ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE CIENCIAS ADMINISTRATIVAS

PROPUESTA DE UN PROGRAMA DE GESTION DE CRISIS

TESIS PREVIA A LA OBTENCIÓN DEL GRADO DE MAGÍSTER EN GERENCIA EMPRESARIAL

JOSE WILLIAN GUALOTUÑA GUALOTUÑA

DIRECTOR: DR. KLEBER HERNAN MEJIA GUZMAN

Quito, Julio de 2007

DECLARACIÓN

Yo, José Willian Gualotuña Gualotuña, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

ING. JOSE WILLIAN
GUALOTUÑA GUALOTUÑA

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por José Willian Gualotuña Gualotuña , bajo mi supervisión.

DR. KLEBER MEJIA GUZMAN
DIRECTOR DE TESIS

AGRADECIMIENTOS

- A la Escuela Politécnica Nacional, a los directivos y profesores de postgrado de la Facultad de Ciencias Administrativas por compartir sus conocimientos y aportar con ello al desarrollo de la sociedad y del país.

- Un agradecimiento especial al Dr. Kleber Mejía Guzmán por su acertada dirección.

DEDICATORIA

- A mis padres que gracias a Dios aun los conservo, por el apoyo incondicional

- A mis hermanos por su apoyo moral que siempre me han brindado.

Willian Gualotuña

CONTENIDO

INDICE DE FIGURAS Y CUADROS

RESUMEN

En los últimos años las crisis inducidas por el hombre han ido en aumento, una de las razones es la complejidad de las organizaciones y de los sistemas, que se han creado con la sistematización y globalización del comercio.

Lo que sabemos con certeza es que los accidentes graves y los desastres nos toman casi siempre desprevenidos, cualquiera sea su causa. A pesar de todos los esfuerzos somos aparentemente incapaces de pronosticarlos o prevenirlos. Da la impresión que los sistemas de gestión, las técnicas de auditoría y los procedimientos de certificación se fijan en los elementos equivocados. Generalmente las auditorías sólo se fijan en si está la documentación; los sistemas de gestión son demasiado burocráticos o no se interesan en identificar riesgos y peligros.

Existen coincidencias entre las crisis causadas por el hombre y los desastres naturales, pero también existen diferencias principalmente en que las primeras no necesariamente suceden, es decir son evitables, de ahí la necesidad de una gestión de crisis efectiva.

Recientes eventos que han tenido lugar a nivel mundial nos han planteado el reto de estar preparados para situaciones inimaginables que pueden poner en peligro el futuro de nuestras organizaciones. Este nuevo reto va más allá del mero plan de respuesta ante emergencias habitualmente aplicados. Las organizaciones deben afrontar un proceso de planificación para la Continuidad del Negocio.

Las amenazas actuales requieren la creación de un proceso interactivo que permita asegurar la continuidad de las actividades básicas y principales del negocio, antes, durante y quizás lo más importante, después de haberse producido una situación de crisis.

En un entorno altamente competitivo, las organizaciones no pueden permanecer inactivas por prolongados periodos, reaccionar en forma lenta o experimentar procesos inflexibles. Por ello surge la necesidad de explicar los objetivos, alcance y fases de un plan de continuidad organizacional.

En este contexto, un programa de gestión de crisis(continuidad organizacional) debe garantizar las operaciones necesarias para cumplir con el funcionamiento establecido en el desarrollo habitual del negocio ante cualquier tipo de desastre, interrupción o contingencia. La alta dirección debe prever la disposición de recursos necesarios para asegurar la continuidad de estas actividades. La gestión ante este tipo de situaciones no debe ser improvisada, lo que demanda una estructura administrativa creada y preparada para tal fin.

La toma de decisiones, su significado e implicación en la gestión de crisis, así como las funciones y responsabilidades, deben estar definidos previamente para una eficaz gestión de la misma.

La importancia del tema ha demandado principalmente en los países desarrollados la creación de centros de estudios dedicados al tema continuidad organizacional, tal es el caso de la University of Southern California(USC) que tiene a su cargo el Centro de Gestión de Crisis. De igual manera la oferta de cursos a nivel de maestría relacionados con el tema, se ha incrementado en los últimos años.

PRESENTACIÓN

El presente trabajo tiene la finalidad de dar a conocer los diferentes conceptos relacionados con la continuidad organizacional y cual debería ser el alcance de la gestión integral de eventos adversos que pueden afectar a una organización.

En este contexto el presente trabajo esta dividido en cinco capítulos, cuyo contenido lo resumimos a continuación:

En el capítulo uno, se describe algunos conceptos y herramientas de gestión contemporáneas relacionadas con el tema en estudio.

En el capítulo dos, se describe la nueva tendencia en la gestión de riesgos empresariales y la continuidad del negocio. En el estudio del estado del arte de la gestión de crisis (GC) se describe su evolución y un análisis de las distintas terminologías utilizadas para nombrar al proceso de gestión integral de la continuidad organizacional.

El capítulo tres, describe los conceptos en los que se fundamenta la gestión de crisis, además del proceso global para realizar una gestión integral, donde una de las principales actividades ha realizarse es el diagnóstico de la preparación organizacional ante eventos adversos. El capítulo termina con la exposición del modelo de gestión de crisis propuesto.

En el capítulo cuatro, mediante un caso práctico se ejemplifica la elaboración de un programa de GC y la aplicación del modelo de GC propuesto, para una empresa de servicios.

Finalmente en el capítulo cinco, se presentan las conclusiones y recomendaciones del tema.

CAPÍTULO 1

CONCEPTOS Y DEFINICIONES

1.1 ESTRATEGIA EMPRESARIAL

La globalización del mercado, los avances tecnológicos y los cambios en el entorno empresarial están motivando a que los directivos de empresas diseñen el futuro en forma meditada, alejada de la improvisación, empleando para ello el análisis conceptual y un proceso metodológico basado en aspectos que configuran el entorno coyuntural, en las expectativas existentes y en los logros esperados.

En este sentido, vale la pena revisar un par de definiciones de Estrategia:

"Estrategia empresarial no es otra cosa que el conjunto de orientaciones, metas y medios que se identifican con la finalidad de definir un derrotero a la empresa. Es el marco de referencia que delimita el campo de acción, el cual permite integrar las actividades y los propósitos de diversas áreas de la empresa y del personal en particular, al señalarles los alcances, las limitaciones y las prioridades del quehacer empresarial y cómo esto incide en las actividades de cada uno".[1]

"Estrategia es el patrón o plan que integra las principales metas y políticas de una organización y, a la vez, establece la secuencia coherente de las acciones a realizar. Una estrategia adecuadamente formulada ayuda a poner orden y a asignar, con base tanto en sus atributos como en sus deficiencias internas, los recursos de una organización, con el fin de lograr una situación viable y original,

[1] Armando Aramajo. (2006). Diseñando la Estrategia Empresarial
http://www.secretosenred/leer_nota.php?ID_contenido=644

así como anticipar los posibles cambios en el entorno y las acciones imprevistas de los oponentes inteligentes".[2]

Un Plan Estratégico es el resultado de un Planeamiento, éste es un proceso y a la vez un concepto que debe formar parte de la cultura empresarial, que involucra actitudes de apoyo, compromiso y manejo del cambio a todo nivel. Para poner en práctica este proceso, es importante tener presente el concepto de Administración Estratégica, el mismo que según algunos autores se define como:
"La Administración estratégica es el arte y la ciencia de formular, implementar y evaluar las decisiones interfuncionales que permiten a la organización alcanzar sus objetivos".[3]

Un dato importante a rescatar, es el hecho de que la Estrategia debe brindar la posibilidad de "*anticipar los posibles cambios en el entorno y las acciones imprevistas*", de ahí que no esta fuera de lugar, lo que el experto en el tema Gestión de Crisis, Ian Mitroff, propone respecto a que "la Gestión de Crisis, debe ser parte de la Planificación estratégica dentro del marco de la cultura de prevención en las organizaciones". [4]

En una situación de crisis la estrategia es la que nos permite evolucionar hacia una situación más favorable. Además, las organizaciones deben adoptar una posición proactiva y no sólo reactiva, deben esforzarse por influir, anticipar y no únicamente responder a ellos.

---

[2] Mintzberg H., Quinn J. y J. Voyer. (2002). El Proceso Estratégico. México : Printice Hall. Primera edición. p.7

[3] David Fred R. (1997). Conceptos de Administración Estratégica. México : Prentice-Hall. Quinta edición. p 4.

[4] Mitroff I. y C. Pearson. (2000). Cómo Gestionar una Crisis. Barcelona : Gestión 2000. pp.119-120.

1.1.1 PROCESOS

Es conocido en el ambiente de gestión empresarial la importancia que se le da a los procesos en las diferentes filosofías y técnicas contemporáneas. En este sentido veamos una definición:

"Proceso es un grupo organizado de actividades relacionadas que juntas producen un resultado de valor a un cliente". The Agenda, Hammer 2001[5]
En este sentido una organización se podría concebir como un conjunto de procesos interrrelacionados, los mismos que están soportados por personas, equipos, herramientas, técnicas y materiales para cumplir los objetivos organizacionales.

Adicionalmente, en un principio de la norma ISO 9004:2000, *Enfoque basado en procesos*, dice: "Un resultado deseado se alcanza más eficientemente cuando las actividades y los recursos relacionados se gestionan como un proceso". Lo anterior se refuerza con otro principio: *Enfoque de sistema para la gestión*: "Identificar, entender y gestionar los procesos interrrelacionados como un sistema, contribuye a la eficacia y eficiencia de una organización en el logro de sus objetivos".[6]

De esta última parte podemos destacar la importancia de entender los procesos como un sistema y por ende la organización, para una gestión efectiva. Con esta consideración, es válido el enfoque de Gestión de Crisis(GC) que se adopta para la propuesta.

---

[5] Arroyo Eduardo. Universidad Metropolitana. Fundamentos de procesos: Definiciones y clasificaciones. http://www.suagm.edu/ac/ac_new_web/oficina_presidente/calidad/links/pres/fundamentos.ppt

[6] www.grupokaizen.com. Procesos de negocios, p.3 www.grupokaizen.com/mck/Procesos_de_Negocios.pdf.

1.1.2 CADENA DE VALOR

Según Porter, valor es la cantidad que los clientes están dispuestos a pagar por lo que una organización les proporciona. En este sentido la meta de cualquier estrategia es crear el valor para los clientes que exceda el costo de hacerlo.[7]
Las actividades de valor se dividen en dos tipos: actividades primarias y actividades de apoyo. Las primarias son aquellas que están implicadas directamente en la creación del producto o servicio, su venta y transferencia al cliente y los servicios post venta. Las de apoyo en cambio, son las que dan soporte a las primarias y además se apoyan entre sí.

En este contexto, la cadena de valor es una forma de análisis de la actividad empresarial mediante la cual se descompone una empresa en sus partes constitutivas, con la finalidad de identificar fuentes de ventaja competitiva en aquellas actividades generadoras de valor.[8]

Mediante este análisis es posible identificar las actividades o los procesos críticos para la organización a los cuales debemos en principio poner mayor atención en la gestión diaria, y muy en especial en la gestión de riesgos.

1.1.3 PROCESOS Y ESTRATEGIA [9]

La teoría administrativa al igual que el de la estrategia ha evolucionado influenciado por los cambios en el entorno organizacional y la economía. En este contexto debemos destacar la intensa competencia por la preferencia del cliente producto de la globalización de la economía, reducción del ciclo de vida de los productos y los cambios tecnológicos continuos, lo cual demanda una diferenciación estratégica para competir en el mercado con ventaja.

---

[7] Lincango Miguel Angel. (2006). Administración por procesos. Universidad Central. Quito. p. 35

[8] www.gestiopolis.com. (2007). Cadena de valor. www.gestiopolis.com/recursos/experto/catsexp/pagans/eco/no12/cadenavalorporter.htm

[9] Aporte de Grupo Kaizen. (2006). Moviendo la frontera de la estrategia. pp. 1-20 http://www.gestiopolis.com/canales5/ger/gksa/docs/38.pdf.

Según Porter, la diferenciación en este ambiente de alta competitividad es “temporal” debido a que los competidores pueden copiar rápidamente la estrategia de una organización.
También se manifiesta que las técnicas para mejorar la eficiencia operativa, tales como la ISO 9000, calidad total, reingeniería, benchmarking, etc logran su cometido únicamente a corto plazo, ya que no logran mantener la ventaja competitiva diferenciadora a largo plazo. En este contexto, las técnicas son un requisito pero adicionalmente hay que buscar la efectividad estratégica cuyo significado es “desempeñar actividades diferentes a la de los competidores”, es decir que la organización debe buscar una innovación estratégica.

Esta evolución de conceptos administrativos y de estrategia, trae consigo nuevos paradigmas gerenciales, que se han movido desde la eficiencia y optimización de la producción, hasta la búsqueda de diferenciación y un posicionamiento único en el mercado, para garantizar la creación de Valor para clientes, accionistas y empleados. En este sentido, la implementación de la GC es una opción para conseguir la diferenciación a largo plazo, ya que es única para cada organización.

1.2 APRENDIZAJE ORGANIZACIONAL

Debido a los constantes cambios en el entorno organizacional, es necesario ser más veloces en adoptar nuevas creencias, en cultivar nuevos valores y en adquirir nuevas habilidades para llegar a un nuevo orden relacional en la organización; en este sentido se manifiesta que el aprendizaje es el testimonio de un cambio.

Fiol y Lyles establecen que el aprendizaje organizacional es "un proceso que emplea el conocimiento y el entendimiento orientado al mejoramiento de las acciones". [10]

[10] Medina César y Mónica Espinosa. (1996). El aprendizaje organizacional: el estado del arte hacia el tercer milenio. www.azc.uam.mx/publicaciones/gestion/num10/doc6.htm

Para Senge las “Learning Organizations(Organizaciones que aprenden) son organizaciones donde la gente expande continuamente su aptitud para crear los resultados que desea, donde se cultivan nuevos y expansivos patrones de pensamiento, donde la aspiración colectiva queda en libertad, y donde la gente continuamente aprende a aprender en conjunto”.[11]

Diseñar una organización que aprende, puede resultar complicado, debido a que es necesario adoptar nuevas prácticas de trabajo y romper con los patrones tradicionales de pensamiento y conducta, por ello además de adoptar una estructura plana y ágil que facilite la comunicación y la transferencia de conocimiento se requiere de persistencia, compromiso y un gran liderazgo.

En el marco de la Gestión de Crisis integral, el aprendizaje contribuye mediante el análisis de experiencias pasadas, a perfeccionar su gestión tanto en la prevención, el tratamiento y la recuperación de un evento adverso.

1.2.1 CULTURA ORGANIZACIONAL

La cultura organizacional lo podemos interpretar como el conjunto de creencias y valores compartidos, los cuales expresan la esencia de una organización, enmarcan las expectativas, suministran alineación y establecen el fundamento para la transformación y el crecimiento.

“La cultura representa la manera como la organización ve el ambiente y se ve a sí misma”.[12]
Entre los principales componentes de la cultura organizacional podemos citar: los valores dominantes, las normas o reglas, la filosofía administrativa, el comportamiento cotidiano y el clima organizacional.

---

[11] Gestión del conocimiento.com. (2006). Aprendizaje Organizativo. http://www.gestiondelconocimiento.com/conceptos_aprendizajeorganizativo.htm

[12] Chiavenato Idalberto. (2002). Gestión del talento humano. Bogotá: Mc Graw-Hill Interamericana. p.14

Una cultura adecuada es necesaria para dar soporte a cualquier emprendimiento en la organización, tal como el de la Gestión de Crisis.

1.3 LIDERAZGO

Según Bennis Warren, "El liderazgo es arte y ciencia a la vez. Los métodos analíticos pueden ser útiles en las ciencias, pero el instrumento principal del líder como artista es el mismo líder y la creatividad que pueda poner en su propia personalidad. Si el líder no comprende sus propios actos puede convertirse en portador de problemas y no en quien debe resolverlos."[13]

A continuación se describen ciertas características que debe cumplir un buen líder:

- Un líder debe enfocar el futuro(visión) desde donde está la organización y nutrir una cultura positiva y creativa marcada por el optimismo.
- Un Líder eficaz hace alianzas y construye equipos. La construcción de equipos, dota a la gente del sentido de la responsabilidad para que el impulso de crecer y transformarse se origine en toda la organización y no sólo en la cabeza.
- Un líder debe establecer flexibilidad y elasticidad dentro de la organización, acondicionándolas para que no nos sorprenda cuando ocurra lo inesperado.

Una buena herramienta para el líder es utilizar el hábito de la reflexión, mediante cuestionamientos tales como: ¿Qué está pasando? ¿Qué no está pasando? ¿Cómo puedo influir en la situación?. [14]

---

[13] Bennis W. y P. Slater. (1999). The temporary society. SanFrancisco : Jossey –Bass. p.127.

[14] Gordon R. Sullivan, Michael V. Harper. Liderar el cambio: Tomado del libro: La esperanza no es un método.
http://www.lafamilia.info/ayudasptrabajarmejor/liderarelcambio.htm

El liderazgo es otro elemento a tomar en cuenta en un emprendimiento de mejora en la gestión organizacional, que influye en el éxito de su implementación.

.3.1 LIDERAZGO EN TIEMPO DE CRISIS [15]

Podemos decir que las épocas de crisis se caracterizan por la modificación de manera incierta de la situación actual, hacia una que se aprecia potencialmente desfavorable, por ello hay una mayor preocupación por el futuro y por las consecuencias de las acciones que se realizan y las decisiones que se adoptan. En estas circunstancias el líder debe ser capaz de articular una *Visión*, difundir su *Ejemplo* y brindar *Apoyo*.

1.3.1.1 UN LÍDER DEBE TENER VISIÓN

En tiempos de crisis un líder debe tener una idea clara del futuro hacia el que se dirige y los caminos a transitar para alcanzarlo. Debe ser capaz de contagiar la visión a sus seguidores. Para ello, él mismo tiene que estar personalmente comprometido y convencido de la validez de lo que hace, de la posibilidad de alcanzar los objetivos y de la razonabilidad de los mismos.

1.3.1.2 UN LÍDER DEBE DIFUNDIR EJEMPLO

Un líder debe ser modelo para quienes lo siguen, ser el espejo en que se miran sus seguidores, ser motivo de inspiración para aquellos a quienes conduce y lidera. En situaciones de crisis, mientras mayor incertidumbre exista sobre la manera de salir de ella, mayor transparencia debe pedirse a la figura del líder.
El líder debe señalar sin vacilaciones el rumbo a seguir, ya que una actitud temerosa, dubitativa, desconcertada, servirá solamente para aumentar la incertidumbre y destruir la confianza. El líder debe mantener y acrecentar, su

---

[15] De la Fuente. (2002). Liderazgo en tiempos de crisis.
http://www.inun.edu.ar/elinun02/ambito/delafuente/Liderazgotiempocrisis3.htm

actitud proactiva, su voluntad incansable y ejercer sin vacilaciones la responsabilidad que le ha sido confiada.

1.3.1.3 UN LÍDER DEBE BRINDAR APOYO

Un líder en tiempos de crisis debe ejercitar una sensibilidad particular que le permita apoyar a quienes dependen de él. Debe privilegiar la comunicación con todos, haciéndose eco de las necesidades de sus subordinados, invirtiendo su tiempo en construir puentes de consenso y cooperación, privilegiando las situaciones que produzcan mayor armonía sobre las decisiones.

Además debe, comprometer su capacidad, sabiduría, aptitudes para relacionarse, convencido de que debe escuchar mucho y hablar sólo lo necesario. Infundir optimismo, mentalidad ganadora, convicción de que las metas van a ser logradas y que todos participarán de los beneficios del éxito.

1.3.2 EL LIDERAZGO DEL FUTURO

Los líderes del nuevo milenio deben estar conscientes de que el futuro es incierto y que es necesario analizar el pasado antes de avanzar a ciegas hacia el futuro.
A continuación indicamos cuatro principios a tomar en cuenta por los nuevos líderes:[13]

- El liderazgo es cosa de todos no sólo de los directivos, por lo que debe ejercerse en toda la organización.
- El liderazgo es una relación basada en la confianza entre los que aspiran a liderar y los que están dispuestos a seguirlos, por lo tanto el éxito del liderazgo dependerá de la capacidad de trabajar y colaborar con los demás.
- Los líderes buscan el sentido de la urgencia y acción, al hacerlo descubren y aprenden. Una de las funciones más importantes de un buen liderazgo es

---

[13] Bennis W., Spreitzer G. y T. Cummings. (2006). Las claves del Liderazgo. Barcelona : Ediciones Deusto. pp. 94-103.

conseguir que sus seguidores actúen, experimenten, opinen, insistan, innoven y aprendan.

