar dos o más riesgos de la empresa con una respuesta genérica.

5.3.1 Técnicas para la Planificación de la Respuesta al Riesgo

Existen varias estrategias de respuesta al riesgo. Por cada riesgo, se debe seleccionar la estrategia que tenga la mayor probabilidad de ser efectiva. Luego, se deben desarrollar acciones específicas a fin de implementar dicha estrategia.

Se pueden seleccionar estrategias principales y de respaldo como:

1. **Prevención.** La prevención de riesgos está cambiando el plan para eliminar el riesgo o la condición o para proteger de su impacto a los objetivos. Aunque el personal no podrá eliminar todos los eventos de riesgo, si es posible evitar algunos riesgos específicos y disminuir sus consecuencias.

Algunos eventos de riesgo que aparecen tempranamente en el proyecto, se pueden tratar mediante requerimientos de aclaración, obteniendo información, mejorando la comunicación o adquiriendo experticia. Algunos ejemplos de prevención podrían ser: reducir el alcance para evitar aquellas actividades de alto riesgo; agregar recursos o tiempo; adoptar un enfoque conocido en vez de uno innovador, o bien evitar un subcontratista que no esté familiarizado con el proceso.

2. **Transferencia.** La transferencia de los riesgos busca trasladar la consecuencia de un riesgo a una tercera parte, en conjunto con la propiedad o responsabilidad de la respuesta. La transferencia del riesgo simplemente le da



a la otra parte la responsabilidad por su gestión; no lo elimina. La transferencia de la responsabilidad por el riesgo resulta más efectiva en el manejo la exposición al riesgo financiero. La transferencia del riesgo casi siempre implica el pago de una prima de seguro a la parte que asume el riesgo. Esto incluye el uso de seguros, bonos de rendimiento y garantías. Para la transferencia de una responsabilidad por riesgos específicos a otra parte, se pueden utilizar contratos.

3. **Mitigación.** La mitigación busca reducir la probabilidad y/o las consecuencias de un evento de riesgo adverso hasta un umbral aceptable. La adopción de una acción temprana para reducir la probabilidad de que ocurra un accidente o para minimizar su impacto en el proyecto, es más efectiva que tratar de reparar las consecuencias una vez que dicho riesgo ha ocurrido. Los costos de la acción de mitigación deben ser adecuados, dada la probabilidad del riesgo y de sus consecuencias. La mitigación del riesgo puede tomar la forma de implementar un nuevo curso de acción que permita reducir el problema, por ejemplo, adoptando procesos menos complejos, realizando más pruebas sísmicas o de ingeniería, o seleccionando a un vendedor o proveedor más estable. Esto puede implicar la modificación de las condiciones, de manera tal de reducir la probabilidad de que ocurra el accidente.

En casos en los que no sea posible reducir la probabilidad, una respuesta de mitigación podría abordar el impacto del riesgo, fijando vínculos que determinen la gravedad o seriedad.

5.3.2 Resultados de la Planificación de la Respuesta Frente al Riesgo

El plan de respuesta al riesgo (algunas veces denominado *registro o catastro de riesgos*) debe redactarse con lo que se indica a continuación:

- * En los riesgos identificados, es necesario hacer una descripción, de las áreas afectadas, sus causas y de qué manera estos podrían llegar a afectar.



-
- * Establecer las responsabilidades asignadas conforme a los resultados de los procesos de análisis cuantitativo y cualitativo de los riesgos.
 - * Respuestas convenidas, incluida la prevención, transferencia, mitigación o aceptación de cada riesgo en el plan de respuesta al riesgo.
 - * Acciones específicas para implementar la estrategia de respuesta que se haya seleccionado.
 - * Presupuesto y tiempos de las respuestas.
 - * Planes de contingencia y planes de retroceso

En los resultados de la planificación también se pueden presentar diferentes secuelas de los riesgos de la siguiente forma:

1. **Riesgos Residuales:** Son aquellos que permanecen aun después de haberse adoptado las respuestas de prevención, transferencia o mitigación. Esto incluye también riesgos menores que se hayan aceptado y abordado.
2. **Riesgos secundarios.** Son aquellos riesgos que surgen como resultado directo de la implementación de una respuesta al riesgo. Estos deben identificarse y planificar las respuestas frente a ellos.
3. **Acuerdos contractuales.** Se pueden efectuar acuerdos o convenios contractuales de forma tal de especificar la responsabilidad de cada una de las partes por riesgos específicos, en caso de ocurrir estos.
4. **Cantidades de reservas por contingencia necesarias.** El análisis probabilístico de la empresa y los umbrales o niveles de riesgo ayudan al gerente de la empresa a determinar la cantidad de respaldo o contingencia necesaria para reducir el riesgo de excederse en los objetivos a un nivel aceptable para la organización.
5. **Entradas para otros procesos.** La mayoría de las respuestas frente a riesgos implican el gasto adicional de tiempo, costo o recursos y, demandan cambios. Las organizaciones necesitan asegurarse de que lo que se gaste esté justificado por el nivel de reducción del riesgo. Se deben incorporar estrategias alternativas en los procesos de otras áreas de conocimiento.



6. **Entradas para un plan de proyecto revisado.** Los resultados del proceso de planificación de la respuesta deben estar incorporados en el plan, de forma tal de asegurar que se implementen y monitoreen las acciones convenidas.

5.4 Plan de Respuesta de Emergencia

Una emergencia se considera como un evento no planeado que puede causar daño. Los procedimientos que se establezcan son indispensables para permitir que el personal tenga un manejo adecuado ante una emergencia y permitir de manera rápida y efectiva la respuesta.

Este plan está encaminado a mitigar los efectos y daños causados por eventos esperados e inesperados, ocasionados por el hombre o por la naturaleza; preparar las medidas necesarias para salvar vidas; evitar o minimizar los posibles daños o pérdida de la propiedad; responder durante y después de la emergencia y establecer un sistema que le permita recuperarse para volver a la normalidad en un periodo mínimo.

En este Plan de Emergencias se asignan las responsabilidades a los funcionarios y empleados de la instalación, y se establecen las medidas a tomar y las acciones a seguir antes, durante y después de un evento de emergencia.

Estas acciones abarcan desde atender una pequeña situación de emergencia, hacer un desalojo parcial en cualquier área de trabajo, hasta tener que proceder al desalojo y cierre de todas las instalaciones del Recinto.

Las situaciones de emergencias pueden variar desde un incidente aislado caracterizado por una solución rápida de algunos departamentos pequeños, hasta un desastre mayor que requiera una respuesta coordinada de múltiples departamentos y la utilización de recursos externos.

No obstante las graves consecuencias que día a día dejan los siniestros que ocurren en todas partes del mundo y que son originados por diversidad de causas, algunas de ellas inevitables como los eventos de origen natural. Sigue siendo evidente la deficiente organización para prevenir y atender estas situaciones de crisis. En algunas ocasiones la falta de recursos económicos, el poco interés por parte de los gobiernos en este tema e incluso la poca motivación o desconocimiento de quienes a



nivel privado tienen la responsabilidad de liderar este tema o de ejecutarlo hace que no se atienda y no se implemente las acciones para enfrentar las emergencias.

Las emergencias de origen tecnológico, es decir, aquéllas que se asocian a los procesos industriales de una empresa, se han caracterizado por las enormes consecuencias que se presentan en términos de vidas humanas e impactos ambientales negativos, sin olvidar los daños que se ocasionan en la empresa como son: pérdidas en la producción, el deterioro de la imagen de la organización, los días no trabajados e incluso los posibles conflictos legales que con el tiempo puede afrontar la empresa por ser ella la responsable de la situación ocurrida.

Además de las medidas de prevención, que controlan la generación de los accidentes tecnológicos se deben tener previstas las medidas de respuesta ante una contingencia de este tipo para disminuir la gravedad de sus consecuencias.

El conjunto de actuaciones a desplegar es el plan de emergencia y contingencias, el cual debe estar diseñado de antemano, puesto en conocimiento de todas las entidades y personas que intervienen en él y practicado periódicamente.

5.4.1 Implantación del Plan de emergencia

El implantar un Plan de Emergencia es a primera vista, una tarea compleja pues, para cumplirla, debe satisfacer su principal objetivo: “disponer de un sistema operativo de aviso al personal expuesto. Es compleja porque para conseguirlo se debe lidiar, internamente, como la logística, la economía, la eficacia, la tecnología y la política de administración.

La operatividad requerida complica la implantación, ya que se necesitan disciplinas científicas (telecontrol, comunicaciones, informática, etc.), técnicas (mantenimiento, seguridad, entre otras), y humanistas (como la psicología).

El conjunto de todas estas disciplinas repercuten, en los plazos que fija la administración para la implantación, como en los recursos que inicialmente haya previsto el titular de la organización².

² Experiencias en la Implantación de Planes de Emergencia de Presas. Jorge Durán Bravo, Comité Nacional Español de Grandes Empresas.



La formación de un equipo de trabajo es indispensable para el buen funcionamiento del sistema, se debe formar un grupo interdisciplinario de personas que incluyan todos los departamentos de la organización

En las altas direcciones de la organización los sistemas de gestión para la prevención de riesgos laborales son importantes para el control de los recursos financieros, humanos, tecnologías específicas, infraestructuras y equipos y sistemas de información. Las funciones son tareas que corresponden realizar al personal de la organización. La autoridad competente tiene la capacidad de exigir el cumplimiento de determinadas tareas, asegurar que los informes sobre el sistema de gestión se presente ante la dirección de la organización para su revisión, así como informar de necesidades o recomendaciones para la mejora del Sistema.

Es importante apoyar a la dirección en establecer, documentar, implementar y mantener el sistema de gestión y mejorar continuamente su eficacia así como elaboración de los documentos.

La organización debe asegurarse de que cualquier persona que trabaje para ella y que realice tareas que puedan causar impactos en la seguridad y salud en el trabajo, sea competente, tomando como base su educación, formación o experiencias adecuadas, y deben mantenerse los registros asociados.

La formación técnica y practica en la implantación del plan d emergencia debe de estar bien definida por la dirección de la organización. En dado caso de que sufra cambios en el personal las funciones de desempeño de deben de implantar para cubrir los cargos y responsabilidades en el centro de trabajo.

Las ventajas que tiene el formar al trabajador o trabajadora son evitar accidentes laborales, conocer los riesgos a los que están expuestos así como lograr la competencia requerida en su puesto de trabajo y aumentar la productividad y desempeño laboral.

Los factores que hay que tomar en cuenta al determinar la competencia requerida en una tarea dependen de las funciones y responsabilidades que el puesto de trabajo requiere, así como los resultados de las investigaciones de incidentes y de las capacidades individuales.



Por esto la toma de decisiones es para asegurar que se trabaja de manera segura y tomar conciencia del trabajo en procedimientos de emergencia, beneficios de la mejora del desempeño y de las necesidades de ajustarse a la política de prevención de riesgos.

Deben existir mecanismos para canalizar las comunicaciones internas y las comunicaciones externas. Se deben establecer mecanismos para que se facilite la emisión de comentarios, sugerencias, por parte de los trabajadores.

Las operaciones de seguimiento en un monitoreo y control de los componentes del plan de respuesta analizan diferentes puntos:

1. Control operacional: es la implantación de los programas de la dirección: Se evalúa la efectividad de los mecanismos de control y los programas de la dirección dentro de los riesgos identificados según lo establecido por OHSAS 18001).
2. Responsabilidades: establecer una estructura de la organización, donde se asignan responsabilidades a los encargados que están dentro del plan de respuesta de emergencias.
3. Planes de emergencia y respuesta: Se analizan los planes de emergencia y sus respuesta.se estudia realizar su adecuada comparación con los niveles inherentes de riesgo y la probabilidad que tienen de producirse. También incluye el estudio de los accidentes producidos y su solución.
4. Comunicación: Consiste en un análisis de la comunicación tanto interna como externa de la pruebas para que sean apropiadas.
5. Registro: Consiste en hacer un registro de los accidentes, acciones correctoras y preventivas a lo largo de la implantación del Sistema de Gestión de Salud y Seguridad Laboral.
6. Programa de auditorías internas: consiste en planificar auditorias internas para cada detección sobre las desviaciones de las actividades correctoras y preventivas sobre dichas desviaciones.
7. Revisión por la dirección: Periodicidad establecida de reuniones, acciones tomadas y cambios que den lugar a resultados



El objetivo que se persigue es garantizar que todos los factores posibles que causen una emergencia en la organización se eliminen y que el trabajo se realice correctamente.

Los trabajadores se deberían ubicar en el lugar y la función idónea para ellos a fin de lograr la optimización entre las exigencias del puesto y las capacidades de las mismas. Por tanto, el empresario sería responsable si se derivan daños al contratar o colocar en un puesto de trabajo a personas que no tuvieran las capacidades personales y profesionales necesarias.