- El conocimiento de sí mismo condiciona el éxito de un buen líder, porque mientras no se conozca a sí mismo, no conoce sus fortalezas y debilidades y resulta difícil triunfar en cualquier aspecto de la vida.

1.3.3 MODELO DE DIRECCIÓN DEL FUTURO [13]

El antiguo modelo de dirección así como el liderazgo (los directivos dirigen y los empleados trabajan) tienen poco sentido en economías y sociedades en las que predomina el conocimiento.

Al ser el conocimiento un activo intangible que reside en la mente humana, la función directiva ya no puede orientarse a observar y controlar a los empleados. No tiene sentido ya la separación entre directivos y empleados, al ser el conocimiento la clave del crecimiento y de la diferenciación de las actuales economías.

En estas condiciones, el rol de los directivos del futuro debe pasar: de vigilar únicamente el trabajo a participar en él, de organizar jerarquías a organizar equipos de trabajo, de imponer sistemas y métodos de trabajo a entenderlos, de contratar y despedir personal a buscarlos y conservarlos.

Warren Bennis, propone el Liderazgo Compartido, el cual supone compartir la alta dirección y distribuir las responsabilidades. Esto significa reforzar a personas de todos los niveles dándoles la oportunidad de tomar iniciativas. Esta tendencia es más común en la medida que la estructura jerárquica esta dando paso a formas más planas y descentralizadas, que en opinión de algunos expertos es una forma de generar agilidad, iniciativa y autonomía.

---

[13] Bennis W., Spreitzer G. y T. Cummings. (2006). Las claves del Liderazgo. Barcelona : Ediciones Deusto. pp. 53-61,156.

1.4 GESTION DEL CONOCIMIENTO

En la época actual donde la nueva economía de negocios esta basado en el conocimiento y, las exigencias del mercado son mayores, se establece la necesidad de enfrentar aquella dinámica con un nuevo enfoque.
A pesar de aquello, muchas organizaciones no utilizan todo su potencial basado en el conocimiento para enfrentar esos cambios, ya que generalmente no se encuentran organizados los procesos de generación y explotación del conocimiento o porque la cultura instaurada no ayuda en su aplicación, por ello es muy probable que existan ventajas potenciales que no han sido explotadas o las estrategias establecidas no las apoyan directamente.

En este sentido, Gestionar el Conocimiento significa, identificar, inventariar, aumentar y explotar ese conocimiento en función de la interrelación de los intereses de una organización y de aquellos que son portadores del conocimiento, por lo tanto, estos intereses deben ser conjugados para obtener la ventaja competitiva.

“En las empresas, una parte del conocimiento que poseen es tácito, y por esta razón, tiene lugar una pérdida de conocimiento cuando un empleado se marcha de la empresa, o se encuentra ausente”.[16]

Hoy se habla de Capital Humano, como un proceso que significa identificarse con el portador de determinados conocimientos que los pone en beneficio de la organización, trasladando su valor a la misma.

---

[16] Romero Cuevas y Ramón Salvador. (2005). Gestión del Conocimiento y del Capital Intelectual en una PYME del sector textil, p. 3
https://upcommons.upc.edu/e-prints/bitstream/2117/541/4/Gesti%C3%B3n%20del%20conocimiento%20y%20del%20capital%20intelectual%20en%20una%20PYME%20del%20sector%20textil.pdf

1.4.1 EL CONOCIMIENTO Y LAS ORGANIZACIONES

Las empresas ya sean públicas o privadas, se han convertido de manera dominante en fuertes depositarias y coordinadoras de conocimiento. La información y el conocimiento se están convirtiendo en el principal activo.

Según St-Onge, "Si los administradores, directores y gerentes administraran de manera diferente, adoptando un liderazgo que tome en cuenta la nueva situación, podrían aumentar el valor de la empresa. Calcular solo los bienes tangibles y basarse en la contabilidad tradicional para evaluar los resultados es como manejar mirando el retrovisor, manifiesta el experto". [17]

1.4.1.1 EL VALOR DE LAS ORGANIZACIONES

El valor de una organización, desde el punto de vista de los accionistas se puede definir como el valor monetario de las acciones de la empresa. Esta definición expresada en una ecuación seria:

Valor de Mercado = Número de Acciones x **Valor de Acción**

Para tomar en cuenta el valor del conocimiento en la valoración de la empresa, existen diferentes modelos, tales como Navigator de Skandia[18], Dow Chemical, entre otros. Estos modelos, presentan similitudes que pueden ser representadas a través del modelo utilizado por PriceWaterHouseCoopers (PWC), quien define el valor de las organizaciones de la siguiente manera:

Valor de Mercado = Activos Tangibles + Activos Intangibles

Donde:

---

[17] Muzard Joël. (2006). El Desarrollo del Capital Intelectual y la Administración de Conocimientos. http://www.a-i-a.com/DesarrolloCapitalIntelectual/index.html.

[18] Gestiondelconocimiento.com. (2006). Modelo Navigator de Skandia. http://www.gestiondelconocimiento.com/modelo_navigator_de_skandia.htm

Valor de Mercado: Número de acciones x Valor de cada acción.

Activos Tangibles: Son los activos medidos de acuerdo a los principios contables generalmente aceptados. Es decir, los especificados en los balances anuales(el Capital Contable).

Activos Intangibles: Todo aquel recurso asociado al Capital Intelectual.

1.4.2 EL CAPITAL INTELECTUAL

En opinión de Edwar E. Lawler, existen tres factores que pueden generar organizaciones de éxito, los cuales guardan relación con el aspecto humano de la empresa: el capital humano, las capacidades organizativas y las competencias críticas. Estas dos últimas dependen de la formación y del talento de los empleados, lo cual implica que la organización cuente con buenos sistemas de organización y estilos de dirección apropiados.

Consideremos algunas definiciones de Capital Intelectual, realizadas por algunos especialistas en el tema:

"Son los activos que son recursos no financieros de una Organización". [19]

"Esta compuesto por el Capital Humano y el Capital de Conocimiento. El Capital Humano comprende los talentos humanos individuales y el conocimiento adquirido a través de educación, entrenamiento experto y la cognición. El Capital de Conocimiento es el conocimiento documentado que está disponible en forma de artículos de investigación, reporte, libros, artículos, manuscritos, patentes y software". [20]

---

[19] Chatzkel Jay. (2005). Measuring and Valuing Intellectual Capital: From Knowledge Management To Knowledge Measurement. http://www.tlainc.com/articl10.htm

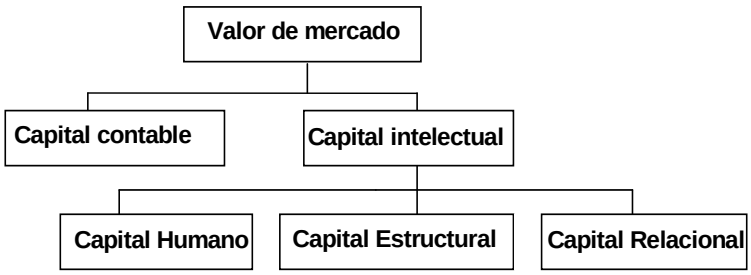
[20] Touraj Nasseri. (2006). Knowledge Leverage : The Ultimate Advantage. http://www.brint.com/papers/submit/nasseri.htm

"Es un sistema compuesto por tres elementos: El Capital Humano, el Capital del Cliente y el Capital Estructural". [21]

Esta última definición resume las ideas generales de las definiciones anteriores, por lo que podríamos decir: *Capital Intelectual* son los recursos no financieros que permiten generar respuestas a las necesidades de mercados y ayudan a explotarlas. Estos recursos se dividen en tres categorías: el Capital Humano, el Capital Estructural y el Capital Relacional.

A continuación se presenta el diagrama de descomposición basado en la anterior definición:

DIAGRAMA 1.1 CAPITAL INTELECTUAL



Fuente: Smith Peter A. (2006). Systemic Knowledge Management: Managing Organizational Assets For Competitive Advantage.

Donde:

a) Capital Humano: "Son las capacidades de los individuos en una organización que son requeridas para proporcionar soluciones a los clientes".

Dentro de esta categoría se encuentran las capacidades individuales y colectivas, el liderazgo, la experiencia, el conocimiento, las destrezas y las habilidades especiales de las personas participantes de la organización.

[21] Smith Peter A. (2006). Systemic Knowledge Management: Managing Organizational Assets For Competitive Advantage. http://www.tlainc.com/article8.htm

b) Capital Estructural: “Son las capacidades organizacionales necesarias para responder a los requerimientos de mercado”.

Dentro de esta categoría se encuentran las patentes, el know-how, los secretos de negocio en el diseño de productos y servicios, el conocimiento acumulado y su disponibilidad, los sistemas, las metodologías y la cultura propia de la organización.

c) Capital Relacional: “Es la profundidad (penetración), ancho (cobertura), y rentabilidad de los derechos organizacionales”. Dentro de esta categoría se encuentran las marcas, los consumidores, la lealtad, la reputación, los canales y los contratos especiales.

Esta descripción breve de la gestión del conocimiento, se lo ha realizado para resaltar la importancia que se debe brindar a la parte intangible de la organización en todo proceso de gestión organizacional.

1.5 RESPONSABILIDAD SOCIAL CORPORATIVA

“El concepto de La Responsabilidad Social Empresarial(RSE) viene a complementar procesos que se iniciaron con el Aseguramiento de la Calidad, la promoción del respeto al Medio Ambiente, el respeto a los derechos laborales, a la Higiene y la Seguridad en el ambiente de trabajo y en un sentido más amplio el respeto de los Derechos Humanos, agregándole dos valores fundamentales, el interés por el colectivo que esta relacionado con la empresa (Grupos de Interés o Stakeholders) y el desarrollo de la ética empresarial como modelo de gestión.”[22]

Diversas corrientes de pensamiento en la última década promueven una gestión empresarial más humanista, donde una de las propuestas es responsabilizar a los directivos de empresas de la adecuada gestión de los riesgos para garantizar su sostenibilidad y contribuir con ello al progreso de la sociedad. En este sentido se

[22] Pool Roberto J. (2006). La Responsabilidad Social Empresarial: El Reto del Siglo XXI, p.2. http://www.mes-d.net/grupcies/boletin/ArticuloII_Edic_33.pdf#search=%22responsabilidad %20social%20%20crisis%20empresarial%22

han desarrollado normas para alentar su cumplimiento. A continuación se detallan dos de ellas.

1.5.1 RESPONSABILIDAD SOCIAL Y LA NORMA SA 8000 [23]

En 1997 se aprobó la Norma SA 8000(Social Accountability) la cual ha sido acogida internacionalmente y cuyo objetivo es permitir que las empresas que se certifiquen en ella, garanticen a sus clientes que sus productos son elaborados bajo condiciones de trabajo humanitario.

Las condiciones desfavorables en las que los trabajadores de muchos países se desenvuelven en los procesos productivos, la ausencia de condiciones de seguridad y bienestar mínimos, han motivado el surgimiento de la Norma Internacional SA 8000, que certifica en Etica y Responsabilidad Social, lo cual supone que las organizaciones que así lo deseen o que sean exigidas por mercados internacionales para poder exportar, deben comprobar que en sus procesos productivos se ofrecen condiciones de bienestar y respeto a los derechos humanos, de libre asociación, de salarios justos y que no presenten ninguna forma de atropello ni discriminación.

Teniendo presente que el concepto de empresa ha evolucionado y que, hoy no se concibe solamente como una unidad de producción y rentabilidad económica, sino como un conglomerado humano que reproduce las características de la sociedad a la cual pertenece, ella tiene que asumir responsabilidades que van más allá de la búsqueda únicamente de la rentabilidad y ampliar su espectro a responsabilidades de orden social tanto con sus miembros como los de su entorno(stakeholders).

---

[23] Gallego Mery. (2003). SA 8000 - Social Accontability. pp. 1-5
http://redalyc.uaemex.mx/redalyc/pdf/215/21513205.pdf

1.5.2 RESPONSABILIDAD SOCIAL Y LA ISO 26000 [24]

La decisión de la Organización Internacional de Estándares (International Organization for Standarization - ISO), de implementar el proyecto de normalización global ISO 26000, en el campo de la Responsabilidad Social(RS), fue acordado mediante una votación a la propuesta New Work Item Proposal (NWIP) en enero del 2005. Esta propuesta preparado por el Consejo de Gestión Técnica (Technical Management Board - TMB), sugirió que el trabajo podría ser mejor conducido dentro de un Grupo de Trabajo (Working Group - WG) directamente bajo la responsabilidad del TMB, y con un liderazgo compartido entre un país en desarrollo (Brasil) con un país desarrollado (Suecia). En su elaboración están involucrados 43 países miembros de ISO (21 de ellos son naciones en vías de desarrollo). La idea de ISO 26000 es dar las pautas para una certificación global de lo que es la RSE.

La discusión de esta norma abarca una diversidad de temas tales como: respeto a los derechos humanos, a la diversidad cultural, al medio ambiente, condiciones socioeconómicas y calidad de vida según prioridad de trabajadores y comunidades locales, mecanismos de identificación de grupos de interés (stakeholders), procedimientos de participación, comunicación e información con los distintos stakeholders, informes públicos transparentes y desempeño auditable, y la promoción de alianzas entre la empresa privada, la sociedad civil y el Estado.

Una diferencia de ISO 26000 con otros estándares es que, no se expedirá ningún documento que acredite certificación, será un proceso voluntario, aunque sus impulsores confían en que esta norma se convierta en el nuevo estándar del mundo de los negocios y que, a la larga, el mercado exija que haya una certificación. Algunos críticos al concepto RSE, afirman que la empresa privada se sobrecarga de exigencias al instarla a lograr metas de responsabilidad social que

---

[24] Norma ISO 26000 Directrices sobre Responsabilidad Social, p.1-5. http://www.bcn.cl/carpeta_temas/carpeta_temas/temas_portada.2005-10-27.0843131984/pdf/ISO_26000.pdf/download

en primera instancia son tareas del Estado. Su argumento es que la RSE no puede ni debe ser considerada como un sustituto de políticas gubernamentales en ese sentido.

1.5.3 RESPONSABILIDAD SOCIAL EN TIEMPOS DE CRISIS [25]

En épocas de crisis, muchas empresas emprenden un proceso de decrecimiento para poder enfrentar las turbulencias del cambiante entorno y uno de los elementos más susceptibles frente a estos efectos es el personal. Así el capital humano que se ha incrementado con el tiempo comienza a reducirse y a descapitalizarse, siendo trasladado, en el mejor de los casos a empresas competidoras y la mayoría de las veces van a la desocupación o subempleo.
En este sentido algunas de las prácticas más frecuentes son: reducciones de jornada, suspensión de la jornada de trabajo, vacaciones colectivas, término del contrato de trabajo, no completar los cargos que resulten vacantes, recurrir a retiros indemnizados y jubilaciones pactadas.

Sin embargo, muchas organizaciones que valoran al Recurso (capacidad de hacer) Humano (capacidad de ser), han pensado en formas creativas frente a la necesidad de desvincularlos. Así, han surgido prácticas relativas a convertir parte de los ex-empleados en proveedores externos, especialmente cuando es preciso y necesario externalizar alguna actividad que habitualmente era propia, de esta manera los mismos empleados, con apoyo de la empresa, pueden formar una organización que proporcione suministros tanto para ella como para otros.

También se recurre a veces al trabajo a tiempo parcial, asumiendo una labor que no demanda una jornada laboral completa. Ello significa que podría trabajar algunas horas cada día de la semana, o trabajar continuamente algunos días o una combinación de estas modalidades, esto ocurre especialmente cuando las

---

[25] www.monografias.com. Pavisich Luis. Las Nuevas Herramientas de la Administración Moderna. http://www.monografias.com/trabajos16/administracion-moderna/administracion-moderna2.shtml.

empresas tienen períodos estacionales en su producción o ventas, pero también se aplica cuando ocurre algún fenómeno o actividad eventual.
En este contexto, existen empresas que utilizan prácticas de outplacement, las que apuntan a la readaptación y recolocación de empleados que están a punto de abandonar la organización.

1.5.3.1 OUTPLACEMENT

Consiste básicamente en preparar al trabajador sicológicamente y apoyarle en el desarrollo de nuevas habilidades, para enfrentar labores similares o actividades absolutamente diferentes a las que realiza actualmente.

No obstante, las prácticas de desvinculación elegidas están a su vez condicionadas por la percepción de los directivos de la magnitud, de la continuidad o discontinuidad de los cambios del entorno, de las características de los componentes humanos (edades, nivel y calificación), las características organizacionales (cultura, valores), visión y características del entorno global.

Algunos de los aspectos a considerar en la política de Outplacement son:

- Involucramiento total de la alta dirección.
- Establecer un consenso entre los actores organizacionales, para evitar un deterioro en el clima laboral y la productividad.
- Evitar la descapitalización de los recursos humanos, considerando el interés de la empresa.
- Apoyar con medios y nuevas herramientas para la reinserción de los trabajadores que deben abandonar la organización.
- De manera preferente, debe dirigirse el apoyo a los grupos con mayores dificultades en el mercado laboral.
- Hacerlo parte de las políticas de Recursos Humanos de la empresa.

A través de esta breve revisión del campo de estudio de la RSE hemos constatado que la tendencia es a exigir de las empresas una gestión mas humanista, y responsable de su sostenibilidad a través de la gestión de riesgos.

Un estudio más profundo del tema requiere de mucho más tiempo y bien puede constituir un tema de tesis, aquí únicamente se ha pretendido dejar constancia del avance en este campo que tiene relación con el objeto del presente trabajo.

1.6 EMPRESAS INNOVADORAS [26]

Estas organizaciones se caracterizan por contar como trabajadores a expertos profesionales por la complejidad de los trabajos que realizan. Además, cada cierto tiempo incorporan innovaciones a sus productos o se crean nuevos productos. Bennis y Slater denominan a este tipo de organizaciones “adhocracias”, mientras que Mintzberg “organizaciones innovadoras”.

Este tipo de organización tiene una estructura muy orgánica, poco formal y sus trabajos especializados están basados en la capacitación de los expertos. Generalmente se conforman equipos de personas para trabajar en un proyecto quienes se coordinan para combinar habilidades y experiencias para resolver problemas. La estructura que tiene sentido en este tipo de organizaciones es la estructura plana, para permitir que equipos multidiciplinarios combinen sus habilidades de una manera ágil y flexible.
Entre los aspectos que condicionan para que un proceso de mejora tenga éxito es contar con una estructura organizacional que lo viabilice.

1.6.1 TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN [27]

El término “Tecnologías de la Información y la Comunicación” (TIC) está relacionado con los aspectos del manejo, procesamiento y comunicación de información. El término “Tecnología de Información”(TI) es también utilizado para

---

[26] Mintzberg H., Quinn J. y J. Voyer. (2002). El Proceso Estratégico. México : Printice Hall. Primera edición. pp. 304-305,321-331

[27] Estrategia Empresarial. Las nuevas organizaciones empresariales en la Nueva Economía: La industria de la información en la Economía del Conocimiento http://publicaciones.estrategia.net/personas/report2.htm#arr

referirse a este aspecto. En la última década las economías desarrolladas se han caracterizado por la progresiva implantación de las Tecnologías de la Información y la Comunicación (TIC) en el conjunto de las actividades económicas, tanto de producción como de distribución y consumo.

Las TICs han transformado el diseño de los puestos de trabajo, el establecimiento de las relaciones jerárquicas y las relaciones entre los diferentes componentes de la actividad empresarial. La estructuración en red de estos componentes hace factible la configuración del conocimiento como elemento central de la organización y la estrategia, ya que las antiguas formas de coordinación, basadas en la jerarquía piramidal, resultan inviables. En la empresa red, la división del trabajo se fundamenta en la división del conocimiento, los puestos de trabajo se diseñan para que el factor humano sea parte activa de su actividad, con lo cual se transforman las relaciones jerárquicas, al situar la toma de decisiones en el lugar de trabajo.

La evolución de las diferentes concepciones de la organización empresarial se ha producido por el inicio y la consolidación de las TICs como elemento estratégico de la actividad económica. Sin embargo, se debe tener presente que una inversión en tecnologías digitales únicamente generará aumentos sostenidos en la productividad empresarial si se compagina con cambios organizativos y aumentos en la capacitación del personal, evidenciando con esto que las habilidades del factor trabajo y los activos intangibles son los elementos centrales de ese cambio.