En la contratación de trabajadores, la empresa debe cumplir una serie de prescripciones en materia de prevención de riesgos laborales, para asegurar que todos los trabajadores que estén en un mismo centro de trabajo o realicen tareas para las que han sido contratados a cuenta de dicha empresa principal, tengan la información y formación preventiva necesaria y puedan realizar sus cometidos en adecuadas condiciones de trabajo.

★ Actuaciones frente a sucesos previsibles

Ante un suceso que se puede prevenir el plan de emergencia es un documento que recoge el conjunto de medidas diseñadas e implantadas para evitar la pérdida de materia y personal en situaciones de emergencia y, en su caso, para minimizar las consecuencias derivadas de un siniestro y optimizar los recursos disponibles existentes al respecto.

Por ello, la investigación de accidentes y daños de salud de los trabajadores es recomendable investigar el mayor número posible de incidentes que tengan lugar en la empresa. Los incidentes son aquellos eventos que, aunque no hayan generado accidentes, puedan desembocar, si no se corrigen, en la generación de lesiones o daños de mayor importancia.

La documentación de los sistemas preventivos de emergencias, requiere una gestión que establece a un incidente para mejorar el procedimiento de control y mantenimiento de la documentación. Se necesita llevar uno de los y los registros del sistema de prevención de riesgos laborales, ya que es uno de los aspectos más importantes del sistema de prevención.



La evaluación periódica del sistema preventivo y del conjunto de elementos fundamentales que lo componen es una actividad ineludible que ha de permitir su mejora continua para poder garantizar, tanto el cumplimiento de las exigencias reglamentarias en materia de gestión preventiva, como la eficacia del propio sistema. El objetivo es establecer el procedimiento que permita a la organización la realización de la auditoría del sistema de prevención de riesgos laborales. La auditoría se lleva a cabo para determinar su eficacia y la efectividad de la implantación del sistema de prevención, contribuyendo así a la mejora continua de la seguridad y salud laboral.

La eficacia en la respuesta de una empresa ante una situación de emergencia, va a depender directamente de la existencia del “Plan de Emergencia” y del grado de entrenamiento alcanzado por la empresa en el mismo.

La guía del plan de respuesta de emergencia contemplará una serie de pasos con el fin de especificar y concretar las tareas descritas que proporcionen un soporte técnico necesarios para resolver los problemas presentados en diferentes situaciones. No obstante, siempre podrá recurrir a asesores externos especializados en la materia para la gestión del tema dedicando el tiempo necesario para llevar adelante la elaboración e implantación del plan de emergencia.

5.5 Monitoreo y Control de los Riesgos

El monitoreo y control de los riesgos es el proceso de mantener un registro de los riesgos identificados, monitorear los riesgos residuales e identificar los nuevos riesgos, asegurando la ejecución de los planes de riesgo y, evaluando su eficacia en la reducción del riesgo.

El monitoreo y control de los riesgos registra las métricas de riesgos que guardan relación con la implementación de planes de contingencia. El monitoreo y control de riesgos es un proceso continuo que se lleva a cabo durante toda la vida útil de la empresa. Los riesgos cambian a medida que la empresa madura, se desarrollan nuevos riesgos o desaparecen los riesgos anticipados.



Los buenos procesos de monitoreo y control de riesgos dan información que ayuda en la toma de decisiones efectivas antes de que ocurra el accidente. Se hace necesaria la comunicación con todos los demás accionistas del proyecto, de forma tal de evaluar periódicamente la aceptabilidad del nivel de riesgo.

Se han producido o han surgido riesgos que no estaban previamente identificados.

El control del riesgo puede implicar la selección de estrategias alternativas, la implementación de un plan de contingencia, la realización de una acción correctiva o bien la re-planificación. El responsable de la respuesta al riesgo debe informar periódicamente al gerente y al líder del equipo, sobre la efectividad del plan, de cualquier efecto no anticipado, y de cualquier otra corrección a mitad de curso que sea necesaria para mitigar el riesgo.

Los resultados del trabajo y otros registros de riesgo proveen información acerca del rendimiento o desempeño de la respuesta y de los riesgos del mismo. Entre los informes utilizados comúnmente para monitorear y controlar los riesgos, se incluyen: Libros de Obras, Listados de Ítemes de Acción, Advertencias o Notas de Escalamiento. A medida que se mide e informa de, el rendimiento o desempeño, pueden aparecer riesgos potenciales que no hayan aparecido anteriormente.

5.5.1 Estrategia del Monitoreo y Control de los Riesgos

En este apartado se menciona algunas estrategias que ayudarán a tener un mejor control y monitoreo de los riesgos presentes en la empresa.

1. Auditorías a las respuestas de riesgos del proyecto: Los auditores de riesgos revisan y documentar la efectividad de la respuesta al riesgo en prevención, transferencia o mitigación de la ocurrencia del riesgo, como así también la efectividad del responsable del riesgo. Las auditorías de riesgos se realizan durante periodos programados de modo tal de controlar el riesgo.
2. Revisiones: Se deben programar regularmente revisiones de los riesgos. El riesgo debe ser un tema de la agenda de todas las reuniones del equipo de trabajo. Durante ciclos establecidos, es posible que las demandas de análisis cuantitativo y cualitativo se incrementen adicionalmente.



3. **Medición del rendimiento técnico:** La medición del rendimiento técnico compara los logros técnicos durante la ejecución, con el programa de logros técnicos del plan. Toda desviación, como por ejemplo la llegada de nueva tecnología, puede implicar un riesgo.
4. **Planificación adicional de la respuesta al riesgo:** Si surgiera un riesgo que no se haya anticipado en el plan de respuesta al riesgo, o cuyo impacto en los objetivos sea mayor que el esperado, es posible que la respuesta planificada no sea la adecuada. En este caso, será necesario realizar una planificación adicional de respuesta a fin de controlar el riesgo.

CAPITULO 6

PLAN DE ADMINISTRACION DE INCIDENTES

En este capítulo se hace referencias a la parte administrativa en el manejo de incidentes, donde se establecen los pasos a seguir en las funciones, preparación, protocolos que ayudaran a la empresa a enfrentar los inesperados impactos. Una vez que se plantió la parte de planeación, identificación y análisis en los capítulos anteriores con ayuda del NIMS (National Incident Magement System) y de OHSAS (Occupational Health and Safety Assessment Series) ayudara a tener un panorama mas claro de como manejar esta información.

6.1 National Incident Magement System (NIMS)³¹

Un incidente es un suceso que ocurre de manera inesperada y que puede afectar al desarrollo de cualquier negocio. Este capítulo describe el desarrollo de los sistemas de administración de incidentes para dirigir, controlar y coordinar las operaciones de respuesta y recuperación.

Las organizaciones deben de manejar un sistema de respuesta a los incidentes en materia de seguridad, ya que al no estar preparado las consecuencias que se produzcan podrían causar daños irreparables como pérdidas humanas. Tener un plan definido mejora las perspectivas de éxito. Como tal, un plan debería cubrir todas las etapas del proceso de respuesta a incidentes, desde preparar la infraestructura y responder de todas las formas, hasta aprender la lección de un incidente resuelto exitosamente.

Si se cuenta con un plan, es posible moverse rápidamente dentro de un conjunto de actividades planificadas, incluyendo una oportunidad para contener el daño y reducir las pérdidas por el incidente. Tener una lista de verificación que seguir y una lista de



gente a quien llamar es de suma importancia en un ambiente de completo estrés posterior al incidente.

La dirección del National Incident Management System (NIMS) establece el marco amplio y el enfoque de la gestión a nivel geográfico, organizativo y jurisdiccional en diferentes niveles de gestión de incidentes.

El NIMS utiliza un enfoque sistemático para integrar a los mejores procesos y métodos existentes en un marco nacional unificado para la gestión de incidentes. La gestión de incidencias se refiere a cómo se manejan los incidentes en todas las actividades de seguridad nacional, incluida la prevención, protección, respuesta, mitigación y recuperación. Este marco constituye la base a un conjunto diverso de organizaciones públicas y privadas que lleven a cabo la gestión de emergencias de manera integrada y eficaz.

La gestión de emergencias es la integración de todas las actividades necesarias para construir, mantener y mejorar la capacidad de preparación, protección, respuesta, recuperación, o mitigar los desastres ó amenazas de manera coordinada. Lo hace a través de un conjunto básico de conceptos, principios, procedimientos, procesos organizativos y requisitos de la norma aplicable a una amplia comunidad de usuarios.

6.1.1 Función y Organización

Los componentes del sistema de manejo de incidentes se adaptan a cualquier situación de incidentes locales que requieren la activación de ayuda mutua entre estados a una respuesta coordinada. Las funciones se van a diseñar para trabajar en equipo de una manera flexible y sistemática.

Los principales componentes que integran al sistema son:

1. Preparación,
2. Comunicación,
3. Gestión de información,
4. Gestión de recursos y de mantenimiento.



1. La preparación en la gestión de incidentes implica una combinación integrada de una evaluación planificada con procedimientos y protocolos en la formación de ejercicios calificados del personal. En dicha gestión se otorga licencias y certificaciones en las evaluaciones del personal y de los equipos. La autogestión de incidentes tiene el objetivo de alcanzar y mantener un ciclo continuo de planificación, organización, capacitación, equipamiento, adiestramiento, evaluación y corrección.
2. En la comunicación y gestión de la información las actividades de respuesta a incidentes se basan en comunicaciones y sistemas de información que ofrezcan un panorama operativo común a todos los sitios de mando y coordinación. El cuadro de operaciones común se basa en los conceptos de, fiabilidad y portabilidad, además toma en cuenta la resistencia y la redundancia de las comunicaciones y los sistemas de información.
3. La gestión de los recursos se necesita para apoyar los objetivos de incidentes críticos. El flujo de recursos debe ser fluido y adaptable a los requisitos del incidente. Define mecanismos estandarizados y establece el proceso de gestión de los recursos para identificar las necesidades, el orden y la adquisición, movilización, seguimiento e informar, recuperar, desmovilizar y reintegrar los recursos de inventario.

Los componentes mencionados anteriormente describen las medidas y capacidades específicas que la gestión del personal de emergencias, así como su respuesta de organizaciones afiliadas y deben desarrollar e incorporar en sus programas de preparación global para mejorar la preparación de las operaciones necesarias para la gestión de emergencias para todos los riesgos y las actividades de respuesta a incidentes. En el desarrollo y la ampliación de los programas de preparación y las actividades dentro de sus jurisdicciones u organizaciones, la gestión de emergencia y personal de respuesta debe aprovechar las actividades de preparación y relaciones de colaboración en la mayor medida posible.



6.1.2 Preparación para Funciones

Las actividades de preparación en las funciones del personal deben ser coordinadas entre todos los organismos competentes. Cada integrante desempeñará un papel con un programa de divulgación para promover y apoyar la preparación individual.

Las organizaciones de preparación se encargarán de la coordinación para la respuesta a incidentes ante un evento planeado. Estas organizaciones son grupos de personas que se asignarán ciertas responsabilidades durante el desempeño del manejo del incidente.

Las actividades que sirven para que el personal responsable pueda coordinar las responsabilidades son:

1. Establecer y coordinar las operaciones de planes de emergencia con sus respectivos protocolos y procedimientos.
2. Establecer las normas y protocolos necesarios para promover la seguridad de respuesta.
3. Adoptar normas para solicitar y proporcionar los recursos.
4. Identificar los recursos y otros requerimientos para establecer prioridades para su uso.
5. Fomentar la formación de ejercicios para la evaluación de acciones correctivas.
6. Llevar a cabo evaluaciones posteriores a la acción para fortalecer la preparación en el futuro.

Los planes deben constituir la base de la formación. Estos deben llevarse a cabo periódicamente para asegurar que todos los individuos involucrados en la respuesta son capaces de ejecutar sus tareas asignadas. Es esencial que abordar los planes de formación y de hacer ejercicio permita la incorporación de revisiones posteriores a la acción. Las lecciones aprendidas y acciones correctivas son los acuerdos de la responsabilidad después de un incidente importante o el ejercicio. Los planes que



marcan las funciones de cada integrante deben ser actualizados periódicamente para reflejar los cambios en el manejo de emergencias y el medio ambiente de respuesta a incidentes, así como los cambios institucionales o de organización.

Los planes son el núcleo operativo de la preparación. Estos proporcionan mecanismos para el establecimiento de prioridades, la integración de múltiples organizaciones y las funciones de cada quien. Los planes también deben incorporar estrategias para mantener la continuidad de la organización durante y después de los incidentes e incorporar la planificación anticipada como es la gestión de recursos y las comunicaciones.

Los recientes desastres naturales y los provocados por el hombre han demostrado la necesidad de una capacidad robusta de continuidad de negocio, a fin de garantizar la preservación de la organización. El objetivo de una capacidad de continuidad robusta es tener la resistencia para afrontar cualquier reto, amenaza o vulnerabilidad. Los planes de continuidad deberán presentarse en todas las organizaciones.