1.6.2 EMPRESAS DE SERVICIOS [28]

Esta nueva era de los negocios se caracteriza por el hecho de que el sector de los servicios domina en cifras el empleo de mano de obra; la prosperidad de este

[28] Hoffman D., Bateson J. (2002) Fundamentos de Marketing de servicios. México : Printice Hall. pp. 3-20

sector se debe básicamente a los adelantos tecnológicos, los cambios demográficos y las presiones de la competencia.

Los servicios están por todas partes, trátese de una consulta médica, de una asesoría, de la educación o los servicios electrónicos. El imperativo de los servicios refleja la idea de que los aspectos intangibles del producto se convierten en las características fundamentales que distinguen a los productos en los mercados. Sin duda, los cambios de orden tecnológico, político y económico en conjunto, han contribuido a hacer del recurso intangible “capital humano” un elemento crucial para el éxito de las empresas de servicios.
En este nuevo escenario se ha visto la aparición de un creciente número de pequeñas empresas en el sector de servicios, que hacen uso intensivo del conocimiento para brindar servicios generalmente a empresas grandes. Dentro de este grupo están las nuevas empresas tecnológicas, las empresas de consultores y profesionales, los profesionales autónomos, entre otros.

El nuevo entorno de trabajo y de comunicación que se han desarrollado sobre la base de las tecnologías de información nos ha cambiado la forma de pensar y ver el mundo. Estos cambios y avances también imponen un cambio necesario al interior de las empresas para garantizar la disponibilidad de sus servicios de información, bajo la premisa de "no parar" dentro del concepto de continuidad del negocio.

Los temas tratados en la sección 1.6 tienen el objetivo de hacer notar, cuan importante es el diseño adecuado de la estructura organizacional de acuerdo a su línea de actividad económica, para llevar adelante un proceso de gestión con la colaboración y compromiso de todo el personal.
Siendo la empresa del caso práctico, una empresa de servicios del sector de las tecnologías de la información, son aspectos a considerar para llevar adelante un proceso de mejora.

CAPITULO 2

RIESGOS ORGANIZACIONALES

2.1 ADMINISTRACION DE RIESGOS

Toda empresa esta sujeta a diversos riesgos, tanto internos como externos que en forma directa o no, pueden afectar el adecuado cumplimiento de las metas y objetivos fijados, así como su supervivencia.

Antes de continuar, es preciso aclarar ciertas terminologías relacionadas con el tema, los cuales han sido tomados de diferentes fuentes del internet, referenciados en la bibliografía.[29]

Incidente: Suceso del que no se producen daños o estos no son significativos, pero que ponen de manifiesto la evidencia de riesgos derivados del trabajo.
Siniestro: Es todo evento repentino, no planeado, que pueda tener consecuencias negativas sobre el sistema.
Amenaza: Es la posibilidad de que un siniestro o una condición indeseada pueda ocurrir. También se utiliza el término peligro con el mismo significado. Puede decirse que amenaza es un riesgo no evaluado. La Amenaza es cualitativa: Por ejemplo cuando hablamos de un fuego como amenaza y no sabemos cuál es su probabilidad de ocurrencia ni su severidad (gravedad) esperada. La Amenaza no permite tomar ninguna decisión de Administración de Riesgos. Por lo tanto es necesario cuantificarla.
Probabilidad: Está determinada por la posibilidad de que ocurra un evento que pueda originar consecuencias negativas.
Riesgo: posibilidad de ocurrencia de toda aquella situación que pueda entorpecer el normal desarrollo de las funciones de la entidad y le impidan el logro de sus

[29] Albaladejo Juan Carlos. Que es la prevención de riesgos laborales: Objetivos y Definiciones, p.2,3 http://www.prevention-world.com

objetivos. Un riesgo que afecta las operaciones y las puede paralizar se define como "desastre".

Un desastre es "un evento que altera los procesos críticos de la organización que afectan su misión y degrada su servicio a un punto donde el impacto financiero y operacional se convierte en inaceptable" (Hiles, Barnes, 2002).

Riesgo absoluto: el máximo riesgo sin los efectos mitigantes de la administración del riesgo.

Riesgo residual: es el riesgo que queda cuando las técnicas de la administración del riesgo han sido aplicadas.

En la literatura encontramos que los términos “Administración de Riesgos” y “Gestión de Riesgos” son usados indistintamente para referirse al proceso de identificación, valoración y tratamiento de los riesgos en las organizaciones, por lo que para el objeto de nuestro estudio tendrán el mismo significado.

A continuación señalamos una definición bastante completa de Gestión de Riesgos:

“Es el término utilizado para describir al proceso lógico y sistemático de comunicación, establecimiento del contexto, identificación, análisis, evaluación, tratamiento y monitoreo de riesgos asociados con una actividad, función o proceso de tal manera que permita a las organizaciones minimizar las pérdidas y maximizar las oportunidades”.[30]

Existen varios enfoques y metodologías para la Administración de Riesgos, así mismo varias clasificaciones. [31]

Una de las clasificaciones parte del carácter de las consecuencias, se divide en dos grupos: *riesgos puros* y *riesgos especulativos*, los primeros provocan pérdidas; los especulativos podrían generar pérdida o ganancia.

---

[30] Civil Aviation Authority of New Zealand. (2006). Rule Development Process: Risk Management Methodology, p.3
https://www.caa.govt.nz/rules/Rule_Dev_Process/Risk_Management_Methodology.pdf

[31] Koprinarov Bratoy. 2005. El riesgo empresarial y su gestión
http://www.analitica.com/va/economia/opinion/5753437.asp

Otra clasificación se deriva de la estructura general de la empresa. Cada empresa contiene cuatro elementos principales: el personal, la tecnología, los materiales y el entorno. En cada uno existe un potencial de riesgos, los que se derivan en el ámbito del personal no son de la misma naturaleza que los del ámbito de la tecnología y por ende los efectos negativos no pueden minimizarse con los mismos métodos.

Desde la misma perspectiva se ha desarrollado una clasificación más detallada basada tanto en el criterio de la estructura como en el criterio de las principales funciones de una empresa. En este sentido, los riesgos son de carácter económico, de mercado, de crédito, de legalidad, de carácter tecnológico y operacional.
Los riesgos de carácter económico tienen que ver con la probabilidad de perder la ventaja competitiva, de empeoramiento de la situación financiera, de bajar el valor de su capital, etc. Los riesgos de mercado están relacionados con la inestabilidad de la coyuntura económica, con las pérdidas potenciales por cambios en los precios de los artículos de venta que produce la empresa, con problemas de liquidez, etc. El riesgo de crédito se produce normalmente cuando las contrapartes no cumplen sus obligaciones contractuales. El riesgo legal se presenta con la probabilidad de producirse pérdidas, porque las actividades de la empresa no están conformes con la legislación y la normativa vigentes o, porque la contraparte no tiene la autoridad legal para realizar una transacción, o porque en un negocio internacional aparece una incoherencia normativa de los países involucrados. Los riesgos de carácter tecnológico son los relacionados con la probabilidad de daños ambientales, averías, incendios, fallas de los equipos, etc. Finalmente, riesgo operacional es la probabilidad de perdidas por errores e ineficiencia de la organización interna.

Otra clasificación, centra su atención en la relación “objetivo/subjetivo” de los factores que producen los riesgos. Este enfoque destaca dos tipos de riesgos: inherentes e incorporados. Los primeros son los que emanan de la actividad propia de la empresa, estos deben minimizarse. El riesgo incorporado es producto de la inoperancia del personal, el cual debe disminuirse.

Considerando que los riesgos empresariales son principalmente decisiones, eventos o procesos, ejecutados u omitidos en situación de incertidumbre, que potencialmente y/o probablemente originan resultados en forma de pérdidas o de beneficios para la empresa, su gestión debe ser el conjunto de las actividades que persiguen el doble objetivo tanto de proteger la empresa y sus colaboradores como de explotar las oportunidades que le beneficien.

2.1.1 RIESGOS E INCERTIDUMBRE

El riesgo, definido en su forma mas general, es la probabilidad de que ocurran acontecimientos desfavorables. Así mismo, todo riesgo esta expuesto a dos factores: probabilidad e impacto. De esta manera los riesgos que tienen mayor prioridad a ser tratados son los que tienen un impacto y una probabilidad mayor.[32]

En este sentido dentro del proceso de evaluación es necesario determinar la probabilidad de ocurrencia realizando un análisis cualitativo o cuantitativo(valor numérico) y, el impacto en términos monetarios.

Tanto el riesgo como la incertidumbre es posible describirlos mediante distribuciones de probabilidad. “Para poder administrar el riesgo, necesitamos verlo. Para ver el riesgo nos valemos de distribuciones de probabilidad.”[33]
Para eventos repetibles y medibles, la probabilidad representa la frecuencia relativa de ocurrencia de un evento. Para eventos no repetibles o mensurables, la probabilidad es la expresión del grado de creencia que tiene un individuo acerca de la ocurrencia de un evento incierto, en este caso las probabilidades son subjetivas por naturaleza y es posible que dos personas asignen diferente probabilidad de ocurrencia a un mismo evento.

---

[32] Ivorra José. (2002). La gerencia de riesgos - factor crítico de éxito http://www.willydev.net/descargas/WillyDev_GerenciadeRiesgosFactorCriticodeExito.pdf p.5

[33] Bustamante Alejandro. UCEMA-MAG Evaluación de riesgo agropecuario: Simulación Montecarlo. http://www.cema.edu.ar/~alebus/riesgo/montecarlo.PPT

La evaluación del riesgo puede resultar muy compleja debida a la naturaleza de cada riesgo o por falta de información, lo cual va requerir de un análisis más profundo que amerita el uso de fórmulas, modelos y simulaciones matemáticas para determinar un valor de impacto y probabilidad confiables, lo que implica recurrir a especialistas en análisis de riesgos. Esto podría significar el consumo de mucho tiempo y dinero justificables únicamente cuando la incertidumbre es considerable y el impacto sea alto.

"Uno de los modelos más conocidos es, la simulación de Montecarlo es una técnica que combina conceptos estadísticos (muestreo aleatorio) con la capacidad que tienen los ordenadores para generar números pseudo-aleatorios y automatizar cálculos." [34]

Esta técnica tiene su origen en los 40, y está ligado al trabajo desarrollado por Stan Ulam y John Von Neumann, cuando investigaban el movimiento aleatorio de los neutrones. En años posteriores, la simulación de Montecarlo se ha venido aplicando a una infinidad de ámbitos como alternativa a los modelos matemáticos exactos ó como único medio de estimar soluciones para problemas complejos. Así, en la actualidad es posible encontrar modelos que hacen uso de simulación Montecarlo en las áreas informática, empresarial, económica, industrial e incluso social. En otras palabras, la simulación de Montecarlo está presente en todos aquellos ámbitos en los que el comportamiento aleatorio o probabilístico desempeña un papel fundamental.

Ahora, revisemos uno de los sectores de la industria donde mayormente se hace uso de técnicas y modelos para el análisis de riesgos, el Financiero. Regulaciones como el de Basilea II, al definir nuevos niveles de capital que respalden los riesgos a los que están expuestos, obligan a las entidades a llevar un mejor análisis y control de los riesgos de: mercado (asociado a las fluctuaciones en el precio de los activos), crediticio (asociado a la incertidumbre en el pago de las obligaciones de los deudores) y últimamente el operacional

[34] Faulín Javier. (2006). Simulación de Montecarlo con Excel http://www.abcbolsa.com/articulos_y_colaboradores.htm.

(asociado a la posibilidad de error humano, fallas tecnológicas, fraudes y desastres naturales).[35]

En este sentido se hace uso de varias técnicas y modelos para el análisis, por ejemplo para el riesgo de mercado, para estimar la distribución que permita calcular el valor de las pérdidas(VAR) ó la medida del riesgo alternativo(ES) que estima la pérdida promedio; los métodos más utilizados son el de varianza-covarianza (Markowitz), en él se asume que los rendimientos se distribuyen normalmente.

Otro método utilizado es el de Montecarlo, el cual consiste en construir en base a los datos históricos, un modelo factorial que sirve para generar nuevos datos que estime las pérdidas para distintos escenarios futuros. Con esto se infiere la distribución de las pérdidas y se estima el VAR y el ES.

El riesgo crediticio es una tema en el que aún hay mucho trabajo teórico y aplicado por hacer. El riesgo crediticio es el riesgo provocado por cambios inesperados en la calidad crediticia de los deudores o de quienes emiten deuda. Se estudian las pérdidas posibles debido a la quiebra de los deudores o a la disminución de la calidad de la deuda. El modelo más popular es el modelo KMV; fue desarrollado a inicios de la década de los noventa por la calificadora Moody y es una extensión del modelo de Merton para tomar en cuenta el comportamiento crediticio de los deudores.

El Comité de Basilea consideró siete tipos distintos de pérdidas operativas: fraude interno, fraude externo, prácticas internas, prácticas de los clientes, daño a los activos físicos, fallas en los sistemas y la administración de los procesos bancarios. Cómo evaluar y modelar las pérdidas para cada uno de estos rubros dará lugar a nuevas líneas de investigación. La falta de datos y la dependencia entre los factores de riesgo dificulta el manejo matemático de estos problemas

---

[35] Saavedra Patricia. (2005). Riesgo y los Acuerdos de Basilea II. http://laberintos.itam.mx/despliega.php?idart=21

con la metodología existente. Las pérdidas operativas, cuya frecuencia y monto son aleatorias, obligan a utilizar procesos del tipo de Poisson compuesto.

Concluimos esta sección manifestando que es preferible realizar una evaluación cuantitativa del riesgo cuando sea posible, de no serlo se hará una evaluación cualitativa. En todo caso, existen varios modelos y técnicas que se pueden utilizar en el análisis de riesgos dependiendo de su naturaleza.

2.1.2 PROCESO DE ADMINISTRACIÓN DE RIESGOS

No hay unanimidad de criterios entre los expertos en cuanto al proceso de la gestión de riesgos, sin embargo es posible identificar tres fases de carácter general: una fase de estudio; otra de carácter práctico, la fase de la implementación y la tercera, la fase de control y comunicación. [31]

La primera fase implica tres tipos de actividades: la identificación, el análisis y la evaluación de los riesgos. La identificación de los riesgos implica, primero, explorar el entorno interno y externo para verificar si hay señales de cambio en sus estructuras o en los procesos y tendencias que podrían exponer la empresa a riesgos; y segundo, establecer las amenazas y/o las oportunidades y determinar las probabilidades de su impacto sobre el funcionamiento y los objetivos.

Mediante el análisis se elabora el perfil de cada uno de los riesgos, después se examinan sus correlaciones y la frecuencia de su aparición. Es importante tener en cuenta que mientras el impacto de un solo evento podría ser mínimo, una secuencia de eventos puede amplificar su significación.

La evaluación esta orientada a medir el nivel de los probables daños y el costo de las medidas para evitarlos o disminuirlos; examinar las capacidades y los recursos de que dispone la empresa para afrontar los riesgos identificados, sistematizados

---

[31] Koprinarov Bratoy. 2005. El riesgo empresarial y su gestión. http://www.analitica.com/va/economia/opinion/5753437.asp

y evaluados; y diseñar el programa de la implementación de las acciones(estrategias) para afrontar las amenazas. Para poder especificar las prioridades en la respuesta a los riesgos y tipificar las amenazas como altas, medias o bajas, es de gran importancia evaluar los riesgos en su conjunto, con su jerarquía y sus correlaciones.

La segunda fase abarca la implantación de las acciones de respuesta a los riesgos, las mismas están dedicadas a ejercer influencia con el objeto de alcanzar parámetros que se alinean con las metas de la empresa y convertir de este modo en riesgos “aceptables”. En este sentido algunos expertos en el tema señalan cinco acciones principales: la transferencia, la reducción, la prevención, la aceptación y la diversificación de los riesgos.

La transferencia representa el conjunto de los procedimientos cuyo objetivo es eliminar el riesgo transfiriéndolo de un lugar a otro o de un grupo a otro, ya sea vendiendo el activo dudoso o asegurando la actividad con potencial de riesgo.
La reducción está orientada hacia la limitación de las posibilidades y de las graves consecuencias de un riesgo. En este caso se toman medidas para disminuir el tiempo de la exposición a riesgos.
La prevención es la actividad gerencial que trata de reducir el riesgo a través del rediseño del plan de la empresa.
La aceptación del riesgo o de una parte de éste es una decisión de aceptar la responsabilidad por las consecuencias probables de eventos, procesos y/o decisiones. En este caso la empresa tiene que cubrir las pérdidas con activos adicionales.
La diversificación de riesgos es una forma de intentar extenderlos de una sola área/activo a múltiples, con el fin de impedir la pérdida de todo. Generalmente una empresa realiza la diversificación de riesgos a través de la reducción de su dependencia de proveedores dudosos, o de la sumisión a un solo producto.

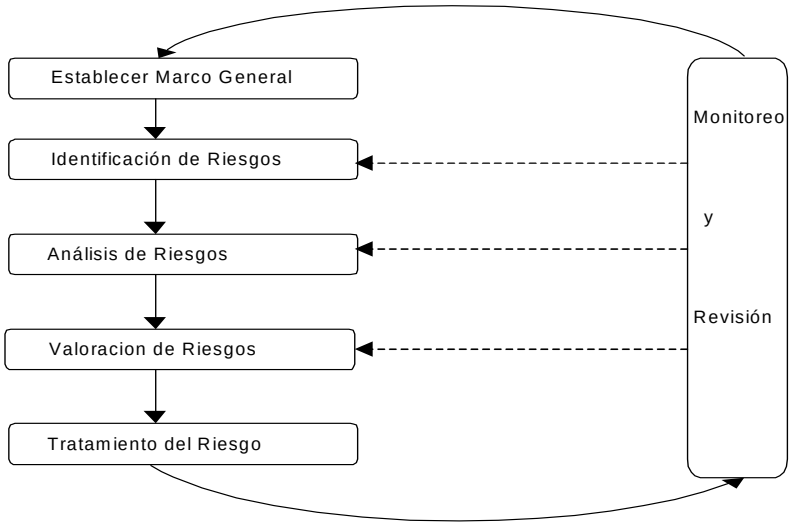
La tercera fase concede un papel principal a los procesos de monitoreo, control y comunicación. El monitoreo es fundamental para un buen funcionamiento de la gestión de riesgos, para llevarlo a cabo es menester diseñar e implantar un

sistema de mecanismos de medición y de seguimiento de las actividades expuestas a riesgos.

Como se ha manifestado, existen varias metodologías para la Gestión de Riesgos, a continuación se revisará una Guía de Administración del Riesgo[36] bastante completa, basado en el Modelo Estándar de Control Interno MECI 1000:2005 el cual se ajusta al marco propuesto por el Committee of Sponsoring Organizations of the Treadway Commission(COSO II).

Dado que la evaluación del riesgo es una parte importante del objeto del presente estudio se realiza una revisión detallada de la mencionada Guía. En este sentido en la Figura 2.1, presentamos una metodología genérica de gestión de riesgos la cual facilitará su análisis.

FIGURA 2.1 METODOLOGIA DE GESTION DE RIESGOS



Fuente: Latinamerica cacs, Presentación Administración de Riesgos, Fernando Izquierdo Duarte, p.7

[36] Guía Administración del Riesgo. Departamento Administrativo de la Función Pública República de Colombia, p.3-28
http://procesos.univalle.edu.co/MECI/Archivos/gu%25EDa_de_adm.riesgo-meci.pdf

Para una adecuada implementación de la Gestión del Riesgo se sugiere primeramente cumplir con las siguientes directrices: compromiso de la alta dirección, conformación de un equipo o comité de gestión del riesgo y la capacitación en la metodología. De igual manera la comunicación es el instrumento que posibilita la difusión de la información sobre las amenazas y los factores de riesgo a todos los miembros de la empresa, así se facilita la prevención y la toma de medidas, se mejora la coordinación a todos los niveles y se consolida la concienciación del personal.

A continuación, se analiza cada una de las fases de la metodología:

a) Establecer el marco general

- Establecer el Contexto Estratégico

  Hay que definir la relación entre la organización y el ambiente en el que opera. Para ello se determinan: aspectos financieros, operacionales, competitivos, políticos, imagen, sociales, clientes, culturales, tecnológicos y legales. De igual manera los grupos de interés relacionados con la organización: propietarios, personal, clientes, proveedores, comunidad local y sociedad.

- Establecer el Contexto Organizacional

  Entender la organización, sus capacidades y habilidades, conocer sus objetivos y estrategias. Por ejemplo, Objetivos del negocio: rentabilidad, crecimiento institucional, posicionamiento competitivo, imagen, servicio al cliente, productividad, calidad, recursos humanos, impacto en la comunidad.

- Identificar Objetos Críticos

  Entendiéndose por objeto, el área, proceso o actividad o cualquier otro elemento en que se pueda subdividir la organización y sobre el cual se pueda efectuar administración de riesgos. Definir los criterios bajo los cuales se pueda establecer la criticidad de un objeto respecto de otro. Por ejemplo, definir los criterios: Pérdida Financiera, Pérdida de Imagen, Incumplimiento de la misión, etc.

Este paso es importante para evaluar y priorizar los riesgos, posteriormente.

b) Identificación de Riesgos

Es la base del análisis de riesgos, se realiza a nivel del direccionamiento estratégico, identificando los factores internos o externos a la entidad y que pueden ocasionar riesgos. Es importante establecer las relaciones con otros riesgos, debido a que una causa puede generar uno o más riesgos y un riesgo puede ser generado por una o más causas. Se debe determinar que es lo que motiva, dispara o genera los eventos y los escenarios más significativos. Un dato importante es, expresar los riesgos en términos de consecuencia y considerar las causas que pueden generarlo. Así por ejemplo: Pérdida de confidencialidad debida a interceptación de la línea de comunicación.

Para que los empleados tengan conocimiento y visualicen los riesgos, es preciso contar con un formato de identificación de riesgos, como el de la Figura 2.2, el cual permite hacer un inventario de los mismos, definiendo en primera instancia las causas o factores de riesgo (internos y externos), los riesgos, una descripción de cada uno de ellos y finalmente definiendo los posibles efectos.

FIGURA 2.2 FORMATO DE IDENTIFICACION DE RIESGOS

PROCESO:				
OBJETIVO DEL PROCESO	**CAUSAS (factores internos y externos)**	**RIESGO**	**DESCRIPCION**	**EFECTOS (Consecuencias)**

Fuente: Guía de Administración del Riesgo, Departamento Administrativo de la Función Pública, República de Colombia, p. 16

Algunos autores sugieren que, durante el proceso de identificación de riesgos se realice una clasificación de los mismos en las diferentes categorías: Riesgos Estratégico, Riesgos Operativo, Riesgos Financieros, Riesgos de Cumplimiento, Riesgos de Tecnología, etc.

c) Análisis de Riesgos

En este proceso se busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de establecer el nivel de riesgo y las acciones que se van a implementar. Este análisis dependerá de la información obtenida en la identificación de riesgos y la disponibilidad de datos históricos y aportes de los empleados.

Se han establecido dos aspectos a tener en cuenta en el análisis de los riesgos: *Probabilidad* e *Impacto*. Por probabilidad se entiende la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de frecuencia, si se ha materializado, o de factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado. Por Impacto se entiende las consecuencias que puede ocasionar a la organización la materialización del riesgo. Otros aspectos a considerar son:
La Calificación del Riesgo: se obtiene a través de la estimación de la probabilidad y el impacto.
La Evaluación del Riesgo: permite comparar los resultados de su calificación, con los criterios definidos para establecer el grado de exposición de la entidad al riesgo.

Para facilitar la calificación y evaluación a los riesgos, se sugiere utilizar la Matriz de calificación, evaluación y respuesta a los riesgos (Figura 2.3), matriz que contempla un análisis cualitativo, que hace referencia a la utilización de formas descriptivas para presentar la magnitud de las consecuencias potenciales (impacto) y la posibilidad de ocurrencia (probabilidad). Tomando las siguientes categorías: leve, moderada y catastrófica en relación con el impacto y alta, media y baja respecto a la probabilidad.

Así mismo, presenta un análisis cuantitativo, que contempla valores numéricos que contribuyen en la calificación y evaluación de los riesgos. En este caso, tanto para el impacto como para la probabilidad se han determinado valores múltiplos de 5. La forma en la cual la probabilidad y el impacto son expresados y combinados en la matriz provee la evaluación del riesgo.

FIGURA 2.3 MATRIZ DE CALIFICACIÓN, EVALUACIÓN Y RESPUESTA A LOS RIESGOS

Probabilidad	Valor			
Alta	3	15 *Zona de riesgo moderado* Evitar el riesgo	30 *Zona de riesgo importante* Reducir el riesgo Evitar el riesgo Compartir o transferir	60 *Zona de riesgo inaceptable* Evitar el riesgo Reducir el riesgo Compartir o transferir
Media	2	10 *Zona de riesgo tolerable* Asumir el riesgo Reducir el riesgo	20 *Zona de riesgo moderado* Reducir el riesgo Evitar el riesgo Compartir o transferir	40 *Zona de riesgo importante* Reducir el riesgo Evitar el riesgo Compartir o transferir
Baja	1	5 *Zona de riesgo aceptable* Asumir el riesgo	10 *Zona de riesgo tolerable* Reducir el riesgo Compartir o transferir	20 *Zona de riesgo moderado* Reducir el riesgo Compartir o transferir
	Impacto	**Leve**	**Moderado**	**Catastrófica**
	Valor	**5**	**10**	**20**

Fuente: Guía de Administración del Riesgo, Departamento Administrativo de la Función Pública, República de Colombia, p. 18

En la matriz, si el riesgo se sitúa en cualquiera de las zonas: riesgo tolerable, moderado o importante, se debe tomar medidas para llevarlo a la zona aceptable o tolerable, de ser posible. Las medidas dependen de la celda en la cual se ubica el riesgo, así: los riesgos de Impacto leve y Probabilidad alta se previenen; los de Impacto moderado y Probabilidad leve, se reducen o se comparten; también es viable combinar estas medidas con evitar el riesgo, cuando éste presente una Probabilidad alta y media, y el Impacto sea moderado o catastrófico.

Cuando la Probabilidad del riesgo sea media y su Impacto leve, se debe realizar un análisis del costo beneficio con el que se pueda decidir entre reducir el riesgo, asumirlo o compartirlo. Cuando el riesgo tenga una Probabilidad baja e Impacto Catastrófico se debe tratar de compartir el riesgo. Siempre que el riesgo sea calificado con Impacto catastrófico la organización debe diseñar planes de contingencia, para protegerse en caso de su ocurrencia.

d) Valoración de Riesgos

La valoración del riesgo es el resultado de confrontar los resultados de la evaluación del riesgo con los controles existentes actualmente, con el objetivo de establecer prioridades para su manejo y fijación de políticas. Es necesario tener claro los controles existentes en los diferentes procesos, los cuales permiten obtener información para efectos de toma de decisiones.

Para realizar la valoración de los controles es necesario recordar que éstos se clasifican en:

- Preventivos: aquellos que actúan para eliminar las causas del riesgo, para prevenir su ocurrencia o materialización.
- Correctivos: aquellos que permiten el restablecimiento de las actividades después de ser detectado un evento no deseable; también permiten la modificación de las acciones que propiciaron su ocurrencia.

Para la evaluación de los controles es necesario determinar si son preventivos o correctivos y responder a las siguientes preguntas:

1. ¿Los controles están documentados?
2. ¿Se están aplicando en la actualidad?
3. ¿Es efectivo para minimizar el riesgo?

Con las respuestas se procede a realizar la valoración:

- Calificados y evaluados los riesgos hay que analizarlos frente a los controles existentes en cada riesgo.
- Ponderarlos según los criterios del Cuadro 2.1, teniendo en cuenta las respuestas a las preguntas anteriormente formuladas.

- Ubicar en la Matriz de calificación, evaluación y respuesta a los riesgos, el estado final, de acuerdo a los resultados obtenidos en la valoración del mismo.

CUADRO 2.1 CRITERIOS PARA LA VALORACIÓN DEL RIESGO

CRITERIOS	VALORACION
No Existen controles.	Se mantiene el resultado de la evaluación antes de controles.
Los controles existentes no son efectivos.	Se mantiene el resultado de la evaluación antes de controles.
Los controles existentes son efectivos pero no están documentados.	Cambia el resultado a una casilla inferior de la matriz de evaluación antes de controles (el desplazamiento depende de si el control afecta a al impacto o a la probabilidad).
Los controles existentes son efectivos y están documentados.	Pasa a escala inferior (el desplazamiento depende de si el control afecta al impacto o a la probabilidad).

Fuente: Guía de Administración del Riesgo, Departamento Administrativo de la Función Pública, República de Colombia, p.20

e) Tratamiento del Riesgo

- Identificar opciones de tratamiento

  Se determinan las posibles formas de reducir o mitigar el riesgo, para la actividad o componente al cual se aplicó el proceso de administración de riesgos. Se pueden aplicar los siguientes tratamientos:

  Evitar: Reduce la probabilidad de pérdida al mínimo al, dejar de ejercer la actividad o proceso. Un ejemplo de esto puede ser el control de calidad, manejo de los insumos, mantenimiento preventivo de los equipos, desarrollo tecnológico, etc.

  Reducir: Se consigue mediante la optimización de los procedimientos y la implementación de controles tendientes a disminuir la probabilidad de ocurrencia o el impacto.

  Transferir: Pasar el riesgo de un lugar a otro, compartirlo con otro, esta técnica no reduce la probabilidad ni el impacto, involucra a otro en la

responsabilidad. Un ejemplo seria, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar

Asumir: Se acepta la pérdida residual probable y las estrategias de prevención se vuelven esenciales.

- Evaluar opciones de tratamiento

  Bajo las consideraciones del marco de referencia definido, hay que establecer cual de las opciones de tratamiento identificadas se ajustan a la organización y reducen el riesgo a un nivel de exposición aceptable. La evaluación debe extenderse a los beneficios u oportunidades que la opción de tratamiento pueda generar. Se sugiere considerar los siguientes factores al momento de evaluar las opciones de tratamiento:

  Eficacia.- Efectividad de la propuesta de tratamiento para reducir el riesgo.

  Factibilidad.- La probabilidad de aceptar la opción propuesta.

  Eficiencia.- Uso óptimo de los recursos, costo/efectividad de la opción.

  Para seleccionar la opción más apropiada se requiere balancear el costo de implementación contra los beneficios derivados.

- Preparar planes de tratamiento

  Elaborar los planes que permitan poner en práctica las opciones de tratamiento del riesgo seleccionadas.

  Debe documentarse el cómo se implementarán las opciones elegidas, identificando responsabilidades, programas, resultados esperados, presupuesto, medición del desempeño y la revisión del proceso en su conjunto. El plan tiene que incluir un mecanismo para evaluar la implementación de las opciones contra criterios de desempeño y responsabilidades individuales, y para controlar hitos críticos de implementación.

- Implementar plan de tratamiento

  Lo ideal es que la responsabilidad para el tratamiento del riesgo sea ejercida por los mejor capacitados para controlar el riesgo. La implementación exitosa del plan requiere de un sistema efectivo de gestión que especifique: los métodos elegidos, la asignación de responsabilidades, las acciones individuales y controles.

e) Monitoreo

En cuanto a este proceso, en la Figura 2.1, el componente *Monitoreo y Revisión* interactúa con cada una de las fases del proceso de Gestión de Riesgos, y a través de él, el proceso se vuelve cíclico.

El monitoreo es esencial para asegurar que las acciones se están llevando a cabo y evaluar la eficiencia en su implementación, adelantando revisiones sobre la marcha para evidenciar todas aquellas situaciones o factores que pueden estar influyendo en la aplicación de las acciones preventivas. Esta tarea debe estar a cargo de los responsables de los procesos y del equipo o comité de gestión del riesgo, su finalidad principal será la de aplicar y sugerir los correctivos y ajustes necesarios para asegurar un efectivo manejo del riesgo, seguimiento y evaluación de resultados y propuestas de mejoramiento y tratamiento de las situaciones detectadas.

Entre los beneficios que la organización obtiene al realizar una gestión de riesgos se tiene:

- Facilita el logro de los objetivos de la organización.
- La organización es más consciente de sus riesgos.
- Mejoramiento continuo del Sistema de Control Interno.
- Optimiza la asignación de recursos.
- Aprovechamiento de oportunidades de negocio.
- Fortalece la cultura de autocontrol.
- Mayor estabilidad ante cambios del entorno.

2.1.3 REGULACIONES Y TENDENCIAS DE LA GESTIÓN DE RIESGOS

En los últimos años, han surgido una serie de requerimientos legales y regulatorios para varios sectores de la industria, exigiendo se desarrollen un sistema de gestión del riesgo y proporcionando cada vez más importancia a lo que es la continuidad del negocio.

Así tenemos: en el Reino Unido el "Tunrbull Report"[37], el cual exige a las empresas contar con un sistema de control interno que facilite la gestión de los riesgos del negocio para que puedan cotizarse en la bolsa de valores de Londres.

En la industria alimenticia, existe un requerimiento para realizar el análisis de riesgo, el cual es exigido por el denominado Hazardous Analysis Critical Control Point(HACCP) convertido recientemente en la ISO 22000[38].
En los EEUU aparece el llamado "Sarbanes Oxley Act"(SOX 404)[39], de manera similar exige que todas las empresas que se coticen en bolsa, tenga implementado un sistema de gestión de riesgos y controles para mitigarlos.

A nivel mundial, tenemos las regulaciones de Basilea II[39] con una serie de exigencias para el sector financiero relación al manejo del riesgo operativo. En este sentido, incentiva a los Bancos a adoptar un enfoque gerencial de administración de riesgos e impulsa una gestión que apunta a mejorar la solvencia del sistema financiero y a elevar los niveles de eficiencia. Esto incluye:

- La utilización de sistemas integrados de gestión de riesgos de crédito, de mercado y operacional.
- La utilización de indicadores que permiten la gestión diaria de riesgos.
- El compromiso de la alta dirección con la gestión de riesgos.
- Contar en la Institución con un Oficial de Gestión de Riesgos.

---

[37] portal.surrey.ac.uk . Key elements of the Turnbull Report
http://portal.surrey.ac.uk/pls/portal/url/ITEM/DA15127938014443E0340003BA296BDE

[38] www.brsltd.org. (2006). HACCP MS e ISO 22000. Requisitos Sistemas de Gestión en Seguridad Alimentaria, pp.1-4
www.brsltd.org/spanish_portal/certificacion_proceso/haccp_9001_spanish/ISO22000_PromoBrochurePages_es.pdf

[39] Ernst&Young. Evaluación del Riesgo empresarial. pp.1-5
http://www.ey.com/global/download.nsf/Uruguay/Boletin_Riesgo_Empresarial/$file/Boletines%20-%20riesgo%20empresarial.pdf#search=%22gestion%20riesgo%20empresarial%22

A través de la revisión del tema gestión de riesgos hemos constatado como el tema ha suscitado el interés en todos los sectores económicos. Anteriormente este estaba restringido únicamente a sectores regulados, pero en la actualidad por la complejidad de las organizaciones y los cambios constantes en su entorno ha motivado la revisión de su alcance y su aplicabilidad a todos los sectores productivos. Sin duda lo descrito en la presente sección(1.6), esta directamente relacionado y con el tema central del presente trabajo, por eso lo hemos tratado más detenidamente para tener una idea lo más clara posible.

2.2 CONTINUIDAD DEL NEGOCIO

"Continuidad de Negocio es el término generalmente usado para referirse al conjunto de acciones o estrategias que una organización establece para asegurar la disponibilidad de sus servicios en caso de que se produzca un grave incidente o una emergencia."[40]

La ausencia de una definición clara y universal de Continuidad de Negocio ha dado lugar a varias interpretaciones, para algunos expertos, Continuidad de Negocio es un sinónimo de Recuperación de Desastres. En la mayoría de las publicaciones especialmente las difundidas en Internet, se refieren a las actividades relacionadas con la recuperación de los sistemas de información en las organizaciones. Algunos autores se refieren a la Continuidad de Negocios en un contexto más amplio, en el que estaría incluido la Gestión de Crisis. Expertos como Hamilton Beazley, Jeremiaah Boenisch y David Harden, en su libro "Continuity Management" realizan el estudio de la Continuidad del Negocio con un enfoque en la "Preservación del Conocimiento Corporativo y la Productividad".

Luego del ataque al World Trade Center en Nueva York y otros acontecimientos más recientes a escala mundial, las compañías han incrementado su interés por tener planes de continuidad de negocios y recuperación en casos de desastre. Sin embargo, en los países subdesarrollados la posibilidad de que ocurra un desastre

---

[40] www.office-shadow.com. Qué es la Continuidad de Negocio
http://www.office-shadow.com/background-information/index.php

natural o un ataque terrorista que ocasione el cese de actividades aún se mira como algo lejano

Cualquier organización puede experimentar un incidente serio, lo cual puede impedir seguir operando normalmente. Las causas potenciales son muchas y variadas: un incendio, una inundación, una explosión, el escape de algún químico, el mal funcionamiento de la infraestructura tecnológica, algún accidente de trabajo, etc.

“Un entorno de operaciones ideal es aquel que está en capacidad de prever toda clase de interrupciones, conseguirlo es prácticamente imposible ya que dentro de los planes preventivos siempre existirán elementos que escaparán de las manos de quienes los diseñan. Sin embargo, toda organización moderna debe contar con un mínimo de respuestas oportunas y planes de contingencia que le permitan superar situaciones predecibles y mantenerse funcionando ante eventos potencialmente riesgosos”.[41]

Según John Sharp, CEO Bussines Continuity Institute(BCI), haciendo una analogía, “la norma 20/80 de la Continuidad del Negocio, establece que el 20% de las empresas sufren algún hecho de caso fortuito o fuerza mayor, ya sea inundaciones, incendio intencional o incluso terrorismo, de los cuales el 80% no se puede recuperar”.[42]

De manera general, las principales etapas de un programa de Continuidad de Negocio son:

- Clasificación de los distintos escenarios de desastres.
- Evaluación de impacto en el negocio.
- Desarrollo de una estrategia de recuperación.
- Implementación de la estrategia.

---

[41] Espiñeira, Sheldon y Asociados. Firma miembro de PricewaterhouseCoopers. (2006). Planificación de la continuidad de operaciones.
http://www.pc-news.com/detalle.asp?sid=&id=11&Ida=2428

[42] www.globalcrossing.com.(2006). Continuidad del Negocio
http://www.globalcrossing.com/espanol/xml/index.xml

- Documentación del plan de recuperación.
- Pruebas y mantenimiento del plan.

Como vemos este proceso es similar al de gestión de riesgos, sin embargo éste último se enfoca más en las acciones de prevención y mitigación, mientras que la continuidad del negocio generalmente concentra su atención en las acciones de recuperación.

En este contexto, analizaremos a continuación la Continuidad del Negocio bajo los enfoque: Sistemas de Información dada su amplia difusión y Preservación del Conocimiento, por ser un campo relativamente nuevo.

2.2.1 CONTINUIDAD DEL NEGOCIO Y LOS SISTEMAS DE INFORMACIÓN

En la era de la información su disponibilidad ininterrumpida es esencial, sin embargo, puede suceder un evento adverso repentino que afecte a los procesos claves del negocio. Así mismo, las presiones competitivas, las exigencias del mercado y un mayor grado de dependencia en la tecnología de los procesos centrales del negocio, están redefiniendo la necesidad de una planificación de continuidad basada en los riesgos.

Cualquier anomalía grave en los activos tecnológicos, puede interrumpir la operación del negocio, y hacerle perder ingresos y credibilidad frente a los usuarios y los clientes. “Hace poco tiempo, se consideraba un Plan de Continuidad, aquel que comprendía lo necesario para recuperar la operación de centros de cómputo”[43]. Actualmente, estas medidas son apenas una parte de los requerimientos de continuidad que se exigen para la mayoría de los centros de operaciones y procesos.

---

[43] Buezo Luis. (2004). ¿Garantizan las empresas la Continuidad de su Negocio? http://www.computing.es

A medida que las regulaciones de los gobiernos exigen mayor calidad de servicio, se hace imprescindible contar con un buen plan de continuidad del negocio, especialmente para aquellas instituciones que tienen alta dependencia tecnológica. En nuestro país, es un claro ejemplo, el caso de las operadoras de la telefonía celular, que al verse interrumpido la disponibilidad del servicio, provoca una reacción de los usuarios con un reclamo público, lo cual causa un daño a la imagen corporativa. En este sentido, la existencia de un plan adecuado es indispensable, pero no constituye una garantía; es necesario contar con toda una arquitectura orientada a la adaptación ante los cambios, una infraestructura física y de comunicaciones de alta redundancia, así como un modelo coordinado de hardware, software, organización y procesos que pueda operar virtualmente desde cualquier localidad.