6.1.3 Protocolos de Planeación y Comunicación.

Los protocolos son conjuntos de acciones que pueden ser diseñados por los individuos con funciones en diferentes distintas en el trabajo. El protocolo establece el reglamento, las autorizaciones, y las responsabilidades necesarias para permitir la rápida ejecución de una tarea.

Los protocolos toma en cuenta un personal específico basado en su formación para que de evalué un acontecimiento y tome las medidas inmediatas. El personal debe estar debidamente capacitado para realizar las funciones asignadas, por lo que se le capacita con cursos y ejercicios concretos que le ayuden a mejorar su desempeño durante un incidente. La formación y ejercicios deben adaptarse específicamente a las responsabilidades del personal involucrado en el manejo de incidentes. Además, los ejercicios deben ser diseñados para permitir al personal simular varios comandos de control o funciones de liderazgo cuando sea posible. Los ejercicios deben llevarse



a cabo con las partes identificadas en los planes estratégicos y operativos, por ejemplo el plan de respuesta de emergencia y contener un mecanismo para incorporar las medidas correctivas en el proceso de planificación.

En la gestión eficaz, la respuesta a incidentes usa en comunicaciones flexibles y sistemas de información que ofrecen un panorama operativo común para la gestión de emergencias y respuesta personal. Las comunicaciones de incidentes se facilitan a través del desarrollo y uso de planes de comunicación. Durante un incidente el enfoque integra enlaces de unidades operativas y de apoyo de las diversas organizaciones para mantener la conectividad de comunicaciones y conocimiento de la situación. Las comunicaciones y la planificación de gestión de la información debe abordar las políticas relacionadas con el incidente, equipos, sistemas, normas, y la formación necesarias para lograr una comunicación integrada. Establecer y mantener un cuadro de operación común y garantizar la accesibilidad son los objetivos principales de la Información y las comunicaciones.

Las comunicaciones y sistemas de información deben ser diseñados para ser flexibles, fiables y escalables para que funcionen en cualquier tipo de incidente, sin importar la causa, tamaño, ubicación o complejidad. Deben ser adecuados para las operaciones en una sola jurisdicción u organismo para ser aplicable a nuevas tecnologías en el contexto de cualquier incidente al que estarían sometidos con una respuesta adecuada. El éxito de las comunicaciones y la gestión de la información exigen que el personal de manejo respuesta de incidentes y sus organizaciones afiliadas utilicen tipos de comunicación normalizados. La elección de la persona responsable de estas comunicaciones se discute en el componente de mando y de gestión como se menciona a continuación:

- * Comunicaciones Estratégicas: son los medios de respuesta a incidentes de la acción.
- * Táctica de Comunicaciones: son las comunicaciones entre el mando y elementos de apoyo.



- * Apoyo a las comunicaciones: consiste en la coordinación en apoyo a las comunicaciones estratégicas y tácticas (por ejemplo, las comunicaciones entre los hospitales sobre los recursos pedidos, envío y seguimiento de los centros de logística, tráfico y comunicaciones de obras públicas).

Las comunicaciones deben describirse en lenguaje sencillo, lo que asegura que la difusión de información sea oportuna, clara, reconocida y comprendida por todos los destinatarios. Los códigos no deben ser utilizados. Todas las comunicaciones deben limitarse a los mensajes esenciales. El uso de las siglas se debe evitar durante los incidentes que requieren la participación de múltiples áreas de la organización. Por ello las políticas y procedimientos de la organización deben definirse para permitir el intercambio de información entre todo el personal de respuesta.

En la administración de incidentes es necesario que el personal deba contar con una metodología y sistemas establecidos para interpretar la información, para que la seguridad se pueda mantener con uso de un lenguaje sencillo. Puede ser apropiado que en la respuesta se utilice un idioma más táctico, para no ocasionar terror en el personal de la organización. El uso de encriptación especializada y el idioma táctico debe ser incorporado en el plan de manejo de incidentes de comunicaciones.

El Internet y otras herramientas basadas en páginas web pueden ser recursos para el personal de gestión de respuesta de incidentes. Por ejemplo, estas herramientas pueden ser utilizadas antes y durante los incidentes como un mecanismo para ofrecer conocimiento de la situación a la organización. El procedimiento para el uso de estas herramientas durante un incidente debe ser establecido para aprovecharlas como valiosos recursos en el sistema de comunicación. La información publicada o compartida durante un incidente a través de estas aplicaciones deben seguir los métodos previstos y normalizados.



6.1.4 Descripción de los Recursos

La gestión de emergencias y las actividades de respuesta a incidentes requieren cuidado en los recursos administrados como es el personal, equipos, instalaciones o suministros para satisfacer las necesidades del incidente. La administración de recursos debe ser flexible y escalable para apoyar cualquier incidente y poder adaptarse a los cambios. La implementación eficiente de los recursos requiere que los conceptos de gestión utilicen en todas sus fases la respuesta a incidentes.

Donde los incidentes de rutina en el área de trabajo, los incidentes requieren una respuesta coordinada de toda la organización. En las etapas iniciales de un incidente, la mayoría de los recursos solicitados se tratan a nivel local a través de acuerdos de ayuda mutua o acuerdos de asistencia. Cuando un incidente crece en tamaño o complejidad, las necesidades de recursos podrán ser satisfechas por otras fuentes. En un caso de competencia por los recursos críticos, se puede establecer prioridades para poder coordinar la asignación de recursos. La distribución se llevará de acuerdo a la disponibilidad y a necesidades del incidente.

6.1.5 Conceptos y Principios

En los conceptos se deben contemplar una normalización para los recursos, de forma que se mejore la identificación y adquisición de estos. El tener una clasificación adecuada de los recursos ayudará a que se va a brindar una rápida respuesta. Se basan en estos cuatro puntos:

1. *Planificación:* El proceso de planificación debe incluir la identificación de necesidades de recursos sobre la base de las amenazas y vulnerabilidades de la competencia y el desarrollo de estrategias alternativas para obtener los recursos necesarios. Las jurisdicciones deberían trabajar juntos antes de un incidente para desarrollar planes para identificar, ordenar, administrar y emplear los recursos.



La planificación puede incluir la creación de nuevas políticas para fomentar la colocación de recursos. Los planes deben prever las condiciones o circunstancias que pueden desencadenar una reacción específica, tales como la reposición de suministros, cuando los inventarios de llegar a un mínimo determinado previamente. Las organizaciones y jurisdicciones deben evaluar continuamente el estado de sus recursos a fin de tener una lista exacta de los recursos disponibles en un momento dado.

2. *Categorización de los recursos:* Los recursos están organizados por categorías, clase, tipo y tamaño. Esto se hace con la finalidad que los recursos sean aprovechados de manera eficiente y fácil de identificar en caso de un incidente.
3. *Identificación de recursos y pedidos:* Estos recursos estarán estandarizados para identificar y llevar un seguimiento de todos los movimientos necesarios para apoyar las actividades de manejo de incidentes. Los recursos de materiales se pueden adquirir por adelantado y almacenado a través de contratos adecuados.
4. *Administración:* Las personas que sean responsables de los recursos tomar la decisión de evaluar la urgencia de la necesidad y cercioran si son las que son suficientes los elementos que están disponibles para su uso o si no pueden cumplir la demanda requerida. Otra parte importante del proceso es la gestión de inventarios según la vida útil y tomar consideraciones especiales de mantenimiento.

6.1.6 Sistemas de Gestión de la Información)

Estos sistemas se utilizan para proporcionar información de apoyo a las decisiones de los administradores mediante la recopilación, actualización y procesamiento de datos y seguimiento de los recursos. Los SGI mejoran el estado de flujo de recursos, de información y proporcionan datos en tiempo real en un ambiente agitado en las distintas jurisdicciones.



Ejemplos de sistemas de gestión de la información incluyen el seguimiento de recursos, el control de transporte, la gestión de inventarios, los informes y los sistemas de información geográfica. La selección y el uso de sistemas de gestión de los recursos deben basarse en la identificación de las necesidades de información dentro de la jurisdicción en estudio.

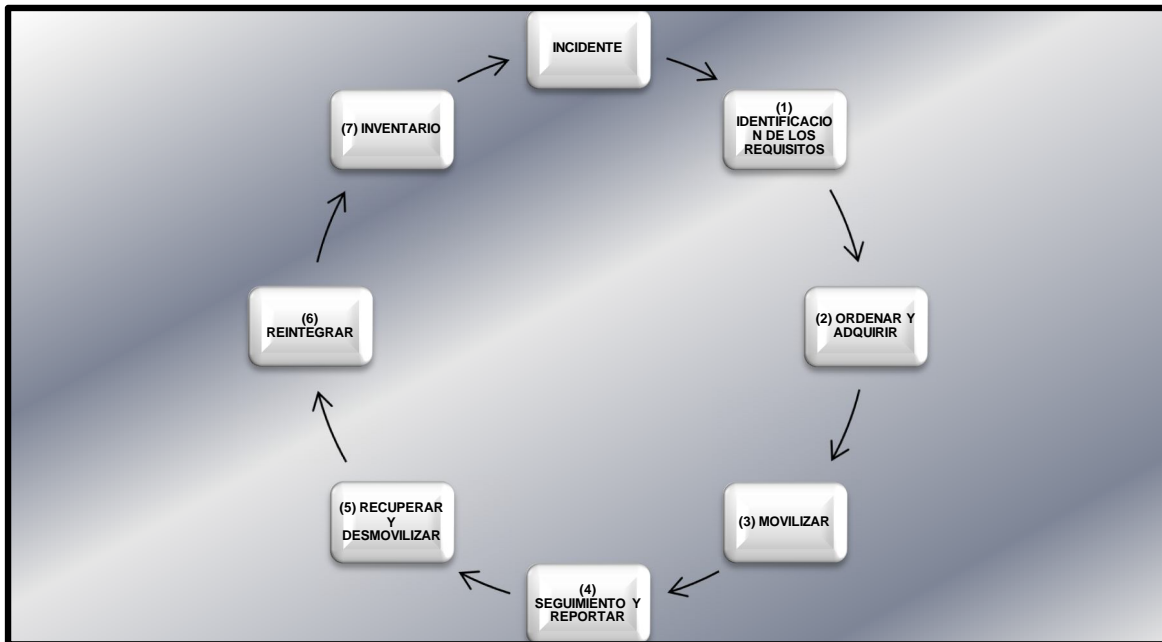
En caso de que la gestión principal de recursos del sistema de información se interrumpa o no está disponible. Las personas con responsabilidades de gestión de los recursos deben ser capaces de identificar y activar los sistemas de copia de seguridad para administrarlos. Los sistemas de gestión de información también deben tener fuentes de alimentación lo suficientemente diversa, para que la información quede respaldada por lo menos cada 24 horas durante el incidente.

6.1.7 Gestión de los Recursos

El mantenimiento de recursos es importante en todos los aspectos, ya que el mantenimiento antes del despliegue de recursos garantiza la disponibilidad y capacidad. El proceso de gestión de los recursos se puede separar en dos partes: la gestión de recursos como un elemento de la preparación y la gestión de los recursos durante un incidente. Las actividades de preparación se llevan a cabo en forma continua para ayudar a garantizar que los recursos están listos para movilizarlos para cuando ocurre un incidente. La administración de recursos durante un incidente es un proceso finito, como se muestra en la Figura 6.1. Comienza identificando los requisitos después de ocurrido el incidente y termina atendiendo a las necesidades específicas del incidente.



Figura 6.1. Ciclo de los Recursos Durante un Incidente



(1) Identificación de los requisitos

Cuando ocurre un incidente, las personas con responsabilidades de gestión de recursos deben identificar, refinar y validar los requisitos de recursos. Este proceso consiste en identificar con precisión (lo que se necesita, cuánto se necesita, dónde y cuándo) y quien va a recibirlo y usarlo. Los recursos son el equipo, los suministros, las instalaciones y el personal, los equipos de respuesta a emergencias.

La disponibilidad y necesidades de recursos cambiarán constantemente como el incidente evoluciona. En consecuencia, toda la gestión de emergencia y personal de respuesta y de sus organizaciones afiliadas que participen en una operación deben coordinarse estrechamente a lo largo de este proceso. En los casos en que se presente de magnitudes externas a la empresa la respuesta federal se coordinará con las estatales, y las jurisdicciones locales. El posicionamiento de los recursos federales se adaptará para hacer frente a la situación específica.



(2) Ordenar y adquirir

Los ciclos de decisión para la colocación y llenado de pedidos de recursos son diferentes para el personal de campo de incidentes para la coordinación de gestión de recursos. Las solicitudes de recursos se desarrollarán con base en las prioridades. Las decisiones sobre la asignación de recursos se basan en el protocolo de organización. Los recursos solicitados serán movilizados sólo con el consentimiento de la jurisdicción a la que se le pide que proporcione los recursos.