La inversión para una adecuada Gestión de la Continuidad del Negocio(BCM sus siglas en inglés) muchas veces resulta ser muy alta, debido especialmente, a que la empresa no cuenta localmente con un líder o experto que conozca del tema, así puede darse el caso de que se requiera de un consultor externo o de un proveedor que proporcione un sitio alterno para el centro de cómputo, un centro de comando para el manejo de incidentes y hasta un lugar alterno donde realizar todas las operaciones críticas hasta que se restablezca el propio.

El beneficio de contar con un Plan de Continuidad del Negocio [44] (BCP sus siglas en inglés) en la empresa es, minimizar el costo de lo que tendrían que pagar y el menor tiempo de recuperación ante un desastre.

Algunos aspectos clave a tomar en cuenta son:

- Los planes de contingencia deberían ser parte de la política de la organización.
- El impacto y el análisis de riesgo ayudan a asegurar que sus disposiciones y planes son apropiados.

---

[44] Landaluce Gonzalo. (2005). Como estar preparado ante un desastre: Planificación de la continuidad de negocios.
http://www.borrmatt.es/redseguridad_anterior.php?id=565&numero=18#

- Sin datos de respaldo la recuperación de un negocio es imposible.
- Sin un plan de recuperación, la recuperación de un negocio es dudosa.
- Una manera de reducir los riesgos a la información de respaldo, es almacenándola fuera de sus propias instalaciones (off-site storage).
- Los cambios en las organizaciones ocurren todo el tiempo, es importante que su plan y disposiciones de continuidad reflejen estos.
- Como regla general, a más esfuerzo en el desarrollo del plan, más fácil será la recuperación.

Con base en la experiencia en el desarrollo e implementación de ese tipo de soluciones, "PWC ha estimado que el 60% de éxito de un Plan de Continuidad del Negocio reside en la eficiencia e idoneidad del personal responsable de su ejecución, un 35% en la infraestructura disponible, y solamente un 5% en la Calidad de los Planes desarrollados".[41]

En el campo de la Seguridad de la Información, existen algunos estándares y regulaciones internacionales relacionados con la continuidad:

- ISO 27000
- ISO17799
- BS7799
- COBIT AUDIT GUIDELINES
- ITIL
- SARBANES OXLEY ACT

De igual manera Certificaciones Internacionales, para los profesionales en esta área:

- CISSP
- CISA
- CISM
- CIA

---

[41] Espiñeira, Sheldon y Asociados. Firma miembro de PricewaterhouseCoopers. (2006). Planificación de la continuidad de operaciones.
http://www.pc-news.com/detalle.asp?sid=&id=11&Ida=2428

Un análisis detallado de cada uno esta fuera del alcance de la presente investigación, sólo se revisará brevemente la nueva Norma ISO 27000 en la siguiente sección.

2.2.1.1 CONTINUIDAD DEL NEGOCIO Y LAS NORMAS ISO 27000 [45]

La información es un activo vital para la continuidad y desarrollo de cualquier organización, pero la implantación de controles y procedimientos de seguridad se realiza frecuentemente sin un criterio común establecido, ante esto la International Organization for Standardization(ISO) decidió desarrollar la nueva serie ISO 27000, la cual es una familia de estándares internacionales para Sistemas de Gestión de la Seguridad de la Información (SGSI), que propone requerimientos de sistemas de gestión de seguridad, gestión de riesgo, métricas y medidas, guías de implantación, vocabulario y mejora continua.

La Norma ISO 17799 relacionada con la Seguridad de los Sistemas de Información, existe desde hace algún tiempo pero no es certificable. Esta norma es prácticamente igual a la primera parte de la norma británica(British Standarization) BS 7799, o sea la BS 7799-1 no certificable. Esta norma británica tiene una segunda parte certificable la BS 7799-2; la ISO 27001 esta basado en su mayor parte en esta última.

Encabezando la nueva serie se encuentra la Norma ISO 27001 la cual ya fue liberada. Esta norma muestra como aplicar los controles propuestos en la ISO 17799, estableciendo los requisitos para construir un Sistema de Gestión de Seguridad de la Información (SGSI), auditable y certificable. El estándar para la seguridad de la información ISO/IEC 27001 (Information technology - Security techniques - Information security management systems - Requirements) fue aprobado y publicado como estándar internacional en octubre del 2005 por la ISO y por la Comisión International Electrotechnical Commission(IEC).

Las demás normas de esta serie están en fase de desarrollo.

---

[45] www.iso27000.es. (2006). ISO 27000.
http://www.iso27000.es/certificacion.html

La ISO 27002 contendrá una guía de buenas prácticas que describe los objetivos de control y los controles recomendables en cuanto a seguridad de la información, esta norma no es certificable.
La ISO 27003 está en fase de desarrollo. Contendrá una guía de implementación de SGSI e información acerca del uso del modelo y de los requerimientos de sus diferentes fases. Tiene su origen en el anexo B de la norma BS7799-2.
La ISO 27004 Especificará las métricas y técnicas de medida aplicables para determinar la eficiencia y efectividad de la implantación de un SGSI y de los controles relacionados.
La ISO 27005 consistirá en una guía para la gestión del riesgo de la seguridad de la información y servirá de apoyo a la ISO 27001 y a la implantación de un SGSI.

Las normas ISO 27006-27009: están sin concretar aún su contenido. A pesar de ello, en ciertas publicaciones de Internet se hace mención a un modelo de normativa ISO, cuya denominación sería ISO/IEC 27006 "Guidelines for information and communications technology disaster recovery services", específicamente orientada a la continuidad y a la recuperación, proporcionando guías específicas para los servicios de recuperación ante desastres, bien sean propios o externos.

Entre los principales beneficios de la implementación de esta nueva serie de Normas ISO, se tiene:

- El establecimiento de una metodología de gestión de la seguridad de la información clara y bien estructurada.
- La reducción de riesgos de pérdida, robo o corrupción de la información.
- Los clientes tienen acceso a la información de manera segura, lo que se traduce en confianza.
- Los riesgos y sus respectivos controles son revisados constantemente.
- Las auditorías externas permiten identificar posibles debilidades del sistema.
- La continuidad en las operaciones del negocio tras incidentes de gravedad.
- La garantía del cumplimiento de las leyes y regulaciones establecidas en materia de gestión de información.

- Incrementa el nivel de concienciación del personal con respecto a los tópicos de seguridad informática.
- Provee la seguridad como una ventaja competitiva para las empresas que realizan operaciones de comercio electrónico.
- Aporta grandes beneficios para los bancos que requieren reducir riesgos operacionales, introducido por el Nuevo Acuerdo de Capitales Basilea II.
- Es consistente con regulaciones como la Ley Sarbanes-Oxley.

A continuación, se detalla una breve descripción para llevar adelante una iniciativa de certificación del ISO/IEC 27001 SGSI.

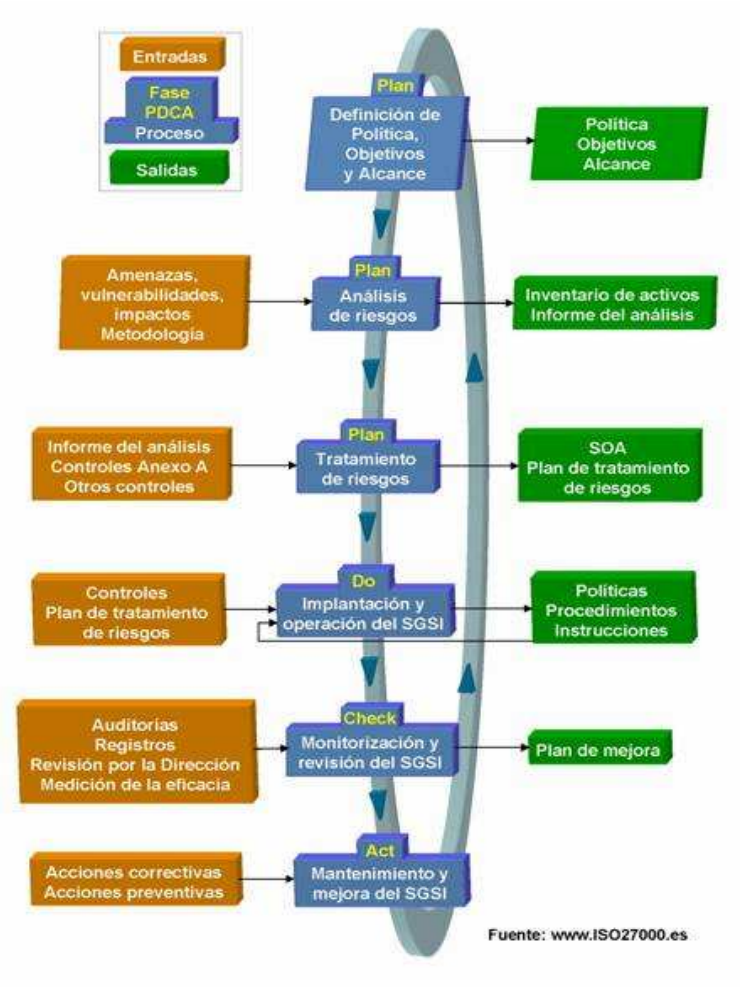
El paso previo a intentar la certificación es la implantación en la organización del sistema de gestión de seguridad de la información según ISO 27001. Este sistema, deberá tener un historial de funcionamiento demostrable de al menos tres meses antes de solicitar el proceso formal de auditoría para su primera certificación. La ISO 27001 exige que el SGSI contemple los siguientes puntos:

- Implicación de la Alta Dirección.
- Alcance del SGSI y política de seguridad.
- Inventario de todos los activos de información.
- Metodología de evaluación del riesgo(no establecido en la ISO).
- Identificación de amenazas, vulnerabilidades e impactos.
- Análisis y evaluación de riesgos.
- Selección de controles para el tratamiento de riesgos.
- Aprobación por parte de la dirección del riesgo residual.
- Declaración de aplicabilidad.
- Plan de tratamiento de riesgos.
- Implementación de controles, documentación de políticas, procedimientos e instrucciones de trabajo.
- Definición de un método de medida de la eficacia de los controles y puesta en marcha del mismo.
- Formación y concienciación en lo relativo a seguridad de la información a todo el personal.
- Monitoreo constante y registro de todas las incidencias.

- Evaluación periódica de riesgos y realización de auditorías internas.
- Mejora continua del SGSI.

El SGSI puede integrarse con otro tipo de sistemas (ISO 9001, ISO 14001). La propia norma ISO 27001 incluye en su anexo C una tabla de correspondencias de ISO 27001:2005 con ISO 9001:2000 e ISO 14001:2004 y sus semejanzas en la documentación necesaria, para facilitar la integración. Lo ideal seria llegar a un solo sistema de gestión y control de la actividad de la organización, que se pueda auditar en cada momento desde la perspectiva de la seguridad de la información, la calidad, el medio ambiente o cualquier otra.

FIGURA 2.4 PROCESO DE IMPLEMENTACIÓN DE LA ISO 27000



Fuente: www.ISO27000.es

La Figura 2.4 ilustra el proceso de implementación de la ISO 27000, en ella se observa que responde a la aplicación del ciclo Deming o modelo PDCA (Plan-Do-Check-Act) de mejora continua, también presente en otras normas.

La Gestión de Riesgos y de la Continuidad de Negocio son dos factores clave en cualquier implantación de un Sistema de Gestión de Seguridad de la Información(SGSI) para cumplir los mínimos requisitos, en conformidad con ISO 27001:2005.

2.2.2 CONTINUIDAD DEL NEGOCIO Y LA PRESERVACIÓN DEL CONOCIMIENTO [46]

Este es un enfoque nuevo en la gestión de la continuidad, su necesidad se ha hecho evidente en la era de la información en la que estamos inmersos, donde la diferenciación y ventaja competitiva esta basada en el capital intelectual.

Se habrán preguntado los directivos de las empresas:
¿Qué sucede si el empleado que realiza alguna actividad crítica en la empresa decide abandonar la empresa y el conocimiento acumulado que lleva en su mente no es transferido?
¿O si el empleado sufre algún accidente grave?
¿O si el empleado debe ser despedido?
¿O si el empleado simplemente se jubila?
Encuestas realizadas a empleados de las compañías dentro de la lista Fortune 100, han demostrado que un 25% están pensando en cambiarse de empleo dentro de un año. De igual manera muchas empresas tienen pensado realizar una reducción de su nómina para disminuir sus gastos operacionales. En este contexto, las consecuencias para las organizaciones son la pérdida del conocimiento. En muchas de las ocasiones el conocimiento que se pierde, puede resultar crítico para el normal funcionamiento de la organización. En la era de la

[46] Beazley H., Boenisch J y David Harden. (2002). Continuity management, New York: Jhon Wiley & Sons Inc. pp. 4-32

información en la que estamos inmersos, muchos de esos temores ya se han concretado.

Las empresas modernas, especialmente las que hacen uso intensivo del conocimiento tales como: la industria del software, las asesorías profesionales, investigación y desarrollo, entre otras, son las que sufren un mayor impacto, sin que esto necesariamente signifique que las demás están exentas.

Se ha realizado un análisis mas ampliado del valor del conocimiento para la organización, en el capitulo uno, aquí expondremos únicamente lo más relevante.

En la era del conocimiento los roles y responsabilidades de los cargos son continuamente redefinidos, el uso de la información es intensiva, la contratación de trabajadores emergentes(temporales) se ha incrementado, la alta movilidad de los trabajadores se ha evidenciado. El énfasis en la más alta calidad, mejora continua y aprendizaje organizacional, requieren acceso prioritario al conocimiento organizacional, incluyendo a las lecciones aprendidas de los éxitos y fracasos del pasado. El conocimiento es acumulativo. A menos que el conocimiento existente sea preservado el nuevo conocimiento no podrá ser construido, ya que debería redescubrirse con cada nuevo empleado.

El conocimiento ha llegado ha ser un activo de capital, que debe ser cuidadosamente adquirido, conscientemente preservado e inteligentemente invertido. El conocimiento no puede ser rastreado ni medido, está en la mente de los empleados, por lo tanto no puede ser apropiado por la organización, sólo tomarlo prestado, a menos que, la organización lo haya recolectado y almacenado para su futuro uso.

Así surge pues la necesidad, de una gestión de la continuidad del conocimiento(KCM sus siglas en inglés), el cual es definido como, la gestión eficiente y efectiva de la transferencia de conocimiento operacional crítico desde los empleados que son despedidos, transferidos o cesados a sus sucesores.

Componentes del conocimiento operacional:

Este conocimiento es multifacético en su contenido, comprensión y en su ámbito; está regado a través de la organización en las siguientes formas:

- *Conocimiento cognitivo*, contiene datos e información de una tarea y de sus fuentes.
- *Conocimiento de habilidades*, necesaria para un buen desempeño del trabajo.
- *Conocimiento del sistema*, comprensión de la relación causa-efecto es esencial para la toma de decisiones.
- *Conocimiento de la red social*, comprensión de la red social crucial que permite obtener cosas de la organización como: más información, consejos, etc.
- *Conocimiento de procesos y procedimientos*, formales o no.
- *Conocimiento heurístico*, son tips, atajos para cumplir tareas, realizar correcciones rápidas que constituyen las mejores prácticas.
- *Conocimiento cultural*, conocimiento de normas organizacionales, valores, roles y estándares de conducta que gobierna la interacción con los compañeros y los grupos de interés.

Existen cinco aspectos que hacen posible la identificación, captura y transferencia del conocimiento operacional, para propósitos de mantenimiento de la continuidad del conocimiento, estos son: contenido, contexto, formato, competencia y receptores.

- *Contenido*, el conocimiento operacional crítico no pierde su relevancia aun cuando el que lo posee deje la empresa. Este conocimiento será tan significativo para el sucesor como lo fue para el antecesor.
- *Contexto*, el empleado sucesor estará operando en el mismo contexto que el cesante. El conocimiento operacional creado en un contexto es más fácil transferirlo a un destinatario que lo utilizará en el mismo contexto.
- *Formato*, la información presentada al sucesor debe estar en un formato estructurado, conciso y relevante para su rápida comprensión.
- *Capacidades*, las capacidades del sucesor deben ser comparables a la del cesante, en cuanto a habilidades y capacidades profesionales.
- *Receptores*, Al definir el perfil del sucesor al mismo nivel que el antecesor, se reduce el problema de transferencia del conocimiento. El conocimiento

transferido debe ser validado por su par o sujeto a una revisión especifica por una persona autorizada.

Para capturar el conocimiento operacional crítico es posible recurrir a varias herramientas como: entrevistas, cuestionarios o una auditoría. Para llevar a cabo este proceso se debe elaborar un cuestionario específico para cada uno de los cargos. La información obtenida es necesario validarla con la ayuda de sus pares de la posición evaluada, de no existir se recurrirá a una contratación externa.
Según expertos en el tema, existen seis pasos para llevar a cabo una KCM:

- Dirigir una evaluación de la gestión del conocimiento para determinar el estado de la continuidad y discontinuidad del conocimiento en la organización.
- Determinar los objetivos y alcance de la iniciativa de KCM.
- Establecer responsables de la coordinación de la implementación de la KCM.
- Planificar la implementación de la iniciativa de KCM
- Crear la metodología para recoger y transferir el conocimiento operacional crítico.
- Transferir el conocimiento operacional.

Mientras que el proceso de evaluación de KCM, implica:

- Determinar la estadística de rotación anual por puesto de trabajo.
- Determinar la estadística de retiro o jubilación por puesto
- Determinar cual de los puestos debe ser parte de la gestión de la continuidad y en que grado.
- Determinar la amplitud o el grado de gestión de continuidad o discontinuidad entre el empleado saliente y el entrante por puesto.
- Generar una evaluación del daño por pérdida de conocimiento, haciendo uso de las estadísticas para estimar el daño a la productividad.
- Identificar áreas donde la gestión de continuidad puede ser enlazada a los sistemas de gestión de conocimiento.
- Evaluar el grado en que la cultura organizacional valora el conocimiento y la compartición del mismo.

Los principales beneficios de la KCM son:

- Facilita el proceso de trasferencia de conocimientos, y no implique un aumento de ansiedad y estrés para el sucesor.
- Incremento de la productividad debido al uso más efectivo del conocimiento operacional base y el uso más eficiente de su tiempo, el cual resulta del análisis del conocimiento llevado a cabo como parte de la gestión de continuidad.
- Preservación del conocimiento operacional a la salida de los subordinados y más efectiva transferencia de ese conocimiento a sus sucesores.
- Retención del conocimiento operacional cuando los colaboradores de confianza dejan el cargo, lo cual reduce el trabajo oculto y mejora la productividad del sucesor.

El tema de KCM como se mencionó anteriormente, es un nuevo enfoque dentro de la Continuad del Negocio, un análisis más profundo sale del alcance del objetivo de la presente investigación. Aquí se han dado las principales pautas para llevar a cabo esta gestión.

2.2.3 ANÁLISIS DE IMPACTO AL NEGOCIO

Mantener todo siempre disponible para actuar en caso de una emergencia, exige una alta inversión en infraestructura; por ello es necesario realizar un Análisis de Impacto al Negocio (BIA sus siglas en ingles), el cual incluye un estudio económico y operacional que muestra los riesgos potenciales que pueden afectar a la empresa.

Definición:" El Análisis de Impacto en el Negocio es un componente fundamental del plan de continuidad de una empresa, el cual incluye un componente exploratorio para revelar cualquier debilidad y un componente de planeación para desarrollar estrategias que permitan reducir el riesgo".[47]

---

[47] Miller Kevin. (2006). Business impact analysis. What is business impact analysis - a definition from Whatis_com.
http://searchstorage.techtarget.com/sDefinition/0,,sid5_gci820947,00.html

Existe un estudio de la consultora Gartner acerca de lo que se puede perder en una hora por carecer de un BCP o de una BCM. “En Estados Unidos, el costo promedio por una hora de sistema caído en cajeros automáticos es 14,500 dólares; en reservaciones de aerolíneas: 69,000 y en una compañía de corretaje: 6.5 millones de dólares”.[48]

Se supone que todo directivo de empresa conoce cuáles son las operaciones críticas de negocio; sin embargo pocos pueden decir cuánto puede perder en uno, dos o tres días si se caen esas operaciones, qué interdependencia hay entre esas operaciones y sobre otros procesos no tan obvios, y cómo la interrupción de las mismas afecta a sus clientes. Esas respuestas nos entregan un Análisis de Impacto del Negocio (Business Impact Analysis, BIA), y es lo primero que debe hacerse en la planeación de la continuidad del negocio.

Algunas preguntas que pueden ayudar a resolver el dilema son:

- ¿Cuánto perdería su negocio en una hora?
- ¿Cuánto tiempo esperara un cliente por su producto o servicio antes que se vaya a la competencia?
- ¿Qué multas o penalidades puede incurrir?

Las respuestas a estas preguntas permitirán formular las estrategias, así como decidir la inversión necesaria para implementarlas y llegar a un punto de equilibrio en donde el desembolso no sobrepase el riesgo de la pérdida.

Los procesos en la organización tienen diferente grado de criticidad, si bien son necesarios, no todos tienen las mismas repercusiones en las operaciones de la organización. En este sentido, una interrupción de la ejecución de uno u otro proceso, no causaría los mismos perjuicios, inclusive puede ocurrir que el impacto para un mismo proceso sea diferente dependiendo del tiempo en que ésta ocurra. El BIA debe establecer el grado de criticidad de dichos procesos basado en la

---

[48] Dora Price. (2006). Continuidad viva del negocio
http://www_tecnologiaempresarial_info
sitio alternativo: http://www.strohlsystems.com/

razón de ser de la organización y el tiempo máximo a partir del cual la interrupción es inaceptable.

El objetivo general del BIA es proporcionar a la dirección de la empresa, la información necesaria para que pueda tomar decisiones en el desarrollo de su estrategia de continuidad. [49]

Como objetivos específicos del BIA podemos mencionar:

- Definir los tipos de impacto que se deberían considerar, (económico, jurídico, comercial, operacional, de imagen, etc.).
- Identificar las funciones críticas de la organización y sus interdependencias.
- Identificar el impacto causado a la organización por la interrupción de cada una de las funciones.
- Definir cuáles son las funciones consideradas vitales y establecer los umbrales máximos de recuperación para cada una de dichas funciones.
- Identificar los recursos mínimos necesarios para una recuperación satisfactoria de las funciones identificadas como críticas.

Los impactos normalmente aumentan de forma acelerada dependiendo de los ciclos de proceso del negocio. Los ciclos más comunes son los siguientes:

- El mismo día (Día 0).
- El día siguiente (Día 1).
- Día 2.
- Días 3 – 7.
- Más de 7 días.

Los impactos más inmediatos son los económicos, tales como pérdida de ingresos por diferentes circunstancias. A menudo, los desastres ocasionan pérdida de activos no asegurados o imposibles de asegurar(pérdida de oportunidades, rotación de personal, responsabilidades legales, etc). Los impactos intangibles son también devastadores para una organización, como por

---

[49] Martínez Juan Gaspar. (2006). Análisis de impacto.
http://www.iee.es/opinion/tribuna.htm

ejemplo: mala imagen para la compañía, pérdida de la confianza de los inversores, consideraciones de tipo ético ante la sociedad.

A continuación se describe algunos de los impactos más comunes en función del tipo de negocio:[49]

a) Recuperación en el mismo día

El tipo de circunstancias e impactos que justificarían una respuesta en el mismo día podrían ser:

- Procesado de funciones financieras muy voluminosas y sensibles al tiempo, por ejemplo: transferencia electrónica de fondos, departamentos de pedidos telefónicos de gran volumen.
- Asuntos relacionados con la salud y la seguridad (servicios públicos).
- Impactos medioambientales (fugas o escapes de productos químicos).
- Las acciones cruciales de la gestión del incidente incluyen: comunicación interna y externa, coordinación y cooperación con las autoridades civiles y activación y coordinación de las actividades de soporte para la recuperación. La comunicación clara y rápida con los clientes es de gran importancia, de no ser así se tendrá reacciones negativas de parte de ellos.

b) 1-2 Días

La mayoría de los negocios pueden sobrevivir durante un día de interrupción. Sin embargo, luego de uno o dos días, empiezan a sentirse los impactos, como :

- El servicio a clientes comienza a deteriorarse sensiblemente (los clientes no pueden comunicarse con la compañía, los pedidos y los envíos comienzan a retrasarse).
- La información relativa a clientes necesita estar restaurada y disponible para satisfacer las necesidades de entregas y gestión de pedidos.
- Los impactos en ingresos comienzan a hacerse evidentes (pérdida de ventas como consecuencia del retraso de pedidos, impactos en el cash flow).

c) 3-7 Días

Este tipo de impactos incluye:

---

[49] Martínez Juan Gaspar. (2006). Análisis de impacto.
http://www.iee.es/opinion/tribuna.htm

- Notoriedad extremadamente alta, (por ejemplo, informaciones negativas en la prensa económica, impacto en la cotización de las acciones).
- Pérdida de clientes (a largo plazo y quizás permanentemente).
- Problemas contractuales graves (plazos incumplidos, cláusulas de penalización, pleitos).
- Amenaza financiera o quiebra.
- La capacidad para recuperarse resulta, a menudo, muy difícil con estos intervalos de tiempo.

d) Más de una semana

Las interrupciones largas generalmente son escasas.

- La reconstrucción de la información, cuando es posible, es enormemente costosa.
- La pérdida permanente de información, impacta sobre la competitividad a largo plazo, (por ejemplo, pérdida de información histórica, incremento en los gastos de litigios).
- La desmotivación y altas tasas de rotación del personal son frecuentes después de que ocurra una interrupción demasiado prolongada.

El tiempo es un factor importante en el proceso de recuperación por lo tanto, en el caso de sistemas de información hay que contar con planes de respaldo. En este sentido existen dos parámetros a tomar en cuenta: el Tiempo Objetivo de Recuperación (RTO) y el Punto Objetivo de Recuperación(RPO).[44] Estos parámetros son utilizados con mayor énfasis en la gestión de riesgos informáticos. Dado un recurso de nuestra organización, el RTO indica el tiempo que éste puede permanecer inhabilitado(interrumpido) sin que las consecuencias para el negocio sean críticas. El RPO en cambio, es el tiempo máximo que nos podemos remontar en el pasado con garantías de reconstruir desde él sus operaciones más importantes hasta el presente; ambas magnitudes se miden en tiempo. Además se manifiesta que el RPO coincide con la periodicidad que es aconsejable seguir

[44] Landaluce Gonzalo. (2005). Como estar preparado ante un desastre: Planificación de la continuidad de negocios.
http://www.borrmatt.es/redseguridad_anterior.php?id=565&numero=18#

para sus copias de seguridad. Los valores del RTO y RPO de un recurso pueden ir desde segundos hasta días y semanas.

De lo tratado en esta sección(2.2), podemos manifestar que al parecer el tema continuidad del negocio tuvo su origen en el área de la organización o sectores de la industria que tienen una alta dependencia en las tecnologías de la información, y en donde no se admite una interrupción que paralice la entrega del servicio. Ultimamente el tema ha evolucionado y su tendencia es a fomentar su aplicabilidad a todas las áreas de la organización y a organizaciones de todos los sectores. También se ha podido evidenciar la semejanza en su proceso de gestión a la gestión de riesgos, bien se podría afirmar que son complementarios, y por tanto directamente relacionado con el tema en estudio.

2.3 ESTADO DEL ARTE DE LA GESTIÓN DE CRISIS

En las secciones precedentes de este capítulo, hemos tratado los temas Gestión de Riesgos y Continuidad del Negocio. Del primer tema de manera general se ha manifestado que trata sobre las acciones tendientes a prevenir y responder a los riesgos a los que una organización se encuentra expuesta. En cambio el segundo tema, hace énfasis en las acciones tendientes a la recuperación del negocio luego de una interrupción. De igual manera hemos revisado las nuevas perspectivas y tendencias de la gestión de los riesgos en distintos campos del sector empresarial.

Lo desarrollado en la presente sección tratará sobre la evolución a un tratamiento integral de estos dos conceptos que se viene dando a nivel mundial, es decir aquel que engloba las acciones tendientes a prevenir, mitigar y restaurar el negocio ante un evento de crisis, procurando con esto, conseguir la continuidad organizacional.

Pese a ser un tema que ha despertado mucho interés últimamente especialmente en los Estados Unidos y Europa aun existe poca literatura en nuestro idioma, no hace mucho, sucedía lo mismo en las regiones mencionadas. La limitada

documentación en nuestro idioma, se enfoca exclusivamente a mantener la continuidad operativa de los procesos dependientes de las tecnologías de la información.

Varias Instituciones han contribuido al desarrollo del tema, este es el caso del Instituto de Continuidad del Negocio(BCI sus siglas en inglés), mediante el documento Business Continuity Management(BCM):Good Practices Guidelines, en el cual se afirma que, "BCM es un proceso de administración holística que identifica los potenciales impactos que amenazan la organización y una estructura para construir resiliencia y la capacidad de respuesta que resguarde los intereses de sus grupos de interés clave, la reputación, la marca y las actividades que crean valor."[50]

En los Estados Unidos el Disaster Recovery Institute Internacional(DRII), el equivalente del BCI del Reino Unido, apoyó la promoción de una base de conocimiento común para la industria respecto al tema planeación de continuidad del negocio, a través de la educación, asistencia y la publicación del recurso estándar base.

En la investigación The 2004 Deloitte Research Study[51], Prospering in the Secure Economy, se enfatiza en la responsabilidad y en el rol del sector privado en mantener una economía segura, mediante la adopción de planes que aseguren la Continuidad del Negocio(BC sus siglas en inglés).
Revistas especializadas en el tema Continuidad del Negocio, también enfatizan en la necesidad de un programa de continuidad organizacional integrado y en la administración centralizada en el nivel más elevado de una organización. Neil Kaufman y Jonathan King en su articulo, The case for a Business Continuity

---

[50] Gregory Shaw. (2004). The competencies required for executive level business Crisis and Continuity Managers. p. 4.
http://www.gwu.edu/~icdrm/publications/PDF/Dissertation_Shaw.pdf

[51] www.deloitte.com. The 2004 Deloitte Research Study
http://www.deloitte.com/dtt/cda/doc/content/DTT_DR_ProsSecExec_Sept2004.pdf

Officer, afirman: "La creación de una posición ejecutiva, tal como un Chief Continuity Officer(CCO), es necesaria para elevar la importancia estratégica de la continuidad del negocio y retomar el control de los procesos. Un programa de BC de clase mundial debería integrar la recuperación de la funcionalidad del negocio, la recuperación de desastres tecnológicos, las actividades de respuesta a emergencias locales y un plan de crisis del capital humano. Estos planes deberían estar integrados no sólo entre ellos sino también alineados a la estrategia y objetivos económicos de la organización. La gestión de BC llega a ser entonces, un importante proceso estratégico que cuando es implementado apropiadamente provee una ventaja competitiva sostenible a la firma (Kaufman, King 2003)". [50]
Todas las organizaciones sean éstas del sector público o privado, con fines de lucro o no, están en posibilidad de sufrir un evento destructivo que podría tener un rango de impacto, desde un mero inconveniente y desastre de corta duración, hasta inhabilitar la entrega de sus productos y/o servicios. Por consiguiente, las funciones organizacionales deben dar soporte a la prevención, la preparación, la respuesta y la recuperación del desastre del negocio, a través de acciones o estrategias tales como: administración del riesgo, planificación de contingencia, gestión de la continuidad, respuesta a emergencia, recuperación y reanudación del negocio. Individualmente estas funciones pueden contribuir a la protección de una organización y su línea de negocios, sin embargo, la eficiencia y efectividad demandan su integración y coordinación dentro de un programa global de gestión de crisis.

Mitroff en su libro “Managing Crises Before they Happen”, afirma “que la mayoría de organizaciones no han sido diseñadas para anticipar crisis o para administrarlas efectivamente una vez que ellas ocurren. Tampoco cuentan con los mecanismos y las habilidades básicas para una efectiva gestión. Esta afirmación, fue luego confirmada por la investigación Business Continuity Readiness Survey, conducida por Gartner Inc, y el Executive Programs and the Society for

---

[50] Shaw Gregory. (2004). The competencies required for executive level business Crisis and Continuity Managers, p.16-26
http://www.gwu.edu/~icdrm/publications/PDF/Dissertation_Shaw.pdf

Information Management, en la cual se determinó que menos del 25 % de las 2000 empresas globales, han invertido en un plan integral de continuidad." [50]
La tendencia en la aceptación de la continuidad organizacional esta cambiando, el crecimiento y dinamismo natural de los negocios, las amenazas tecnológicas y los inducidos por el hombre, la complejidad de los negocios, las regulaciones de los gobiernos, la expectativa de los medios y el público en general, demandan una estrategia global e integrada para la gestión de la continuidad organizacional.

Lamentablemente debido a la falta de incentivos y de estándares reconocidos, algunas empresas todavía lo consideran como un gasto oneroso y no como una inversión en la prevención y continuidad organizacional. Aún cuando la "Gestión de Crisis y Continuidad del Negocio" es reconocida como una función estratégica, sin embargo permanece como un programa discrecional.

2.3.1 ESTANDAR BS 25999 [52]

El Instituto Estándares Británico (British Standards Institution) está elaborando el estándar BS 25999, del cual su primera parte ya fue liberado, el BS 25999-1:2006, que es el código de prácticas que toma la forma de una guía y recomendaciones. Este establece los procesos, principios y terminologías de la gestión de continuidad del negocio(BCM) proveyendo una base para el entendimiento desarrollo e implementación de la continuidad del negocio dentro de la organización, además para proveer confidencialidad en el negocio B2B(negocio a negocio) y B2C(negocio-cliente).
Este pretende ser un punto de referencia sencillo para identificar un rango de controles necesarios para la mayoría de situaciones donde se ponga en práctica el BCM, en la industria y el comercio, a la vez usado por empresas de distintos tamaños y sectores. El BS 25999 contendrá dos partes:

---

[52] www.consultoras.org (2006). BS 25999-1 Code of Practice for Business Continuity Management Just Published.
http://www.consultoras.org/frontend/plantillaAEC/noticia.php?id_noticia=5791&PHPSESSID=964

BS 25999-1:2006 código de la práctica para la gestión de continuidad del negocio.
BS 25999-2:2007 Especificación para la gestión de continuidad del negocio, basado en el PAS 56:2003.
PAS 56:2003[53] es una guía publicada por British Standards Institution (BSI) en colaboración con el Business Continuity Institute (BCI) que establece el proceso fundamental, los principios y la terminología referente a la Gestión de Continuidad de Negocio, incluyendo una serie de buenas prácticas en lo relativo a anticipación a incidentes y respuesta a los mismos. Con la difusión de este estándar es de esperara que tenga mayor acogida en el sector empresarial.

2.3.2 MODELOS DE GESTIÓN DE CRISIS Y/O CONTINUIDAD DEL NEGOCIO

En general, en la literatura y prácticas de negocio actuales existe mucha inconsistencia en cuanto a la terminología utilizada para nombrar el enfoque holístico al tratamiento de riesgos organizacionales. Los términos, “Gestión de Crisis”, “Gestión de Continuidad del Negocio” o su combinación es lo que se viene utilizando.

Como se ha mencionado la limitada documentación existente respecto al tema continuidad organizacional, proviene de instituciones estatales y académicas líderes en el área de negocios, especialmente de los Estados Unidos y del Reino Unido, esto se refleja también en la existencia de pocos modelos reconocidos.
A continuación revisaremos algunos de ellos.

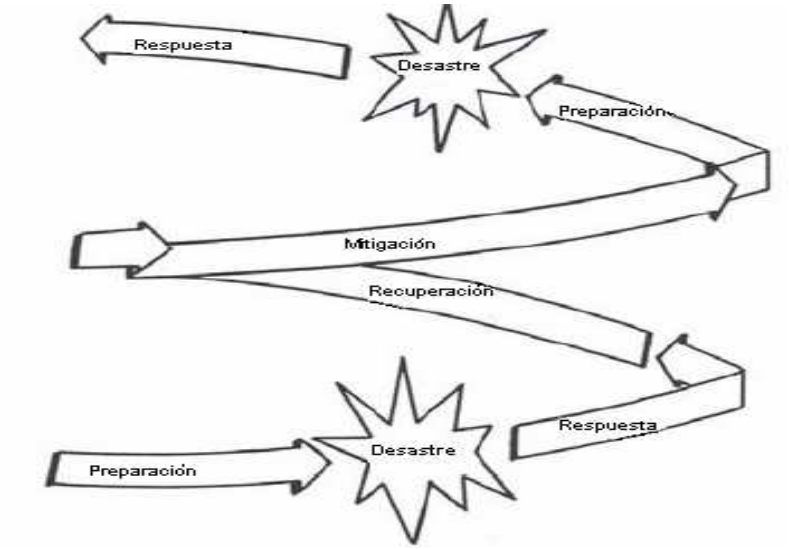
2.3.2.1 MODELO GLOBAL DE ADMINISTRACIÓN DE EMERGENCIAS

“Un primer acercamiento a un modelo lo hizo la Agencia Federal de Administración de Emergencias(Federal Emergency Management Agency) de los Estados Unidos, al representar algunas funciones que intervienen en una gestión

[53] Fernández José Manuel. (2006). BS 25999 Gestión de la Continuidad de Negocio. http://iso9001-iso27001-gestion.blogspot.com/2006/06/bs-25999-gestion-de-la-continuidad-de.html

de emergencia, (Figura 2.5) que ha servido de referencia para las entidades de gobierno. Para la continuidad organizacional es también un aporte valioso ya que nos permite visualizar el punto de inicio y algunas funciones que conforman un programa de continuidad organizacional. Sin embargo es un modelo limitado, ya que en su desarrollo no se concibió que sea para las organizaciones de negocio, sino para entidades de gobierno que prestan servicios de emergencia. **“**[50]

FIGURA 2.5 MODELO GLOBAL DE ADMINISTRACION DE EMERGENCIA



Fuente: Gregory Shaw. (2004). The competencies required for executive level business Crisis and Continuity Managers, p.27. Traducido por el Autor.

Para el autor del presente trabajo, un buen modelo sería aquel que en su representación gráfica exhiba todos los aspectos(humanos, tecnológicos, temporalidad, etc.) que influyen en un evento de crisis a la vez sea lo más sencillo posible para su comprensión y por tanto para su adopción. De igual manera es deseable que no sufra variaciones en el tiempo.

Lo destacable en este modelo, es la representación gráfica de las diferentes fases por las que atraviesa una gestión ante un evento de emergencia, que nos da una primera idea de las diferentes actividades que participan en una gestión de crisis.

No se exhibe en el modelo los aspectos que influyen en un evento adverso.

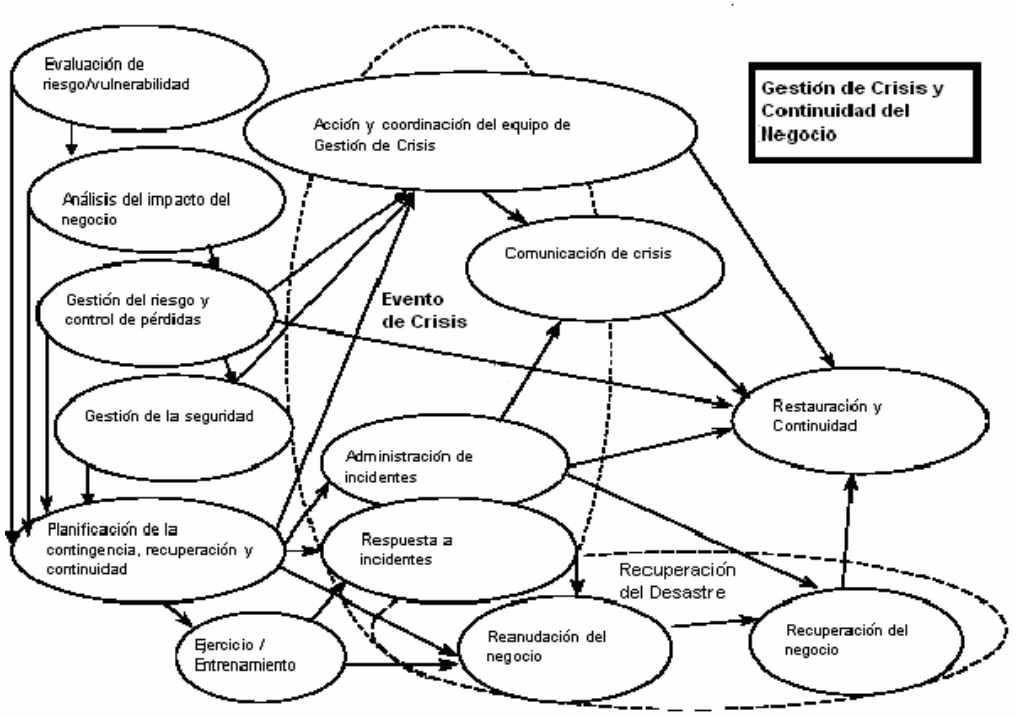
---

[50] Shaw Gregory. (2004). The competencies required for executive level business Crisis and Continuity Managers, p.27 http://www.gwu.edu/~icdrm/publications/PDF/Dissertation_Shaw.pdf.