(3) Movilizar

El personal de respuesta de incidentes iniciará la movilización cuando se les notifique. En el momento de la notificación, se les da la fecha, hora y lugar de partida, el modo de transporte con fecha y hora estimada de llegada, punto de notificación (dirección, nombre de contacto y número de teléfono), asignación del incidente previsto; la duración prevista del despliegue. Los procesos de seguimiento de los recursos y la movilización están directamente vinculados. Cuando los recursos lleguen a la escena, deben registrarse formalmente. La notificación de que los recursos han llegado se realiza a través de las comunicaciones establecidas.

El proceso de movilización puede incluir la planificación de implementación basado en las directrices de equipamiento, capacitación, designación de puntos de concentración. Tales puntos deben tener lugares en las instalaciones adecuadas para el apoyo logístico como es la obtención de transporte para entregar los recursos del incidente lo más rápidamente posible para atenderlos.

Los planes y sistemas para monitorear el estado de movilización de recursos debe ser lo suficientemente flexible para adaptarse a los tipos de movilización. Los gerentes deben planificar y prepararse para el proceso de desmovilización, al mismo tiempo que comienzan el proceso de movilización de recursos. La planificación



temprana para la desmovilización facilita la rendición de cuentas y hace que el transporte de los recursos lo más eficiente posible en términos de costos y tiempo de entrega.

(4) Seguimiento e Información

El seguimiento de los recursos es un proceso estandarizado e integrado antes, durante y después de un incidente por toda la gestión de emergencia. Este proceso ofrece una imagen clara de dónde se encuentran los recursos, ayuda al personal a prepararse para recibirlos permitiendo su coordinación y movimiento adecuado. Los gerentes deben seguir todos los procedimientos de adquisición y gestión de los recursos, junto con la contabilidad, auditoría e inventario.

(5) Recuperar y desmovilizar

La recuperación implica la disposición final de todos los recursos, incluidas las situadas en el lugar del incidente y en instalaciones fijas. Durante este proceso, los recursos son rehabilitados, repuestos o eliminados.

La desmovilización es el regreso ordenado, seguro y eficiente de un recurso de incidente a su ubicación original. Se puede comenzar en cualquier punto de un incidente y debe comenzar tan pronto como sea posible para facilitar la rendición de cuentas. El proceso de desmovilización debe reasignar recursos, si es necesario, y dar prioridad a las necesidades críticas de recursos durante la desmovilización.

La planificación debe incluir disposiciones sobre el retorno seguro de los recursos a su ubicación original y el estado de retorno. La desmovilización debe incluir también los procesos para el seguimiento de los recursos y para hacer frente al reembolso aplicable. Por otra parte, la documentación relativa al transporte de los recursos debe ser recopilada y mantenida para el reembolso.



(6) Reintegrar

Los reembolsos proporcionan un mecanismo para recuperar los fondos gastados para actividades específicas de incidentes. El proceso de reembolso desempeña un papel importante en el establecimiento y el mantenimiento de la disponibilidad de recursos. Los reembolsos deben garantizar que los proveedores de recursos, los recibirán de manera oportuna. Se debe contar con mecanismos para recoger las facturas, la validación de los costos contra el alcance del trabajo, asegurándose de que las autoridades correspondientes estén involucradas.

Los mecanismos de reembolso deben ser incluidos en los planes de preparación, los acuerdos de ayuda mutua y acuerdos de asistencia. Algunos de los recursos prestados pueden o no ser reembolsados, sobre la base de acuerdos establecidos antes del incidente.

(7) Inventariar

La gestión de recursos utiliza varios sistemas de inventario de recursos para evaluar la disponibilidad de los activos proporcionados por las jurisdicciones. Las organizaciones de preparación deben hacer que el inventario sobre los recursos disponibles este actualizado, ya que los recursos identificados dentro de un sistema de inventario no son una indicación de la disponibilidad automática. La jurisdicción o el titular de los recursos tienen la determinación definitiva de la disponibilidad.

La planificación de uso de los recursos, inventario y seguimiento debe distinguir la diferencia fundamental en el despliegue de recursos en las fases de respuesta y recuperación. La fase de respuesta depende en gran medida de los acuerdos de ayuda mutua y acuerdos de asistencia, mientras que los recursos de recuperación se adquieren a través de contratos con organizaciones no gubernamentales o sector privado.



6.1.8 Comando y Gestión de Incidentes

Los componentes del Sistema de Administración de Incidentes descrito anteriormente-Preparación, Comunicaciones Gestión de la Información y Gestión de Recursos proporcionan un marco para facilitar una respuesta clara con una adquisición de recursos y una gestión eficaz en la respuesta a incidentes. El **System Command Incidents (ICS)**, e Información Pública son los elementos fundamentales de la gestión de incidentes. Estos elementos proporcionan a través de la normalización coherente la terminología y las estructuras organizativas establecidas. La gestión de emergencias y respuesta a incidentes se refieren al amplio espectro de actividades y organizaciones que prestan operaciones efectivas y eficientes. En conjunto, estos elementos de mando y de gestión son los aspectos más visibles de la gestión de incidentes.

La mayoría de los incidentes se manejan a nivel local y por lo general a cargo de las comunicaciones locales, centros de expedición y gestión de emergencias.

El ICS es un sistema de gestión de amplia aplicación diseñada para permitir una gestión eficaz, eficiente de los incidentes, mediante la integración de una combinación de instalaciones, equipos, personal, procedimientos y comunicaciones que operan dentro de una estructura organizativa común. El ICS es una forma fundamental de la gestión establecida en un formato estándar, con el fin de permitir a los manejadores de incidentes identificar las principales preocupaciones asociadas con el incidente. También proporciona un mecanismo central flexible para la gestión de incidentes de coordinación y colaboración, ya sea por incidentes en los que se necesitan recursos adicionales o se prestan desde las diferentes organizaciones dentro de una misma jurisdicción o fuera de la jurisdicción, o por incidentes complejo con implicaciones nacionales (tales como una enfermedad infecciosa emergente o un ataque de terrorista). ICS se utiliza para organizar las operaciones sobre el terreno de un amplio espectro de situaciones de emergencia de pequeños incidentes a complejos, tanto naturales como provocados por el hombre.



El nivel de respuesta es el campo donde el manejo de emergencias y personal de respuesta, bajo el mando de una autoridad competente, llevan a cabo las decisiones tácticas y actividades en respuesta directa a un incidente. Como sistema, ICS es extremadamente útil, no sólo proporciona una estructura organizativa para la gestión de incidentes, sino que también orienta el proceso de planificación, construcción y adaptación de esa estructura, para perfeccionar y mantener las capacidades necesarias de los incidentes a gran escala.

El ICS se basa en 13 características de gestión probada, cada uno de ellos contribuye a la fuerza y la eficiencia del sistema en general.

1. Terminología común

El ICS establece una terminología común que permite la gestión de incidentes diversos y organizaciones de apoyo para trabajar juntos a través de una amplia variedad de funciones de gestión de incidentes y situaciones de peligro. Esta terminología común cubre lo siguiente:

- a. Funciones de organización: Las principales funciones y unidades funcionales con responsabilidades de gestión de incidentes son nombrados y definidos.
- b. Descripción de Recursos: Recursos importantes que incluye el personal, instalaciones y equipo pesado que apoyan las actividades de manejo de incidentes y les dan los nombres comunes, para ayudar a evitar confusiones
- c. Instalaciones de Incidentes: Terminología común se utiliza para designar a las instalaciones en las proximidades del área del incidente que se utilizarán durante el curso del incidente.

2. Organización modular

La estructura organizativa ICS desarrolla de forma modular en función del tamaño y la complejidad de los hechos, así como las características



específicas del medio ambiente del peligro creado por un incidente. Cuando sea necesario separar los elementos funcionales se pueden establecer cada uno, de los cuales pueden subdividirse para mejorar la gestión interna y externa de la organización. La responsabilidad de la creación y expansión de la organización depende en última instancia del Comando de Incidentes. A medida que aumenta la complejidad incidente, la organización se expande desde arriba hacia abajo, así es como se delegan las responsabilidades funcionales.

3. Dirección por objetivos

La gerencia por objetivos se comunica a través de toda la organización que incluye:

- * Establecimiento de objetivos de incidentes.
- * Desarrollo de estrategias basadas en objetivos de incidentes.
- * El desarrollo y la emisión de las tareas, planes, procedimientos y protocolos.
- * El establecimiento de tácticas específicas, mensurables o las tareas para las diversas actividades de manejo de incidentes funcional, y dirigir los esfuerzos para llevarlos a cabo, en apoyo de las estrategias definidas.
- * Documentación de resultados para medir el rendimiento y facilitar las acciones correctivas.

4. Incidente de Planificación para la Acción

La planificación de una acción coordinada de un incidente debe guiar todas las actividades de respuesta. Un Plan de Acción de Incidentes, proporciona un medio conciso y coherente de la captura y comunicación de las prioridades de un incidente en general. Sin embargo, no todos los incidentes requieren planes escritos. La necesidad de planes por escrito y accesorios se basa en los requisitos del incidente y la decisión del comandante de incidentes. La mayoría de las operaciones de respuesta inicial no se capturan formalmente,



pero si un incidente es probable que se extienda más allá de un período de actividad, se vuelven más complejo y difícil que se atienda.

5. Control manejable

El tramo de control es la clave para la gestión de incidentes eficaz y eficiente. Los supervisores deben ser capaces de supervisar adecuadamente y del control de sus subordinados, así como comunicarse y gestionar todos los recursos bajo su supervisión.

6. Incidente, instalaciones y ubicaciones

Varios tipos de instalaciones de apoyo operacional se establecen en las proximidades de un incidente, en función de su tamaño y complejidad, para lograr una variedad de propósitos. La identificación y localización de las instalaciones están basadas en los requisitos de la situación. Por lo general las instalaciones designadas incluyen, campamentos, áreas de ensayo, sitios de puntos de distribución.

7. Gestión Integral de Recursos

El mantenimiento de una imagen precisa y actualizada de la utilización de los recursos es un componente crítico de la gestión de incidentes y respuesta a emergencias.

8. Comunicaciones Integradas

Las comunicaciones de incidentes se facilitan a través del desarrollo y el uso de un plan común de comunicación. La conectividad de las comunicaciones y la disciplina permite una conciencia común en la interacción planificada para la preparación de protocolos necesarios para lograr integrarlas s una sola vez.

9. Creación y transferencia de mando

La función de mando deben ser claramente establecidos desde el inicio de las operaciones de incidentes.

10. Cadena de mando y la unidad de mando

La cadena de mando se refiere a la línea ordenada de la autoridad dentro de las filas de la organización de manejo de incidentes. La unidad de mando



significa que todos los individuos tienen un supervisor designado a los que presenta en la escena del incidente. Estos principios aclaran las relaciones de informaciones y eliminar la confusión causada por varias directivas.

11. Rendición de cuentas

La rendición de cuentas efectiva de los recursos en todos los niveles jurisdiccionales y dentro de cada área funcional durante las operaciones de incidentes es esencial.

12. Despacho e implementación

Los recursos deben responder sólo cuando se le solicite o que se expidan por una autoridad competente a través de sistemas establecidos de gestión de los recursos. Los recursos no solicitados deben abstenerse de despliegue espontáneo para evitar sobrecargar el beneficiario y provocar los problemas de composición de rendición de cuentas.

13. Gestión de Información y de Inteligencia

La organización de manejo de incidentes debe establecer un proceso para recopilar, analizar, evaluar, compartir y administrar la información relacionada con el incidente y la inteligencia.

Con lo antes descrito podemos establecer que el Comando de Incidentes es responsable de la gestión global de los incidentes, que incluye comandos asignaciones del personal necesario para apoyar las funciones en cualquier área de la organización.

La función de mando puede llevarse a cabo en una de las dos formas generales, una es el comandante de Incidente aislado que es cuando ocurre un incidente dentro de una jurisdicción única y no hay un organismo jurisdiccional o superposición de funciones. El segundo es un comando unificado, que es un elemento importante en la gestión de incidentes. Proporciona directrices para que los organismos con diferentes responsabilidades legales, geográficas y funcionales para coordinar,



planificar, e interactuar con eficacia. El comando unificado funciona como una organización de gestión única e integrada.

6.2 Occupational Health and Safety Assessment Series(OHSAS) 18001³²

La normatividad Ocupacional Health and Safety Assessment Series (OHSAS) sobre gestión de la Seguridad y Salud en el Trabajo (SST) tienen como finalidad proporcionar a las organizaciones los elementos de un sistema de gestión de la SST eficaz que puedan ser integrados con otros requisitos de gestión, y para ayudar a las organizaciones a lograr los objetivos de seguridad y económicos. Esta normatividad, al igual que otras normas internacionales, no tienen como fin ser usados para crear barreras comerciales o para incrementar o cambiar las obligaciones legales de una organización.