2.3.2.2 MODELO GESTIÓN DE CRISIS Y CONTINUIDAD DEL NEGOCIO (JHON R. HARRALD)

"En 1998, Jhon R. Harrald hizo su aporte con el Framework of Crisis Management and Business Continuity (Figura 2.6). Este ha servido como el modelo unificado para la estructura del curso a nivel universitario del Federal Emergency Management Agency Higher Education Project University-level course "Business and Industry Crisis Management". También ha servido en el proceso de enseñanza en la Universidad George Washington para cursos a nivel de diplomado Crisis Management, Disaster Recovery and Organizational Continuity. "[50]

FIGURA 2.6 MODELO GESTIÓN DE CRISIS Y CONTINUIDAD DEL NEGOCIO



Fuente: Gregory Shaw. (2004). The competencies required for executive level business Crisis and Continuity Managers, p. 28. Traducido por el Autor.

[50] Shaw Gregory. (2004). The competencies required for executive level business Crisis and Continuity Managers. p.27
http://www.gwu.edu/~icdrm/publications/PDF/Dissertation_Shaw.pdf

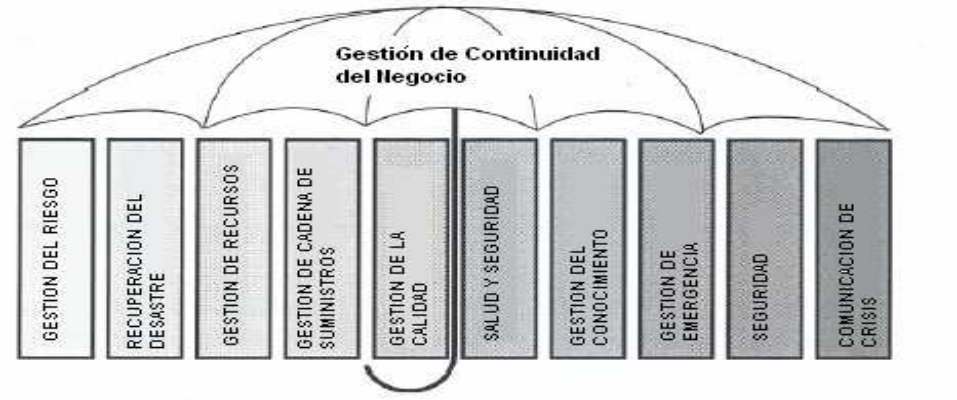
En opinión del autor del presente trabajo, del modelo se destaca su amplitud, pues abarca gran cantidad de funciones que participan en un programa de GC, sin embargo su representación gráfica es bastante compleja lo cual podría constituir un obstáculo para que las organizaciones lo adopten.

2.3.2.3 MODELO PARAGUAS DE CONTINUIDAD DEL NEGOCIO

"En el documento Business Continuity Management: Good Practices Guidelines (2002) se describe a la gestión de la continuidad organizacional como una actividad que unifica un amplio espectro de negocios y disciplinas administrativas. Provee un marco de referencia (en forma de paraguas) (Figura 2.7) para la revisión y rediseño de la manera como la organización provee sus productos y servicios mientras incrementando su resiliencia a la interrupción."[54]

En opinión del autor del presente trabajo, el modelo en su representación gráfica no expresa la temporalidad de las funciones, sin embargo su representación visual hace énfasis en la necesidad de un amplio programa de continuidad organizacional para la empresa.

FIGURA 2.7 MODELO PARAGUAS DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO



Fuente: Smith David. (2002). Business Continuity Institute, p.3. Traducido por el autor.

[54] Smith David. (2002). Business Continuity Institute. Business Continuity Management Good Practice Guidelines, p.3
http://www.auckland.ac.nz/security/images/BCIGPGIntroduction.pdf

Su representación gráfica es de fácil comprensión, en ella se representan las diferentes funciones que involucra un programa de continuidad organizacional, con el paso del tiempo se han ido incorporando otras funciones adicionales.
La desventaja es que no se visualiza las interacciones entre las distintas funciones y tampoco esta representado la temporalidad de un evento adverso.

2.3.2.4 MODELO DE CONTINUIDAD DEL NEGOCIO PROPUESTO POR EL CENTRO DE CONTINUIDAD

En el 2003, el Centro de Continuidad de Reino Unido propuso el modelo (Figura 2.8) con la siguiente explicación "Al no existir un modelo ampliamente aceptado que pueda ser usado para presentar el concepto de gestión de continuidad del negocio, de una manera tal que pueda ser suficientemente simple para permitir un rápido entendimiento a la gente nueva en la industria, sin embargo suficientemente extensivo para ser útil en otras áreas del proceso BCM, tal como la comunicación con el comité administrativo y los programas de cocientización y entrenamiento." [50]

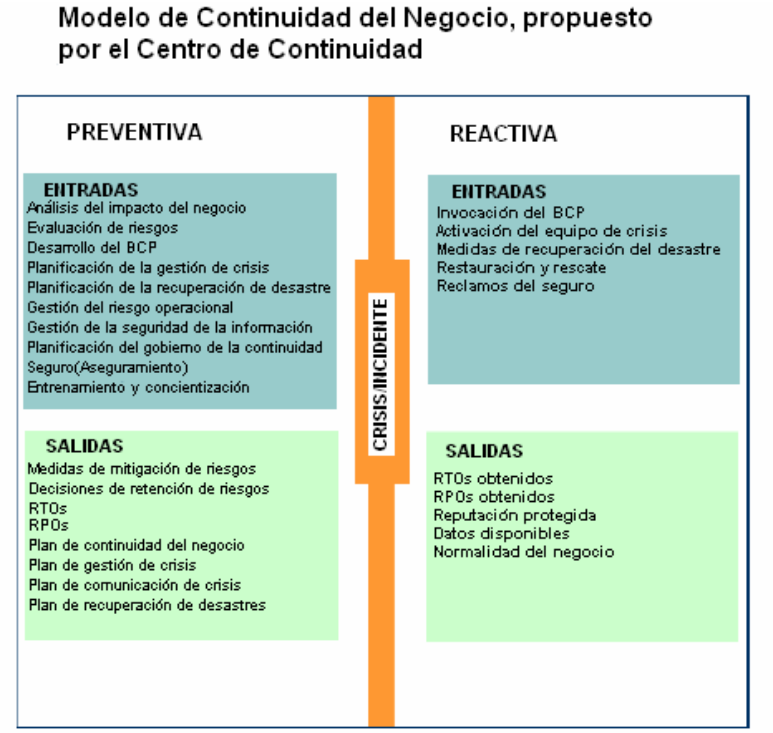
En opinión del autor del presente trabajo, éste es un modelo mucho más completo, en él se incluye un listado quelas funciones que deberían ejecutarse en cada una de las etapas principales(preventiva y reactiva), así como la definición de ciertos indicadores que miden la efectividad de los planes.

Sin embargo, en su representación gráfica no exhibe explícitamente las interrelaciones entre los diferentes planes. ya que como podemos observar únicamente se lista las funciones separadamente. De igual manera no se toma en cuenta a otros aspectos involucrados en un evento de crisis.

FIGURA 2.8

---

[50] Gregory Shaw. (2004). The competencies required for executive level business Crisis and Continuity Managers. http://www.gwu.edu, p. 30



Fuente: Gregory Shaw. (2004). The competencies required for executive level business Crisis and Continuity Managers, p.30. Traducido por el Autor.

2.3.2.5 MODELO DE CONTINUIDAD DEL NEGOCIO DE ASIS INTERNATIONAL

En el 2005, la ASIS[55] International, desarrollo el documento Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management and Disaster Recovery, en el cual se propone el siguiente modelo (Figura 2.9).

En el ASIS framework se enfatiza en la importancia central de la Prueba, Entrenamiento, Evaluación y Mantenimiento, los cuales están ligados completamente al modelo global de gestión de emergencias.

FIGURA 2.9 MODELO DE CONTINUIDAD DEL NEGOCIO DE ASIS INTERNATIONAL

---

[55] ASIS GDL BC. (2005). Business Continuity Guideline: A practical approach for emergency preparedness, crisis management and disaster recovery. http://www.asisonline.org

Fuente: ASIS GDL BC. (2005). Business Continuity Guideline, p.10. Traducido por el Autor.

En opinión del autor del presente trabajo, la ventaja de este modelo es que su representación gráfica refleja un proceso metodológico sencillo.
Su desventaja radica quizás en que no representa otros elementos relacionados y que intervienen en un evento adverso.

2.3.2.6 MODELO DE GESTIÓN DE CONTINUIDAD Y CRISIS DEL NEGOCIO (GREGORY SHAW)

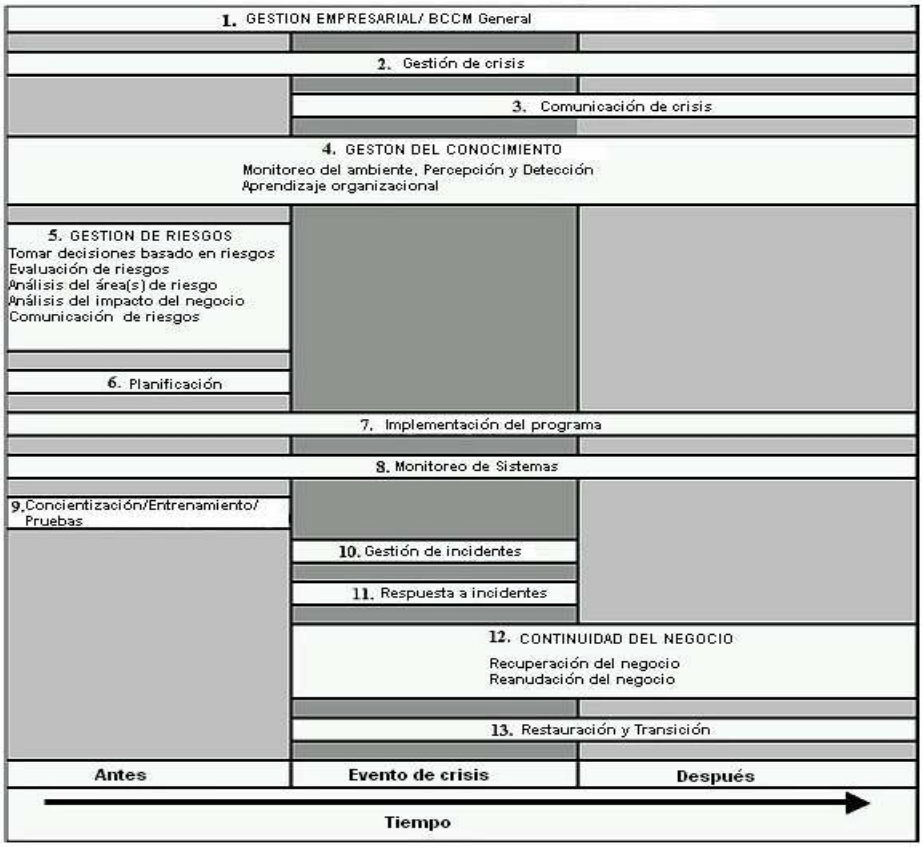
Al no existir un modelo de fácil entendimiento que permita visualizar de forma clara el ámbito de la temporalidad y de las funciones implicadas en la gestión de la continuidad organizacional, en el año 2004, luego de analizar los modelos anteriores, Gregory L. Shaw, de la Universidad George Washington propuso el Business Crisis and Continuity Management Framework [56] (Figura 2.10), según manifiesta, no pretende que sea un modelo común para todas las organizaciones, ya que su principal objetivo es facilitar la visión del ámbito que debe abarcar un programa global de continuidad y las funciones implicadas, debido a que muchas empresas no han implementado un programa de este tipo por falta de una comprensión total.

---

[56] Gregory Shaw. (2004). Crisis Management and Business Continuity, p.11
http://www.gwu.edu/~icdrm/publications/ShawTextbook011105.pdf

En el esquema que el propone, se expone los elementos involucrados en un sistema de gestión de crisis corporativa que asistirá en la integración de todas las funciones relacionadas con la gestión de crisis y continuidad organizacional. Su integración y coordinación puede ser facilitada a través de una responsabilidad y autoridad centralizada bajo la dirección de un ejecutivo de alto nivel.

FIGURA 2.10 MODELO DE GESTIÓN DE CRISIS Y CONTINUIDAD DEL NEGOCIO



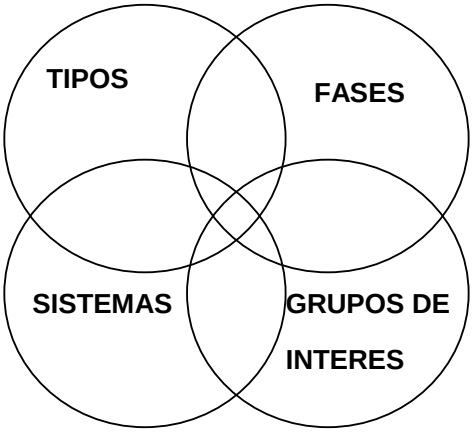
Fuente: Gregory Shaw. (2004). Crisis Management and Business Continuity, p.11.
Traducido por el Autor.

En opinión del autor del presente trabajo, sin duda es un modelo mucho más completo, su representación gráfica es de fácil comprensión, además incluye de manera explícita la temporalidad y las principales funciones que forman parte de un programa integral de continuidad organizacional.

2.3.2.7 MODELO DE GESTIÓN DE CRISIS (IAN MITROFF) [4]

El experto Ian Mitroff mediante un extenso estudio a situaciones de crisis inducidas por el hombre, ha determinado que hay cuatro factores principales críticos en sus causas así como también en su prevención, estos son: *Tipos de Crisis*, *Fases de las Crisis*, *Sistemas y Grupos de Interés* (Figura 2.11).

FIGURA 2.11 VARIABLES DE UN PROGRAMA INTEGRADO DE GESTION DE CRISIS



Fuente: Ian Mitroff. Cómo Gestionar una Crisis. p 30

La anterior figura representa las cuatro variables o factores que conforman un programa integrado de Gestión de Crisis(continuidad organizacional), en ella se representa las interacciones y superposiciones entre sí. Además, podemos deducir que cada tipo de crisis tiene que ser gestionado a lo largo del tiempo, debido a que el factor fases está presente en todas las crisis. De igual manera, los grupos de interés deben considerarse respecto a cómo pueden afectar o resultar afectados por la interacción de sistemas tecnológicos, humanos y organizacionales. En principio cada crisis lleva una mezcla de estos factores. En un programa de GC sistémico, es importante que los planes y procedimientos de crisis no se preparen aisladamente.

---

[4] Mitroff I. y C. Pearson. (2000). Cómo Gestionar una Crisis. Barcelona : Gestión 2000. pp.29-41

.

A continuación vamos a profundizar el estudio en el conocimiento de cada uno de estos factores identificados por Mitroff, lo cual nos facilitará la comprensión de su enfoque, considerando que la presente investigación tiene su base en lo que el experto propone.

a) Tipos de crisis

Los tipos de crisis potenciales son incontables, ninguna organización puede prepararse para todos. Sin embargo se puede dar tratamiento a un conjunto de *tipos* manejable. Existen tipos de crisis comunes a todas las organizaciones y otros que dependen de la naturaleza del negocio, para los cuales una organización se debe preparar.

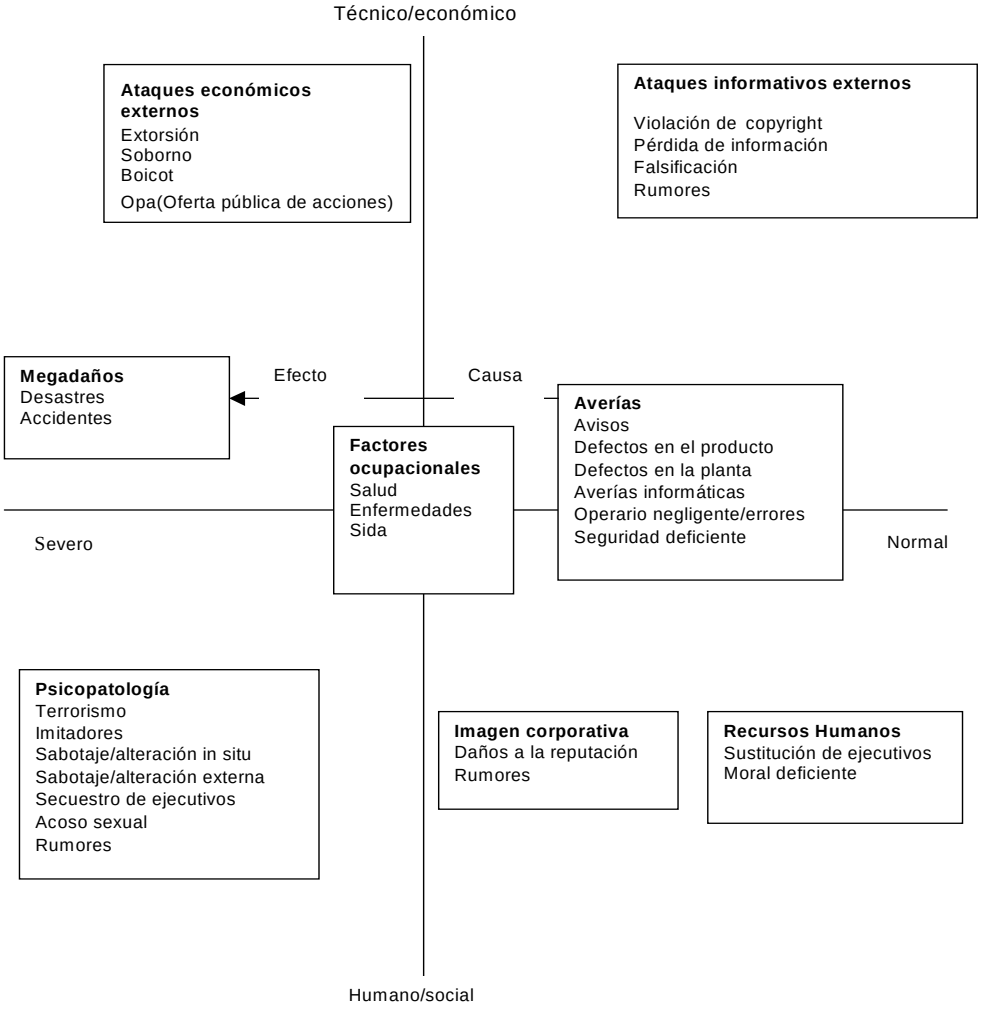
Fruto de un estudio realizado durante tres años y patrocinado por la National Association of Manufacturers – NAM, Mitroff y sus colaboradores obtuvieron una interpretación estadística de la naturaleza de las crisis. Adicionalmente Mitroff, desarrolló un conjunto de herramientas basado en los cuatro factores para llevar a cabo el diagnóstico y determinar el perfil de preparación de las organizaciones. ante crisis

La Figura 2.12, resume gráficamente los diferentes de tipos de crisis que pueden afectar a una organización, agrupadas en familias. En ella podemos apreciar la estructura esencial de las crisis, en la cual el eje vertical representa la diferenciación entre crisis que son vistas como esencialmente técnicas o económicas en su origen o aquellas que son esencialmente humanas o sociales. Mientras que el eje horizontal muestra la normalidad observada (sucesos cotidianos o normales) versus la anormalidad de una crisis.

La preparación para todas las familias de crisis resultaría costosa, sin embargo es posible prepararse al menos para una crisis de cada familia y por tanto tener un grado de protección, de ahí la importancia de un buen análisis de los riesgos (crisis potenciales) y el posible impacto en el negocio.

Las categorías genéricas de “familias” de crisis van desde las crisis técnicas y económicas a crisis humanas y sociales. Al interpretar los diferentes tipos de crisis es importante considerar estas familias ya que pueden ser aplicadas a cualquier organización o industria.