La OHSAS 18001 especifica los requisitos para un sistema de gestión que permita a una organización desarrollar e implementar una política y unos objetivos que tengan en cuenta los requisitos legales y la información sobre los riesgos para la seguridad. Pretende ser aplicable a todos los tipos y tamaños de organizaciones y ajustarse a diversas condiciones geográficas, culturales y sociales. El éxito del sistema depende del compromiso de todos los niveles y funciones de la organización y especialmente de la alta dirección. Un sistema de este tipo permite a una organización desarrollar una política que establece objetivos y procesos para alcanzar los compromisos de la política, tomar las acciones necesarias para mejorar su desempeño y demostrar la conformidad del sistema con los requisitos. El objetivo global de esta OHSAS 18001 es apoyar y promover las buenas prácticas en SST en equilibrio con las necesidades socioeconómicas. .

6.2.1 Requisitos del sistema de gestión de la SST

Como primer paso se recomienda hacer una revisión inicial de comparación de la gestión actual de la Seguridad de la organización con los requisitos legales u otros requisitos aplicables), con el fin de determinar el grado con que estos requisitos se están cumpliendo



La revisión inicial proporcionará información que una organización puede usar para formular planes para implementar y priorizar mejoras en el sistema de gestión de la seguridad

El propósito de una revisión inicial debería ser considerar todos los riesgos a los que la organización se enfrenta, como base para establecer el sistema de gestión.

Una organización debería considerar, pero no limitarse, a los siguientes puntos dentro de su revisión inicial:

- * Requisitos legales y otros requisitos
- * Identificación de los riesgos
- * Evaluaciones de la seguridad en el área de trabajo
- * Examen de los sistemas, prácticas, procesos y procedimientos existentes
- * Evaluación de las iniciativas de mejora
- * Evaluación de la retroalimentación de la investigación de los incidentes
- * Sistemas de gestión pertinentes y recursos disponibles.

Cuando ya existan procesos de identificación de peligros y evaluación de riesgos, debería revisarse su adecuación frente a los requisitos del estándar OHSAS 18001 u otras aplicables a la organización. Hay que destacar que una revisión inicial no sustituye a la implementación del enfoque sistemático estructurado de la identificación, evaluación y determinación de los riesgos. Sin embargo, una revisión inicial puede proporcionar elementos de entrada adicionales para planificar estos procesos.

1. La alta dirección debe definir y autorizar las políticas de seguridad de la organización y asegurarse de que, dentro del alcance definido de su sistema de gestión está:
2. La naturaleza y magnitud de los riesgos
3. Prevención de los daños y el deterioro de la salud, haciendo explícita la mejora continua de la gestión de la seguridad
4. Compromiso de cumplir al menos con los requisitos legales aplicables



5. Hacerles conscientes a los trabajadores de sus obligaciones individuales en materia de seguridad
6. Hacer revisiones periódicas para asegurar que sigue siendo pertinente y apropiada para la organización.

La alta dirección deberá demostrar el liderazgo y compromiso necesarios para que el sistema de gestión de la SST tenga éxito y se logre un mejor desempeño.

6.2.2 Planificación y Desarrollo del sistema de gestión de la SST

Los riesgos pueden potencialmente causar daños o deterioro a la salud de las personas. Por tanto, es necesario identificar los riesgos como se describe en el capítulo 2. Una organización necesita aplicar el proceso de identificación y evaluación de riesgos para determinar los controles necesarios para reducir el riesgo de incidentes.

Es importante recomendar que las organizaciones desarrollen evaluaciones de riesgos genéricas para actividades típicas que pueden ocurrir en varios sitios o ubicaciones diferentes. Estas evaluaciones genéricas pueden ser útiles como punto de partida para evaluaciones más específicas, pero podría ser necesario adaptarlas para que resulten apropiadas a una situación concreta.

Este enfoque puede mejorar la velocidad y eficacia del proceso de evaluación de riesgos, y mejorar la coherencia de la evaluación de riesgos para tareas similares.

Cuando el método de evaluación de riesgos de la organización use categorías descriptivas para evaluar la severidad o probabilidad de daños, estas deberían estar claramente definidas. Por ejemplo, se necesitan definiciones claras de términos como “probable” e “improbable” para asegurar que personas distintas las interpretan de forma coherente. La organización debería tener en cuenta los riesgos para colectivos sensibles (por ejemplo, trabajadoras embarazadas) y grupos vulnerables (por ejemplo, trabajadores sin experiencia), al igual que las susceptibilidades particulares de cualquiera de los trabajadores involucrados en el desempeño de



tareas concretas (por ejemplo, la capacidad de una persona daltónica para leer instrucciones).

La organización debería valorar como la evaluación de riesgos tendrá en cuenta el número de personas que podrían estar expuestas a un riesgo determinado. Los peligros que podrían causar daño a un número elevado de personas deberían considerarse cuidadosamente, incluso cuando sea mucho menos probable que sucedan tales consecuencias severas.

La evaluación de riesgos que vaya a estudiar el daño causado por la exposición a agentes físicos, químicos, y biológicos podrían requerir medir las concentraciones de exposición con instrumentos y métodos de muestreo apropiados. Estas concentraciones deberían compararse con los límites de exposición o estándares aplicables en el trabajo. La organización deberá asegurarse de que la evaluación de riesgos tiene en cuenta las consecuencias de la exposición tanto a corto como a largo plazo y los efectos aditivos de múltiples agentes y exposiciones.

En algunos casos la evaluación de riesgos se lleva a cabo mediante muestreo para cubrir diversas situaciones y ubicaciones. Deberá tenerse cuidado de asegurarse de que las muestras utilizadas son suficientes y representan de forma adecuada todas las situaciones y ubicaciones que se están evaluando.

6.2.3 Determinar la Necesidad de Controles

Una vez completada una evaluación de riesgos y habiendo tenido en cuenta los controles existentes, la organización deberá ser capaz de determinar si los controles existentes son adecuados o necesitan mejorarse, o si se requieren nuevos controles. Si se requieren controles nuevos o hay que mejorarlos, su selección deberá determinarse por el principio de jerarquía de controles, es decir, la eliminación de riesgos cuando sea factible, seguida a continuación por una reducción del riesgo con la adopción de equipos de protección individual como último recurso.

A continuación se proporcionan ejemplos de implementación de la jerarquía de controles:



- * Eliminación: modificar un diseño para eliminar el riesgo, por ejemplo, introducir dispositivos de elevación mecánica para eliminar el riesgo de la manipulación manual.
- * Sustitución: sustituir un material menos peligroso o reducir la energía del sistema (por ejemplo, reducir la fuerza, amperaje, presión, temperatura, etc.)
- * Controles de ingeniería: instalar sistemas de ventilación, protecciones de máquinas, engranajes, insonorización.
- * Señalización, advertencias, y/o controles administrativos: señales de seguridad, marcado de área peligrosa, marcas para caminos peatonales, sirenas/luces de alarma, procedimientos de seguridad, inspección de equipos, controles de acceso, sistemas seguros de trabajo, permisos de trabajo y etiquetado, etc.

6.2.4 Iniciar una Auditoría

Una vez que se haya implementado todo el proceso de evaluación y se tenga bien definido los riesgos y como afectan se recomienda a la organización hacer auditorías periódicas que contengan los siguientes criterios:

- * Definir los objetivos, alcance y criterios de la auditoría. Los criterios de auditoría son las referencias frente a las que se comparan las evidencias de la auditoría, por ejemplo, OHSAS 18001, política y procedimientos de SST.
- * Seleccionar los auditores y el equipo de auditoría apropiada para la auditoría, teniendo en cuenta la necesidad de objetividad e imparcialidad.
- * Determinar la metodología de la auditoría.
- * Confirmar los preparativos de auditoría con el auditado y con otros individuos que vayan a tomar parte en la auditoría.
- * Una parte importante de este proceso es la determinación de cualesquiera reglas de SST aplicables en el lugar de trabajo. En algunos casos los auditores podrían necesitar formación adicional y podría requerírseles cumplir requisitos adicionales.



Una o más personas pueden llevar a cabo auditorías del sistema de gestión de la Seguridad. Un enfoque de equipo puede incrementar la involucración y mejorar la cooperación. Un enfoque de equipo también puede permitir que se usen un mayor rango de habilidades especializadas y permitir que los auditores individuales tengan competencias específicas.

A fin de mantener la independencia, objetividad e imparcialidad, los auditores no deberían auditar su propio trabajo.

Los auditores necesitan entender sus tareas y ser competentes para llevarlas a cabo. Los auditores deberán estar familiarizados con los peligros y los riesgos de las áreas que están auditando, y con cualesquiera requisitos legales y otros requisitos aplicables. Necesitan tener experiencia y conocimiento de los criterios de auditoría pertinentes y de las actividades que están auditando, para poder evaluar el desempeño y determinar las deficiencias.

6.2.5 Realizar las Revisiones de los Documentos.

Previo a la realización de una auditoría, los auditores deberán revisar los documentos y registros pertinentes del sistema de gestión de la SST, y los resultados de auditorías previas. La organización deberá usar esta información al hacer sus planes de auditoría.

La documentación que puede revisarse incluye:

- * Información sobre las funciones, responsabilidades y autoridades
- * La declaración de las políticas de seguridad
- * Objetivos y programas de seguridad
- * Procedimientos de auditoría del sistema de gestión de la seguridad
- * Los procedimientos e instrucciones de trabajo en seguridad
- * Resultados de la identificación de riesgos
- * Requisitos legales y otros requisitos aplicables
- * Informes de incidentes, no conformidades y acciones correctivas.



La cantidad de documentación a revisar y el detalle proporcionado en los planes de auditoría deberán reflejar su alcance y su complejidad. Los planes de auditoría deberán cubrir con los objetivos de la misma; así como, los criterios la metodología, la ubicación, el calendario de auditores y las funciones y responsabilidades de las distintas partes auditoras. La información para la planificación de la auditoría puede estar contenida en más de un documento. La atención deberá centrarse en proporcionar información adecuada para implementar la auditoría.

Si se necesitan incluir otras partes en el proceso de auditoría (por ejemplo, representantes de los empleados), esto deberá incluirse en los planes de auditoría.

CAPITULO 7

EL PLAN DE CONTINUIDAD DE NEGOCIO

7.1.-Iniciación del Plan de Continuidad de Negocio²⁶

La continuidad del negocio la define la Business Continuity Institute (BCI) como un proceso de gestión integral que identifica los impactos potenciales que amenazan una organización y proporciona un marco para la creación de una respuesta eficaz que salvaguarde los intereses de sus grupos de interés clave, la reputación y el valor de la creación de actividades.

Se comenzó a pensar más en la continuidad de negocio a través de los sucesos producidos de manera inesperada tanto en organismos mercantiles como para organismos públicos. Según la BCI la continuidad del negocio no es simplemente recuperación ante una crisis, más bien es un enfoque global de toda una gestión encaminada a un objetivo final de una organización.

Crea todo un marco estratégico de cómo la organización se fortalece en productividad y al mismo tiempo aumenta la resistencia ante un evento que provoque interrupciones o pérdidas. En forma general, el plan de continuidad consiste en identificar los impactos potenciales que amenazan a la organización, proponiendo un marco adecuado para reforzar la capacidad de dar respuesta ante cualquier riesgo.

Hay muchos posibles riesgos a los que está expuesta la organización por ello la implantación de un plan de continuidad de negocio no es algo que manejarse a la ligera. Consiste en una serie de pasos que conduce a una gestión adecuada de los riesgos.

El proponer una inversión de todo un estudio de riesgos para la continuidad de negocio no es fácil, ya que se debe presentar con una amplia explicación de todos los puntos en qué consistirá y que forma parte de los objetivos de la organización.



Es por eso que se crea todo un programa de venta de la seguridad de la información que consiste en seis pasos:

1. Entendimiento de los objetivos de la organización.
2. Técnicas de venta apropiada del plan de continuidad.
3. Diseño de la estrategia de la venta del plan de continuidad.
4. Componentes bien definidos de la propuesta del plan de continuidad especificando punto por punto lo que cubre en su totalidad marcando tiempos y papel por desarrollar desde las altas direcciones hasta los obreros.
5. Cierre de la venta del plan de continuidad.
6. Mantener comunicación después de la venta.

7.2.- Análisis del Plan de Continuidad²⁶

El objetivo principal es el diseño y la aportación de recursos para hacer frente a una situación de amenaza a la organización reflejada en impacto económico.

En la metodología de hacer un análisis de continuidad tiene seis puntos básicos:

1. Ver el valor de cualquier propiedad.
2. Frecuencia de un acontecimiento no deseado en el periodo de un año.
3. Impacto
4. Respuesta al impacto
5. Costo de la respuesta
6. Incertidumbre

Dentro de las metodologías existentes esta la Metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas), tiene como objetivo estudiar los riesgos entorno a la propiedad y su información y de ahí partir para la prevención, reducción y control de los riesgos ya investigados.

A su vez esta metodología maneja 3 submodelos:

Figura 7.1.- Submodelos de Prevención y Control²⁶

Dentro de las metodologías de administración y análisis de riesgos se mencionó en los capítulos 4 y 5, que entre los factores más importantes está la organización general dentro de una empresa, que conduzca a tener un control permanente con procedimientos de reglamentación y auditorías. Es importante la comunicación que se establezca dentro de la empresa con un plan informativo de seguridad y seguimientos bien establecidos.

7.3.- Análisis de Impacto³⁰

El objetivo es proporcionar la información necesaria para tomar las decisiones según sea la estrategia de recuperación. El impacto que se presente puede ser económico, jurídico, comercial y operacional de imagen, por tal motivo se deben fijarlas prioridades y establecer los umbrales máximos de recuperación como se ha mencionado antes.



7.3.1 Tipos de Impacto Económico.

Los impactos son las consecuencias de un evento no deseado referidas en un periodo de tiempo y pueden ser de diversos tipos como:

1. Pérdida de ingresos: cuando en una organización mercantil es la generación de ingresos y producir beneficios. El impacto puede impedir ese flujo y se debe valor cuantitativamente.
2. Incremento de costos y gastos: la interrupción de determinadas funciones pueden generar un incremento en los gastos de la organización, como multas, defectos, falta de control entre otros.
3. Ausencia del personal: este se da por un incidente o accidente y provoca que el personal, no se desempeñe adecuadamente. La valoración del personal debe ser cauteloso y minucioso.
4. Impacto operacional: se refiere a las funciones que afectan al funcionamiento de la organización.
5. Impacto comercial: si la interrupción de funciones dura más tiempo del previsto, el cliente se ve forzado a cambiar de proveedor, que las ventas se pierdan en la interrupción y puedan no recuperarse. Si presentan un servicio público, puede generar responsabilidades jurídicas y desconfianza del ciudadano.
6. Pérdida de la calidad: función que afecta la calidad del producto o servicios de la organización teniendo que interrumpir actividades.
7. Impacto a imagen: en el paro de actividades no se ven las pérdidas inmediatas en la imagen, pero con el tiempo se detecta el deterioro de la imagen de la organización, lo que se transforma en pérdida de mercado y desconfianza en el cliente.
8. Incumplimiento de obligaciones jurídicas: al interrumpirse las actividades puede generarse un problema por incumplimiento de obligaciones, lo que conlleva a causando sanciones o multas.



9. Impacto ambiental: depende del grado de sensibilidad de la sociedad ante la necesidad de conservación del medio ambiente.
10. Desmoralización del personal: interrupción cuya función afecte moralmente al personal, por ejemplo cuando hay pérdidas humanas.

En la siguiente tabla se muestra una serie de ejemplos de cómo serían los criterios de valoración de los diferentes impactos que puede sufrir una organización.

Tabla 7.1 Criterios de impactos en la organización³⁰

TIPOS DE IMPACTO	CRITERIOS DE VALORACIÓN			
	LEVE	MEDIO	GRAVE	CATASTRÓFICO
Ausencia del personal	Riesgo leve en la salud interno.	Riesgo grave en la salud de personal interno.	Peligro de muerte en el personal interno.	Peligro de muerte en el personal interno y externo..
Impacto operacional	Produce retrasos en funciones no vitales	Produce retrasos en funciones vitales	Produce retrasos graves en funciones vitales.	Produce interrupción inmediata en funciones vitales
Impacto comercial	Interrupción leve en el suministro de servicios o productos. La pérdida de venta se recupera al reanudar las actividades	Obliga al cliente a cambiar de forma transitoria. Las ventas ya 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.
Pérdida de la calidad	Produce un incremento leve en los productos defectuosos. No afecta al flujo necesario de salida de productos.	Produce un incremento sensible de productos defectuosos. Se resiente la salida de productos	Produce un incremento notable de productos defectuosos. La salida neta de productos cae gravemente.	Falla generalizada del producto con suministro interrumpido.



Impacto a imagen	Conocido por algunos clientes. Sin presencia de medios de comunicación.	Pérdida de confianza de un producto o servicio en una parte de la organización.	Pérdida de confianza en varios sectores de servicio o productos. Comentarios adversos de los medios de comunicación.	Pérdida de confianza del mercado y daños a la imagen. Campaña continúa de los medios de comunicación. Impacto en la bolsa de valores.
Incumplimiento de obligaciones jurídicas	Incumplimiento leve de algún contrato.	Incumplimiento de algún contrato que obliga a renegociar.	Incumplimiento grave de un contrato que causa responsabilidades legales.	Deja a la organización al margen de la ley.
Impacto ambiental	Impacto leve en el entorno de la organización	Daño leve del entorno de la organización de alcance limitado.	Produce impacto ambiental fuera del entorno de la organización con 1km ² sin riesgo para las personas.	Daño ambiental con extensión de varios kilómetros.
Desmoralización del personal	Inquietud de algunas personas del personal que es disipada por el propio entorno de trabajo.	Inquietud en un área de la organización.	Inquietud generalizada en la organización.	Produce graves problemas laborales con repercusiones en el exterior.

Esta información nos servirá para aquellas funciones críticas, de cómo se van a tomar las decisiones en las altas direcciones con criterios bien definidos actuando en los tiempos correctos para no gastar tantos recursos en la recuperación de un impacto.

7.4 Desarrollo de Estrategias de Continuidad.

Una vez que ya están las funciones críticas causadas por el impacto es tiempo de estudiar las posibles opciones para decidir la estrategia de recuperación que se va a dar en la brevedad posible dentro de los límites que quedaron como objetivo desde el principio.



Se puede comenzar con los siguientes puntos:

- * Tener las alternativas disponibles con ventajas y desventajas con un entorno de costos, incluyendo las medidas de a su vez reducir los riesgos.
- * Combinar con las áreas que están en funcionamiento las estrategias de recuperación de manera que salga pronto la organización del impacto que sufrió.
- * Tener como aprobación la estrategia por las encargadas de las unidades de negocio.
- * Presentar las conclusiones a la dirección para obtener la aprobación.

Existen varias formas de cómo tener un sistema de respuesta, en primer lugar dependiendo de los umbrales de recuperación, es el sistema de protección de información que se le va a dar y el tiempo de disponibilidad de la información.

Con el fin de garantizar su consistencia a lo largo de las diferentes unidades de negocio, el plan de continuidad de negocio debe considerar:

- * Condiciones para la activación del plan de continuidad.
- * Una estrategia de recuperación de desastres teniendo en cuenta aspectos como, costos de las diferentes alternativas, tiempos de recuperación, prioridades ante la emergencia.
- * Identificación de las responsabilidades y procedimientos de emergencia.
- * Implementación de procedimientos de emergencia para permitir la recuperación en un tiempo limitado.
- * Procedimientos de contingencia y procedimientos de regreso a la operación normal
- * Documentación de procedimientos y procesos acordados.
- * Educación apropiada sobre manejo de emergencias.
- * Cronograma de pruebas del plan de continuidad del negocio.



-
- * Responsabilidades individuales de ejecución y propietarios de cada plan de continuidad.

Una vez teniendo el escenario definido se requiere determinar cómo se va a actuar y la fórmula para su ejecución.

7.5 Entrenamiento y Pruebas de Mantenimiento de los Planes de Continuidad.²⁸

El plan de mantenimiento de planes y continuidad es un proyecto que debe abarcar a toda la organización. Esta deberá tener sesiones de seguimiento para conseguir los resultados requeridos, es decir debe de tener un seguimiento de pruebas para informar de los avances que se han obtenido y llegar al objetivo deseado. Además se debe entrenar a todos los que integren el plan de continuidad, de tal forma que los componentes de recuperación estén bien definidos no solo con un manual de “Plan de Respuesta”. Este Pla debe reflejar bien que hay un organismo vivo, que está constantemente evolucionando conforme marque las necesidades de recuperación ante las diferentes crisis que se puedan enfrentar.

Este plan deberá estar definido por lo siguiente:

1. **Objetivos:** Se debe desarrollar de forma que el personal siempre esté preparado para responder ante una crisis con revisiones periódicas, ejercicios de entrenamiento y pruebas anuales.
2. **Revisiones Periódicas:** Las revisiones periódicas son importantes, ya que en ella se darán cuenta si la disponibilidad de los recursos para la recuperación serán suficientes ante una crisis.
3. **Ejercicios de Entrenamiento:** Todo el personal que este dentro del equipo de recuperación tendrá que asistir a todas las sesiones que se impartan para estar actualizado en los procedimientos de respuesta, en estas sesiones se deberán identificar las necesidades del entrenamiento que se



debe de tener, como hacer un ensayo de en una situación de contingencia simulada, revisando y actualizando la documentación actual con exactitud de las responsabilidades del equipo y de los procedimientos. Desarrollar la metodología del entrenamiento, contemplar el caso de capacitación externa en caso que se requiera y realizar los entrenamientos periódicos. En estas sesiones cada integrante es libre de contribuir de acuerdo a los diferentes escenarios, en funciones y necesidades que se requiera

Los formatos de reunión en las sesiones impartida se deberán tocar los siguientes puntos:

- * Revisión del proceso de recuperación
 - * Seguimiento de las fases de recuperación
 - * Escenario
 - * Discusión de los puntos de referencia
 - * Revisar las necesidades
 - * Contemplar un lugar externo en dado caso que se requiera
4. Pruebas: Las pruebas son una parte importante del buen funcionamiento del plan de respuesta a una emergencia, se recomienda que se realicen anualmente determinando elementos tecnológicos y logísticos. Estas recomendaciones se basan en la experiencia de muchos ejercicios de recuperación y en dificultades surgidas en la práctica.

7.6 Gestión de la Crisis y Comunicación

El personal del área de relaciones públicas será el encargado de controlar toda la información y facilitarla a los medios de comunicación y entidades externas.

Este departamento deberá desarrollar, coordinar y evaluar los planes para un adecuado manejo de la información, no solo consiste en informar a los medios de comunicación de los acontecimientos, sino también a los trabajadores y familiares.



Es necesario que todos estos grupos reciban la información necesaria adecuada al momento.

Los objetivos en esta fase serán:

- * Establecer un programa que comunique la gestión de la crisis en la organización.
- * Tener una coordinación oportuna de la gestión de la crisis con organismos públicos
- * Establecer la comunicación oportuna con los grupos más afectados, como clientes, directivos y propietarios.

El departamento de relaciones públicas debe participar con el personal encargado de la gestión de accidentes para adquirir la mayor cantidad de información del lugar hora y causas de los sucesos. Tiene que informar si se dañaron las instalaciones, como los accesos actuales al edificio y si es necesario abrir más accesos en un corto plazo.

El departamento de relaciones públicas debe tener un amplio conocimiento en cómo manejar la información a los medios de comunicación para adelantarse a los acontecimientos sucedidos durante la crisis. Las responsabilidades del departamento mencionado deben ser las siguientes:

- * Coordinar los trabajadores del portavoz que se haya designado para la difusión de la información.
- * Dependiendo de la magnitud y gravedad de la crisis se deberá asignar el cargo y autoridad para brindar la información o en caso necesario llamar a un experto técnico en la materia.
- * Dar seguimiento periódico y recabar la información actualizada referente a los sucesos ocurridos.



-
- * Desarrollar una estrategia para atender a los medio de comunicación, es decir implantar el contacto y teléfonos que estén disponibles para proporcionar el avance de los acontecimientos a cada uno de ellos
 - * Organizar conferencias de prensa en la medida que sea necesaria.
 - * Coordinar la difusión d la información en los trabajadores
 - * Comunicar con las autoridades locales o estatales para notificar de la crisis.
 - * Preparar comunicaciones escritas y orales detallando la situación y el Plan de Acción Corporativo.
 - * Asegurar que durante los trabajos de recuperación, se registre y documente la información referente al acontecimiento.

7.7 British Continuity Institute (BCI)

El “British Continuity Institute (BCI) y British Standar Institute (BSI)” define “Business Continuity Management” (BCM) como un proceso de gestión integral que identifica potenciales impactos de una amenaza a la organización y provee una estructura flexible y una capacidad de efectiva respuesta que resguarde los intereses de sus inversionistas, clientes, empleados, reputación, marca y creación de valor. Teniendo en cuenta las siguientes aclaraciones:

- * BCM no es solo una respuesta, es la capacidad de una empresa para hacer frente a los impactos de un medio incierto.
- * BCM no es solo apagar fuego, es entender que pueden existir riesgos y establecer estrategias si pensamos que vamos hacia ello.
- * BCM no es solo tener planes súper elaborados, es tener planes que se acomoden a la naturaleza de su negocio.
- * BCM no está anexado al negocio, debe estar incorporado íntegramente con el gerenciamiento del proceso, gerenciamiento del riesgo en general como parte de un buen gerenciamiento del negocio.



La realización del BCM en la organización traerá grandes ventajas como por ejemplo:

- * Administrar la continuidad del negocio.
- * Resistencia del negocio ante interrupciones.
- * Detectar los aspectos vulnerables y las posibles causas.
- * Protege y asegura la imagen de la empresa.
- * Abre nuevas oportunidades de mercado y ayuda a ganar nuevos negocios.
- * Aumenta la disponibilidad del negocio.

7.7.1 Componentes de la Empresa

Los efectos de los incidentes, son múltiples afectando todos los niveles de la organización, el tema es tratado desde diferentes puntos de vista, pero se puede resumir como:

- * Las personas: son quienes trabajan en la organización, toman decisiones, soportan los procesos, operan máquinas. En este aspecto es importante tener en cuenta que si bajo los problemas organizacionales, profesionales o del hogar, estos individuos presentarán un buen rendimiento.
- * Los procesos: diversidad de estos existen en la organización, algunos más importantes que otros, incluso al nivel de detener el proceso productivo completo. Hay que identificar cada uno de ellos para determinar su impacto.
- * Tecnología: está presente en todos los lugares de la organización desde la oficina, en el área de producción, área de distribución y las comunicaciones entre equipos. No se trata sólo del uso de los sistemas informáticos, también los sistemas de control y procesos, comunicación telefónica. La importancia se nota cuando falla y prescinde de ella.
- * Comunidad o sociedad. Este punto no aparece en forma definida en las clasificaciones encontradas pero se ha considerado importante ponerla aquí porque hay dos puntos desde donde se puede enfocar el impacto. Los



Clientes son los que adquieren o utilizan nuestros servicios. Por otra parte, este punto está además va directamente relacionado con la reputación y la marca .Esto es especialmente importante cuando los incidentes son internos, pero se afectan a la comunidad.

7.7.2 Manejo de Continuidad de Negocio

Mientras el Business Continuity Management (BCM) es un programa de nivel estratégico, para llevar a la práctica este se debe elaborar un Business Continuity Management Program BCMP (Programa de Gerenciamiento y Continuidad del Negocio) el cual se define como un proceso de gerenciamiento continuo, para asegurarse, que regularmente se revisen los escenarios de posibles emergencias ,accidentes, desastres y amenazas .Lo que también involucra en la evaluación de los impactos de dichos eventos es una elaboración de estrategias de recuperación y planes de mantenimiento, documentación y entrenamiento al personal; la realización de pruebas o simulacros.

Un componente importante del BCMP es el Business Continuity Planning (BCP) o Plan de Continuidad de Negocio (PCN) que es la documentación, las actividades y recomendaciones para usar en los momentos de emergencia de continuidad de negocios los incidentes o crisis. Típicamente es un plan que cubre todo el personal clave, recursos, servicios y acciones que se requieren en el proceso de BCM. Un Business Continuity Management Program se compone de los siguientes pasos:

1. Definición del Programa. El objetivo de esta primera fase es establecer la necesidad de desarrollar el BCM en la organización, de tal manera que se comunique la importancia de realizar este plan, involucrando a los directivos y el personal de la empresa. Para esto, es importante: definir un comité responsable del plan, asignar responsabilidades por cada equipo de trabajo, indicar las actividades de cada una de las fases del proyecto, documentar los procesos, presentar los avances y obtener la aprobación por parte de los directivos.



-
2. Evaluación de amenazas y riesgo. Revisar de acuerdo a nuestro negocio cuáles son los riesgos o amenazas a los cuales se expone el negocio agrupándoles como se trato en el capítulo 2. La importancia de este paso es clave en la elaboración del programa, si evaluamos mal los riesgos obviamente se obtendrá un plan que no servirá para realizar una evaluación y control de riesgos y amenazas. Se debe tener en cuenta lo siguiente:
 - * Identificar riesgos Cuantitativo y Cualitativo.
 - * Evaluación de riesgos y amenazas
 - * Gestión y Control de riesgos
 3. Después de realizar la evaluación y el control de riesgos los resultados obtenidos incluyen la documentación de:
 - * La probabilidad de ocurrencia, en la organización, de un tipo específico de amenaza.
 - * Concentración de riesgos donde el número de actividades de misión crítica es localizado dentro del mismo edificio o en el mismo lugar.
 - * Una estrategia de gestión de control de riesgo y plan de acción.
 4. Análisis Impacto en el Negocio. El objetivo de un Análisis de Impacto del Negocio es identificar las actividades de misión crítica de una organización, sus dependencias y sus puntos de fallas así como analizar el impacto y el efecto que se generaría en caso de la perdida e interrupción de las actividades de misión crítica. A su vez, informar y permitir opciones para crear una resistencia en las operaciones de negocio de la organización. Sin embargo, la clave para realizar un análisis de impacto del negocio es analizar el negocio como un todo más no como componentes, procesos o funciones individuales. Para cumplir con este propósito es necesario que:
 - * Identifique componentes de los procedimientos de respuesta a emergencia.
 - * Especifique los procedimientos de respuesta a una emergencia.
 - * Identifique requerimientos de control y autoridad.
-



-
- * Procedimientos de control y autoridad.
 - * Respuesta a emergencia y recuperación de heridos.
 - * Seguridad y recuperación.

5. Desarrollo Implementación del plan de continuidad negocios. Esta fase involucra el diseño, desarrollo e implementación de planes de continuidad del negocio para evitar interrupciones de acuerdo a los marcos establecidos. Un buen desarrollo e implementación de un BCM incluye:

- * Identificar requerimientos para el desarrollo de los planes.
- * Definir requerimientos de control y administración de la continuidad.
- * Identificar y definir un formato y la estructura principal de los componentes de los planes.
- * Elaborar un borrador de los planes.
- * Definir procedimientos de gestión de crisis y continuidad del negocio.

7.7.3 British Standar Institute (BSI)

Las normas del BSI están regularmente formuladas por los miembros y otras partes interesadas acerca de la legislación vigente, la reglamentación y las normas que existen a nivel nacional e internacional para la Gestión de la Continuidad de Negocios.

Es difícil dar una lista definitiva porque hay cambios y modificaciones periódicas a nivel de país y con frecuencia incompatibles terminologías entre los países, sectores y legisladores.

El documento estándar a seguir se basa en la información proporcionada por los miembros en todo el mundo. Al final del documento se tiene una página de resumen de las iniciativas internacionales en curso y proyectadas en particular las patrocinadas por la Organización Internacional de Normalización (ISO) y el Comité de Convenio de Supervisión Bancaria.

Cada sección se divide en cuatro apartados. Para algunos países en los que podría no tener los datos disponibles en una sección particular.



Los cuatro apartados son los siguientes:

LEGISLACIÓN: Gobierno de leyes que incluyen los aspectos de la Continuidad del Negocio de Gestión por su nombre o son lo suficientemente similares en la naturaleza (la recuperación de desastres, respuesta a emergencias, gestión de crisis) asimilarse a la legislación BCM para este fin. Para ser incluido en esta categoría debe ser legalmente exigible la legislación aprobada por un grupo nacional, federal, estatal o del gobierno provincial en función de la estructura legal en cada país en particular.

REGLAMENTO: Las reglas obligatorias o documentos auditados a la orientación de organismos reguladores oficiales en todos los sectores como Servicios Financieros, Energía, Petróleo y Gas que, razonablemente, podría interpretarse como que tiene algunas implicaciones sobre las disposiciones BCM de una organización.

NORMAS: Las normas oficiales de nacionales (e internacionales) acreditadas por organismos de normalización que se refieren a la continuidad del negocio como un subconjunto relacionado total o específicas o como las tecnologías de la Continuidad del Servicio. La lista también incluye normas para temas diferentes pero relacionados entre sí (como la Seguridad de la Información).

7.8 Plan de Recuperación de Desastres

La mayoría de las empresas dependen en gran medida de la tecnología y los sistemas automatizados. De manera que su interrupción, incluso para un par de días puede causar pérdidas económicas graves y amenazar la supervivencia. La continuidad de las operaciones de una organización depende de la conciencia de la administración de desastres potenciales, su capacidad para desarrollar un plan para minimizar las interrupciones de las funciones críticas y la capacidad de las operaciones de recuperación oportunamente y con éxito. Un plan de recuperación



de desastres es una declaración completa de acciones coherentes que deben tomarse antes, durante y después de un desastre.

El plan debe ser documentado y probado para asegurar la continuidad de las operaciones y la disponibilidad de recursos críticos en el caso de un desastre. El objetivo principal de la planificación de recuperación de desastres es proteger a la organización en caso de que la totalidad o parte de sus operaciones y / o servicios son inutilizables. La preparación es la clave. El proceso de planificación debe reducir al mínimo la interrupción de las operaciones y garantizar un cierto nivel de estabilidad de la organización y una recuperación ordenada después de un desastre. Otros objetivos de la planificación de recuperación de desastres son:

- * Proporcionar un sentido de seguridad
- * Minimizar el riesgo de retrasos
- * Garantizar la fiabilidad de los sistemas de reserva
- * Proporcionar un estándar para probar el plan.
- * Minimizar la toma de decisiones durante un desastre

El proceso del plan de recuperación se puede resumir en de tres partes ilustra el proceso de planificación. La metodología se describe a continuación:

1. Obtener el compromiso de la Alta Dirección

La alta dirección debe apoyar y participar en el desarrollo del proceso de planificación de desastres de recuperación. La administración debe ser responsable de coordinar el plan de recuperación de desastres y asegurar su eficacia dentro de la organización. El tiempo y los recursos deben estar comprometidos con el desarrollo de un plan eficaz. Recursos podrían incluir tanto los aspectos financieros como el esfuerzo de todo el personal involucrado

2. Establecer un comité de planificación



Un comité de planificación debe ser diseñado para supervisar el desarrollo y la implementación del plan. El comité de planificación debe incluir a representantes de todas las áreas funcionales de la organización. Los miembros clave del comité deben incluir el gerente de operaciones y el gerente de procesamiento de datos. El comité también debe definir el alcance del plan.

3. Realizar una evaluación de riesgos

El comité de planificación debe preparar un análisis de riesgo y análisis del impacto empresarial que incluye una amplia gama de posibles desastres, así como las amenazas naturales, técnicos y humanos.

Cada área funcional de la organización debe ser analizada para determinar las consecuencias potenciales y el impacto asociado con varios escenarios de desastre. El proceso de evaluación de riesgos también debe evaluar la seguridad de los documentos más importantes y vitales.

Tradicionalmente, el fuego ha representado la mayor amenaza para una organización. Destrucción humana intencional, sin embargo, también deben ser considerados. El plan debe prever el "peor caso" la situación: la destrucción del edificio principal. Es importante evaluar el impacto y las consecuencias resultantes de la pérdida de información y servicios. El comité de planificación también debe analizar los costos relacionado con la reducción del riesgo de exposición.

4. Establecer prioridades para el procesamiento y las operaciones

Las necesidades críticas de cada departamento dentro de la organización deben ser evaluados cuidadosamente en áreas tales como:

- * Las operaciones funcionales
- * El personal clave
- * Información
- * Sistemas de procesamiento de Servicio
- * Documentación



- * Registros Vitales

- * Políticas y procedimientos

Las operaciones de elaboración deben ser analizadas para determinar la cantidad máxima de tiempo que el departamento y la organización puede funcionar el uno sin el crítico del sistema.

Las necesidades críticas se definen como los procedimientos necesarios y los equipos necesarios para continuar las operaciones cuando una instalación de departamento, centro de cómputo, principal o una combinación de estos se destruyan o se vuelven inaccesibles.

Un método para determinar las necesidades críticas de un departamento es el de documentar todas las funciones realizadas por cada departamento
Determinar estrategias de recuperación de información

Las alternativas más prácticas para el procesamiento en el caso de un desastre deben ser investigadas y evaluadas. Es importante tener en cuenta todos los aspectos de la organización tales como:

- * Instalaciones
- * Hardware
- * Software
- * Comunicaciones
- * Archivos de datos
- * Servicio al cliente
- * Las operaciones de usuario

Las alternativas van a depender de la evaluación de la función del ordenador, pueden incluir dentro de este plan sitios calificados como calientes que no son más que los que afectan directamente a la organización o sitios fríos que son afectaciones más leves en la organización. En las alternativas de recuperación se recomienda tener dos centros de datos, que estén respaldados en diferentes equipos o centro de



servicio, esto dependerá del tipo de servicio que la organización adopte para sus respaldos.

Los acuerdos por escrito para las alternativas de recuperación específicos seleccionados deben estar preparados, de manera que incluyan consideraciones especiales como pruebas de recuperación, costos, procedimientos especiales de seguridad, notificaciones de operación, requerimientos del personal o circunstancias en una situación de emergencia.

5. Realizar la recopilación de datos

Se recomienda la recolección de datos de materiales y documentación para un fácil acceso como:

- * Números de teléfono Crítico
- * Inventario de las comunicaciones
- * Los formularios de inventario
- * Seguro de inventario de la política
- * Lista de proveedores
- * Microcomputadora inventario de hardware y software
- * Oficina de inventario Estacionamiento fuera de lugar de almacenamiento de inventario
- * Los archivos de software y los datos de copia de seguridad Teléfono de inventario
- * Especificaciones de Ubicación temporal
- * Otros materiales y documentación

6. Organizar y documentar un plan por escrito

Un resumen de los contenidos del plan debe estar preparado para guiar el desarrollo de los procedimientos detallados. La alta dirección debe revisar y aprobar el plan propuesto. El esquema en última instancia, puede ser utilizado para la tabla de contenido después de la revisión final.

Proporciona una hoja de ruta para el desarrollo de los procedimientos



Un formato estándar debe ser desarrollado para facilitar la redacción de procedimientos detallados y la documentación de otro tipo de información que debe incluirse en el plan. Esto ayudará a asegurar que el plan de emergencia sigue un formato consistente y permite el mantenimiento en curso del plan. La normalización es especialmente importante si más de una persona está involucrada en los procedimientos por escrito.

El plan debe ser desarrollado a fondo, incluyendo todos los procedimientos detallados para utilizar antes, durante y después de un desastre. Puede que no sea práctico pero se pueden desarrollar procedimientos detallados hasta definir alternativas de copia de seguridad.

Los procedimientos deben incluir los métodos para el mantenimiento y actualización del plan para reflejar los importantes cambios internos, externos o sistemas. Los procedimientos deben permitir una revisión periódica del plan por parte del personal clave de la organización.

El plan de recuperación de desastres debe ser estructurado con un enfoque de equipo. Las responsabilidades específicas se deben asignar al equipo apropiado para cada área funcional de la empresa.

Debe haber equipos responsables de las funciones administrativas, instalaciones, logística, soporte al usuario, copia de seguridad informática, restauración y otras áreas importantes de la organización.

El equipo de gestión es especialmente importante, ya que coordina el proceso de recuperación. El equipo debe evaluar el desastre, activar el plan de recuperación, y proponerse en contacto con los jefes de equipo. El equipo directivo también supervisa, controla los documentos y el proceso de recuperación. Miembros del equipo de la gerencia del equipo deben ser el final de los tomadores de decisiones en el establecimiento de prioridades, políticas y procedimientos.

Cada equipo tiene responsabilidades específicas que se deben completar para asegurar la ejecución exitosa del plan. Los equipos deben tener un



gerente asignado y un suplente en caso de que el director del equipo no está disponible. Otros miembros del equipo también deben tener tareas específicas cuando sea posible.

7. Desarrollar criterios y procedimientos de prueba

Es esencial que el plan sea completamente probado y evaluado en forma regular (al menos una vez al año). Los procedimientos para poner a prueba el plan deben ser documentados. Las pruebas se proporcionarán a la organización con la seguridad de que todas las medidas necesarias se incluyen en el plan. Otras razones para la prueba son:

- * Determinación de la viabilidad y compatibilidad de las instalaciones de seguridad y los procedimientos
- * Identificación de áreas en el plan que necesita modificaciones
- * Proporcionar capacitación a los gerentes y miembros del equipo
- * Demostrar la capacidad de la organización para recuperar
- * Proporcionar motivación para el mantenimiento y actualización del plan de recuperación de desastres

8. Prueba del Plan

Después de los procedimientos de prueba se han completado, una prueba inicial del plan debe realizarse a través de un recorrido estructurado de prueba. La prueba deberá proporcionar información adicional sobre cualquier medida adicional que pueda necesitar para ser incluidos, los cambios en los procedimientos que no son eficaces, y otros ajustes necesarios. El plan debe ser actualizado para corregir los problemas identificados durante la prueba. En un principio, la evaluación del plan debe hacerse en secciones y después del horario normal para minimizar las interrupciones a las operaciones generales de la organización.

Tipos de pruebas son:

- * Lista de verificación de las pruebas
- * Las pruebas de simulación



-
- * Pruebas en paralelo
 - * Las pruebas de la interrupción completa

9. Aprobar el plan

Una vez que el plan de recuperación de desastres ha sido escrito y probado, el plan debe ser aprobado por la alta dirección. La responsabilidad última de la alta dirección que la organización tiene un plan documentado y probado.

La administración es responsable de:

- * Establecer políticas, procedimientos y responsabilidades para la planificación integral de contingencia.
- * Revisar y aprobar anualmente el plan de contingencia, la documentación de esos exámenes por escrito
- * Si la organización recibe tratamiento de la información de una empresa de servicios, la gestión debe:
- * Evaluar la adecuación de los planes de contingencia para su oficina de servicios
- * Asegúrese de que su plan de contingencia es compatible con el plan de su agencia de servicios.

CAPITULO 8

CONCLUSIONES

Como resultado de la elaboración del presente trabajo como Tesis, se concluye lo siguiente:

1. En base a la **hipótesis** establecida se desarrollaron una serie de criterios específicos que ayudarán a la empresa a identificar los riesgos previsibles a los que se esta expuesta y encontrar las soluciones probables para no salir del mercado.
2. Conocer la organización implica identificar sus objetivos, necesidades e intereses de las partes interesadas, las obligaciones y el ambiente donde la empresa está situada, seguido de la identificación de actividades, activos, y recursos, incluyendo aquellos necesarios para entregar productos y servicios críticos.
3. La concepción de que los desastres son eventos sociales más que naturales, nos obliga a considerar a la protección civil como un tema social que juega un papel clave en los procesos que inciden en los indicadores de desarrollo. En el proceso de construcción de este escenario, basado en la información estadística histórica disponible de nuestro país, así como la evaluación objetiva del presente y una concreta perspectiva del futuro nos ayuda a tener visibles los cambios y retos a vencer. Reconocer las condiciones indispensables para conseguirlo, permite identificar los factores de cambio, proyectarlos en la revisión y rediseño de nuestras prioridades y enfocar adecuadamente la planeación.



-
4. Es necesario continuar el esfuerzo de revisión crítica de los programas, planes, reglamentos y acciones vinculadas a la protección civil para no quedar rezagados, continuar con el reto de consolidar las tareas bien logradas y mantener una dinámica de mejora continua.
 5. Proponer un conjunto de procedimientos para identificar, analizar, evaluar y controlar los efectos adversos de los riesgos a los que está expuesta una empresa, con el propósito de evitarlos, reducirlos, retenerlos o transferirlos.
 6. Mantener un proceso continuo y permanente para la prevención, mitigación, preparación, respuesta y recuperación ante un incidente que amenace vidas, propiedades, operaciones o medio ambiente.
 7. Tener la combinación de personal, equipo, procedimientos de comunicación operando mediante una estructura organizacional común, diseñada para ayudar en la administración de los recursos durante los incidentes para reducir la severidad o consecuencia de una emergencia.
 8. El sistema de respuesta debe permitir una sencilla identificación de la naturaleza y extensión del incidente, cuales son las acciones para tomar el control de la situación, como contener el incidente y como comunicar a las partes interesadas. Este conjunto de acciones son la respuesta inmediata al incidente, también conocido como Plan de administración de Incidentes.
 9. La continuidad del negocio es un manejo de procesos que identifica impactos potenciales que pueden ser vividos en una organización y provee un marco de trabajo para la construcción de la capacidad de una respuesta efectiva la cual resguarda los intereses de los propietarios, reputación, marca y valores creando actividades de prevención lo cual significa que este sistema permite proteger los intereses de la empresa ante un desastre natural, caída de



negocios, crisis administrativa, emergencia administrativa, caída de los productos, ventas, crisis sociales de un país, crisis políticas, planes de contingencia, o simplemente un plan alterno.

10. La continuidad de negocio se encuentra dentro de los estándares de mitigación de riesgos que le dará a la empresa en un momento dado los parámetros para levantarse de un mal momento de cualquier índole, siempre y cuando se cuente con un plan bien diseñado que pueda abordar cada uno de los problemas presentados ante cualquier circunstancia que afecta la empresa y que forma parte clave para no salir del negocio.



REFERENCIAS

1. Journal NFPA Latinoamericano “Caso de estudio sobre implementación de la NFPA 1600: Programa Global para la Continuidad de los Negocios de Goodyear” por Michael W. Janko
2. Administración del Riesgo en Proyectos Modulo 1”
Notas del Ing. Ramon Dominguez Betancourt
3. Guía Básica para la Elaboración de Atlas Estatales y Municipales de Peligros y Riesgos. Fenómenos Geológicos
CENAPRED y Sistema Nacional de Protección Civil.
Primera Edición 2006.
4. Geología
José Ma.Fuster, Editorial Paraninfo
4° Edición.
5. Conceptos Básicos sobre Peligros, Riesgos y su representación Geográfica, de la Guía Básica para la Elaboración de Atlas Estatales y Municipales de Peligros y Riesgos.
Enrique Guevara O., et. al., CENAPRED y Sistema Nacional de Protección Civil. Primera Edición 2006.
6. Programa Especial de Prevención y Mitigación del Riesgo y Desastre 2001-2006.
Secretaría de Gobernación, CENAPRED y Dirección General de Protección Civil.
Primera Edición 2006.
7. Diagnostico de Peligros e Identificación de Riesgos de Desastres en México.”
Secretaría de Gobernación
CENAPRED y Dirección General de Protección Civil.
Primera Edición 2001.
8. Ciencias de la Tierra, Una Introducción a la Geología Física
Edward J. Tarbuck, Editorial PEARSON.
8° Edición.
9. Las Organizaciones Internacionales y la Lucha Contra el Terrorismo, Centro Superior de Estudios de la Defensa Nacional



Jesús Joaquín Val Catalán Jefe de la Escuela de Altos Estudios de la Defensa,
Edición 2005.

10. National Strategy for Combating Terrorism
February 2003
11. A research guide to concepts, theories, data bases and literatura,
Schmid, Alex P., Política Terrorism New Brunswick, N.J.,
Transaction Books, 1983, pp119-153
12. Acerca de los sicarios y los asesinos, ver Weinberg,
Leonard B. y Davis Paul B. Introduction to Political Terrorism,
Mc Graw-Hill Publishing
Company, New Cork, 1989, pp 19-22
13. La ideología de la cultura libre y la gramática del sabotaje
Rotterdam, Pasquinelli, Matteo. Editores del NA
Edición 2008.
14. Una Breve Historia de Terror”
Enrique Obando Arbulú.
15. Ley de protección civil
Nueva Ley publicada en el Diario Oficial de la Federación
12 de mayo de 2000
16. A Guide to the Project Management
Body of Knowledge (PMBOK® Guide)
Edition 2000
17. Instituto de Gestión de Proyectos
Four Campus Boulevard, Newtown Square
PA 19073-3299 USA, ©2000
18. The Delphi Method. Techniques and Applications
Linstone, H., Turoff, M.
Addison-Wesley, 1975, p.3
19. Manuel de Prospective Strategique. Dunod. Paris
Godet, Michel. (1996).
20. Technological forecasting for decision making
MARTINO J.P



Mac Graw Hill, 1993.

21. Política Pública de Seguridad y salud en el Trabajo. Programa de Autogestión en Seguridad y Salud en el Trabajo
Lineamientos Generales de Operación (PASST).
2007-2012
22. La Simulación como una herramienta para el manejo de la incertidumbre
Fabian Fiorito Universidad de CEMA.
Master en Finanzas 2006.
23. Una Reparametrización de la distribución triangular en las distribuciones
Juan F. Olivares Pacheco, Davis Elal Olibero, Hector W. Gomez y Heleno Bolfarine.
Junio 2009 ,pp145 a 156.
24. Introductory Statistics for Business and Economics.
John Wiley, Wonnacott R. y Wonnacott T.
Nueva York, EE.UU. (1990).
25. Experiencias en la Implantación de Planes de Emergencia de Presas
Jorge Durán Bravo.
Comité Nacional Español de Grandes Empresas
26. Guía de planificación de continuidad del negocio
(BUSINESS CONTINUITY PLANNING GUIDE),
Business Continuity Institute
www.bsi.com
27. Planes de Contingencia. La continuidad del negocio en las organizaciones
Juan Gaspar Martínez,
Editorial Díaz de Santos
2004.
28. Política de Continuidad del Negocio (BCP,DRP),
SISTESEG Bogotá Colombia.
<http://www.business-continuity-world.com>.
29. British Standar Institution,
Talking Business Continuity,
<http://www.talkingbusinesscontinuity.com/>.
30. Business Continuity and Disaster Recovery,
<http://www.bcm-institute.org/bcmi10/en/about-us>.



-
31. National Incident Management System,
Homeland Security Washington
Edition 2008
 32. Sistemas de Gestión de la Seguridad y Salud en el Trabajo.
Directrices para la implementación de OHSAS 18001
2007
 33. <http://www.seguridad.unam.mx>
 34. Department of Homeland Security de USA.
<http://www.dhs.gov>.
 35. <http://www.snet.gob>
 36. <http://spain.irca.org/inform/issue19/LBird.html>
 37. <http://ggc-tec35.wikispaces.com/1.1+LITOSFERA>