FIGURA 2.12 FAMILIAS DE CRISIS



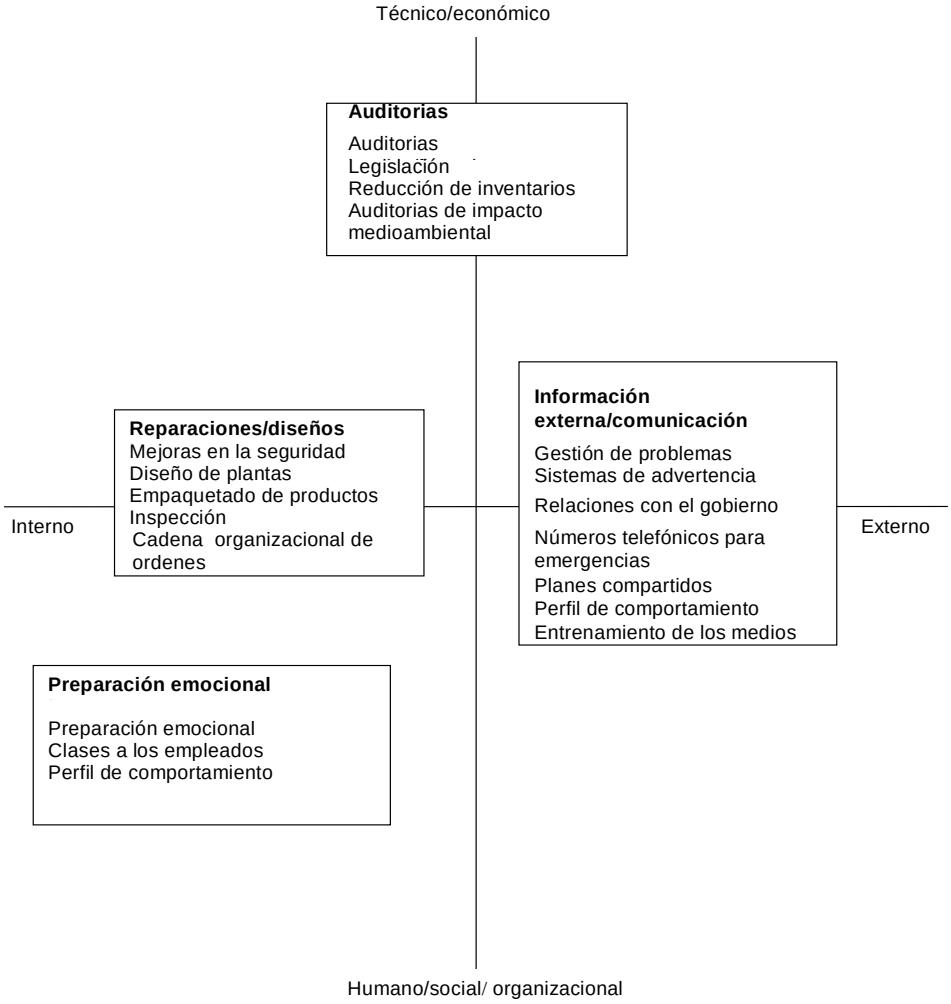
Fuente: Ian Mitroff. Cómo Gestionar una Crisis. p. 33.

Como complemento, la Figura 2.13 muestra las acciones preventivas, las cuales también tienden a agruparse en familias. La implementación de las acciones preventivas contribuyen a la reducción de la exposición de la organización.

De manera similar a la figura anterior, el eje vertical representa el origen de las acciones preventivas, sean éstas esencialmente técnicas o económicas o

aquellas que son humanas o sociales. Mientras que el eje horizontal determina las acciones preventivas que son consideradas internas y las que son externas.

FIGURA 2.13 FAMILIAS DE ACCIONES PREVENTIVAS



Fuente: Ian Mitroff. Cómo Gestionar una Crisis. p. 34.

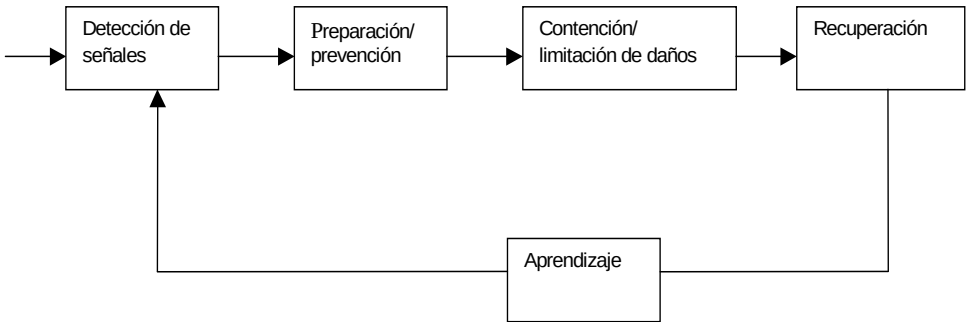
Es importante señalar que ningún ítem de las familias debe ser interpretado literalmente, así por ejemplo, la familia de crisis titulada Psicopatología, intenta interpretar la crisis concreta de alteración de un producto, la cual podría darse por la inyección de una sustancia extraña en productos alimenticios o farmacéuticos; otro ejemplo de la misma familia en el campo tecnológico, podría ser la alteración electrónica de la información; por lo que cada organización puede suponer que

una forma aplicable de alterar el producto puede darse dentro de su propio campo.

b) Fases de las crisis

La Figura 2.14 muestra las cinco fases por las que toda crisis pasa: detección de señales, preparación y prevención, contención de daños, recuperación y aprendizaje.

FIGURA 2.14. FASES DE LA GESTIÓN DE CRISIS



Fuente: Ian Mitroff. Cómo Gestionar una Crisis. p. 36

Detección de señales

Por lo general todas las crisis dejan un rastro de señales de detección temprana, la dificultad está en identificar las señales indicadoras de una crisis de las que no lo son, ya que una organización es bombardeada de todo tipo de señales. Las organizaciones preparadas evalúan constantemente sus estructuras operativas y de gestión, mientras que, las que son propensas a la crisis tiende a olvidar o incluso a ignorar las señales que indican un punto débil potencial en operaciones y estructura.

Preparación/prevención

La prevención de todas las crisis no es posible, pero se debe pensar en mecanismos que permitan tratar de impedirlas para gestionar adecuadamente las que ocurran, esto implica realizar sondeos cuidadosos y continuos de operaciones y estructuras de gestión de desastres potenciales.

Contención/limitación de daños

La finalidad de la contención de daños es detener los efectos de una crisis, por ejemplo evitando que afecte partes no contaminadas de una organización o entorno. No es recomendable improvisar los mecanismos y actividades de contención en el momento que ocurre la crisis.

Recuperación

Las organizaciones preparadas para las crisis tienen implementado programas de reanudación de la actividad a largo y corto plazo, esto incluye la identificación de los procedimientos y servicios básicos para una operación mínima del negocio así como la asignación de responsabilidades para la reanudación.

Aprendizaje

El aprendizaje implica reflexionar sobre las lecciones críticas que pueden obtenerse de las experiencias propias de la organización y de las experiencias de otras organizaciones. Las que están preparadas para la crisis, evalúan los factores que les permitieron actuar bien y aquellos que no, además hacen énfasis en mejorar sus capacidades de gestión de crisis futuras.

c) Sistemas de crisis

Actualmente la mayoría de las organizaciones generalmente centran su atención en las causas tecnológicas de una crisis y tienden a prestar poca atención a factores humanos y organizacionales (infraestructura o cultura).

La Gestión de Crisis(GC) efectiva requiere una infraestructura organizacional apropiada, incluyendo canales abiertos y efectivos de comunicación entre los diversos niveles y divisiones de la organización. Las actividades requeridas en este campo, deben integrarse con las actividades y las responsabilidades de cada empleado.

Existen algunas justificaciones equivocadas que se usan para bloquear los esfuerzos emprendidos en la organización respecto a la gestión de crisis, Mitroff

lo llana racionalizaciones. A continuación presentamos un listado de algunas de ellas que obstaculizan la gestión de crisis:

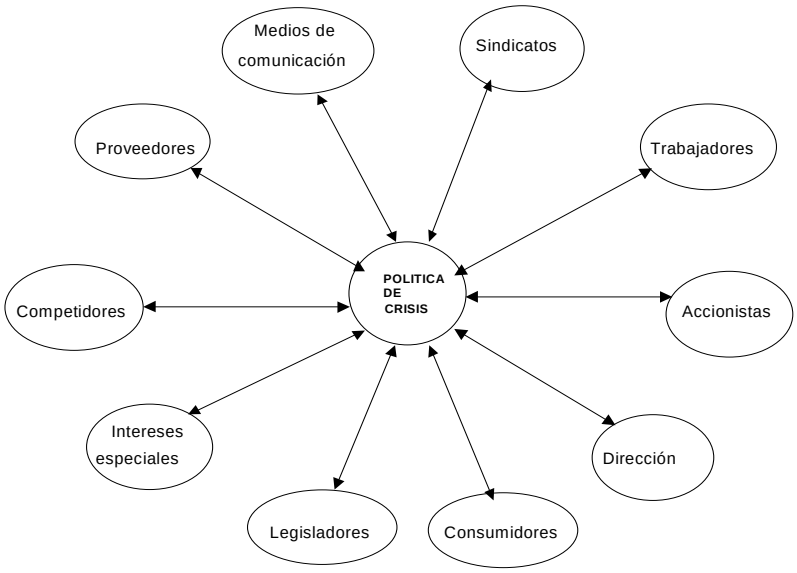
- Nuestro tamaño nos protegerá.
- Las compañías excelentes y bien administradas no sufren crisis.
- Los empleados que traen malas noticias merecen ser castigados.
- La gestión o prevención de crisis es un lujo
- Los objetivos del negocio justifican el uso de medios de alto riesgo.
- Nuestra especial ubicación nos protegerá
- Si alguna crisis ocurre alguien nos rescatará
- El medio ambiente es benigno(podemos protegernos nosotros mismos)
- Los accidentes son simplemente un coste de hacer negocios.
- La mayoría de las crisis se resuelven solas, por lo tanto el tiempo es nuestro mejor aliado.
- Basta con reaccionar a una crisis cuando se haya producido.
- Somos un equipo que funcionará bien durante la crisis
- Solo los altos ejecutivos necesitan estar enterados de nuestros planes de crisis ¿Por qué asustar a nuestros empleados o a la población?.
- Sabemos como manipular a los medios de comunicación.

Todas estas aseveraciones influyen para que la organización goce de excesiva confianza y no emprenda una planificación seria de GC.

d) Grupos de interés de la crisis(Stakeholders)

Los grupos de interés lo conforman: miembros internos(trabajadores, alta dirección), y aquellos grupos externos que pueden afectar a las capacidades de la crisis(proveedores, clientes, competidores, medios de comunicación), como lo muestra la Figura 2.15. Los grupos de interés pueden hacer que una crisis importante tenga mas o menos probabilidades de suceder.

FIGURA 2.15 GRUPOS DE INTERÉS ORGANIZACIONALES FUNCIONALES



Fuente: Ian Mitroff. Cómo Gestionar una Crisis. p. 40

La Política de crisis no es más que el reconocimiento de todos aquellos grupos de interés relacionados con la organización y que estarían involucrados(afectados), cuando una situación de crisis se presente. Así tenemos por ejemplo en el caso de una crisis de insolvencia, los grupos afectados entre otros serían: los empleados(se verían afectados por el pago retrasado de sus sueldos), los proveedores(al no recuperar oportunamente los valores por ventas a crédito), el gobierno(al no disponer de los valores correspondientes al pago de impuestos de la compañía), los organismos de crédito(por la dificultad de recuperar los valores prestados).

En resumen, en las páginas anteriores se ha descrito brevemente varios modelos, los cuales son aportaciones de instituciones estatales(EEUU y Gran Bretaña principalmente) y de algunos catedráticos y expertos. En general, hemos visto cierta evolución respecto al tema y su afán por representar de mejor manera un modelo que sea de fácil comprensión para ser adoptado por quienes deseen elaborar e implementar un programa de continuidad organizacional.

Existen ciertas coincidencias así como también diferencias entre ellos, de los cuales podemos citar que, en algunos no es visible la temporalidad por la que atraviesa un evento de crisis, en otras no se da un tratamiento sistémico. En lo

que se refiere a la representación gráfica de algunas no es de fácil comprensión o no refleja todo lo que representa un proceso de continuidad organizacional.

Dentro de las coincidencias, podemos destacar los modelos de Shaw y el de Mitroff, específicamente en lo que respecta a la temporalidad de la crisis, Shaw lo representa mediante las etapas Antes, Durante y Después; mientras que Mitroff lo hace mediante las Fases: detección de señales, prevención, contención, recuperación y aprendizaje.

Dentro de las diferencias, podríamos decir que, Mitroff no da nombres a las funciones que intervienen en un programa de continuidad organizacional, lo cual constituye una de las principales diferencias comparado con otros modelos, ya que éstos por lo general dan nombres tales como: plan de gestión de riesgos, plan de comunicación de crisis, plan de continuidad del negocio, plan de emergencias etc; Mitroff, hace énfasis en la definición de estrategias o acciones necesarias para cada una de las fases por las cuales atraviesa un evento de crisis, sin dar nombres concretos, con ello hace viable una visión integral de la GC y evita el tratamiento parcial, por tal motivo, su modelo se ha tomado como punto de partida para elaborar la propuesta de la tesis.

2.3.3 MODELO DE GC PROPUESTO POR EL AUTOR

En las secciones precedentes se han expuesto algunos modelos de continuidad organizacional, en la mayoría de ellos lo que primordialmente se destaca son las diferentes funciones que están involucradas en un proceso de gestión integral de continuidad, habiendo cierta coincidencia. De igual manera, en sus representaciones gráficas se refleja en cierta forma la temporalidad de un evento de crisis.

Otro aspecto que destaca en algunos modelos, es el hecho de que se utiliza nombres específicos para referirse a las funciones que intervienen en la Gestión de Crisis (continuidad organizacional), así tenemos por ejemplo en el modelo Paraguas: la Gestión del Riesgo, Gestión de la Emergencia, Gestión del

Conocimiento, entre otros. De igual manera en el modelo propuesto por Gregory Shaw, se tiene la Gestión de Riesgos, Gestión de Incidentes, Continuidad del Negocio, Comunicación de Crisis, entre otros. Este aspecto sin embargo, puede inducir o dar a entender que los diferentes planes, como se los llama, sean elaborados aisladamente lo cual estaría contradiciendo al objetivo de un modelo de continuidad organizacional sistémico e integral.

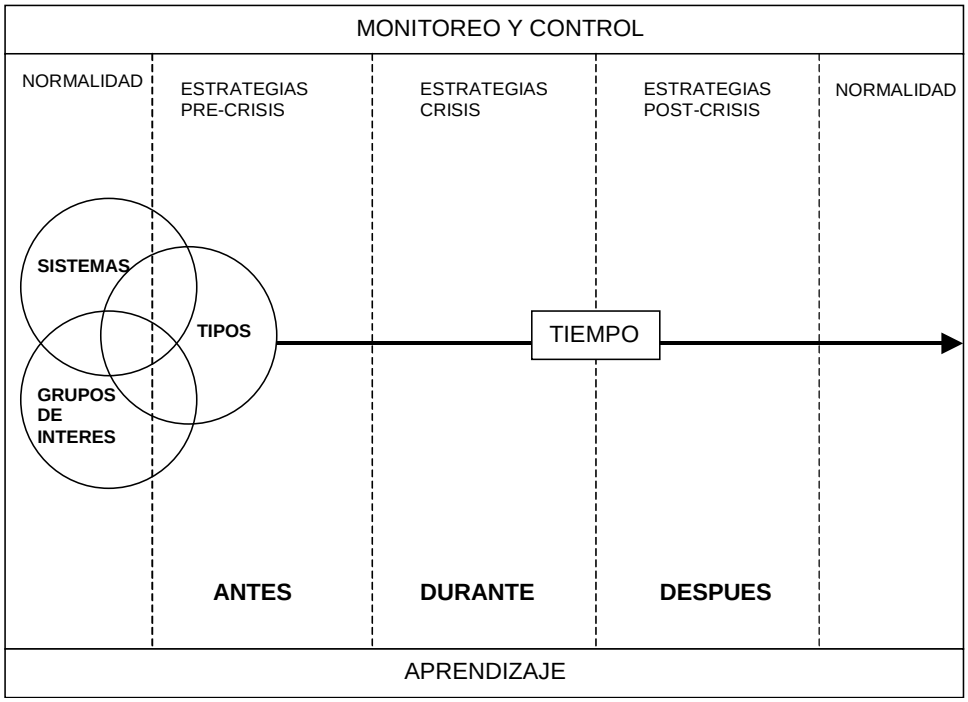
Un aspecto a destacar en el modelo de Mitroff, y que los demás no lo han considerado(al menos en su representación gráfica), es que el experto a llegado a contemplar en su modelo los factores(Tipos, Fases, Sistemas, Stakeholders) que estarían presentes en un evento de crisis, los cuales pueden influir en su gestación o en su tratamiento.

De los modelos analizados, a juicio del autor del presente trabajo, el de Mitroff es el que más se ajusta a esta búsqueda de ciertas características tales como: la temporalidad, tratamiento integral y representación gráfica completa y a la vez sencilla, que a su juicio, un modelo de gestión de crisis(continuidad organizacional) debería tener. Por tal motivo, la presente propuesta se sustenta en la base teórica y el enfoque sistémico del modelo de Mitroff. También se ha tomado en consideración la representación gráfica del modelo de Shaw, específicamente en la representación de la temporalidad, para el desarrollo del modelo alternativo.

En este sentido, el gráfico (Figura 2.16) representa el modelo propuesto. En él se pretende resaltar el origen de un evento de crisis partiendo desde un estado de Normalidad, en este estado los factores (los mismos identificados por Mitroff) Sistemas y Grupos de interés, están interrelacionados para cumplir con los procesos del negocio. De esta interrelación, en cualquier instante puede surgir un evento adverso, que de no ser identificado y tratado adecuadamente podría desembocar en una situación de crisis(Tipo de crisis). Explícitamente se representa la temporalidad de una crisis, reflejado en sus diferentes Fases(Antes, Durante y Después) en las cuales diferentes acciones o estrategias deben ser ejecutadas ante un evento adverso, para retornar nuevamente al estado de

Normalidad, evidenciando con esto que el modelo contempla también la continuidad del negocio.

FIGURA 2.16 MODELO DE GESTION DE CRISIS PROPUESTO



Fuente: Elaborado por el autor

Las líneas discontinuas denotan que el tiempo para cada fase no es algo fijo esto dependerá de la naturaleza de la crisis, de igual manera representa el carácter repentino de una crisis.

En la organización que cuente con un programa de Gestión de Crisis y una cultura de prevención instaurada que permita la detección de las señales tempranas, un evento de crisis en curso puede ser evitado, tratado y/o controlado ANTES(mediante acciones de prevención) de que se materialice o, en caso contrario ejecutar las estrategias de contención(DURANTE) para reducir el impacto.

Todo evento de crisis por mínimo que sea obligatoriamente pasará por la fase DESPUES, en la cual intervendrán todas las funciones necesarias para la completa restauración y retorno a la normalidad.

Un adecuado monitoreo y control permitirá cumplir con los objetivos de la gestión de continuidad organizacional. El aprendizaje organizacional está presente en todo proceso de Gestión empresarial, no solamente en el de GC. Tanto el monitoreo y control como el aprendizaje, son procesos continuos en el tiempo.

Como podemos evidenciar, existen tres etapas principales que son parte del factor Fases, las cuales representan la temporalidad de un evento de crisis. En cada etapa se deben ejecutar ciertas acciones para llevar a cabo la gestión de una crisis, las cuales constituyen las estrategias de un programa de GC, el mismo que se va perfeccionando mediante un proceso cíclico, a través del aprendizaje y la mejora continua. Las etapas mencionadas son: ANTES (PRE-CRISIS), DURANTE (CRISIS) Y DESPUES (POST-CRISIS).

De manera general y haciendo una analogía con las fases identificadas por Mitroff(en el modelo propuesto están implícitos y los denominamos sub-fases), las acciones involucradas en la etapa ANTES son las que tiene que ver con la detección de señales, la preparación y la prevención. Las acciones involucradas en la etapa DURANTE son las relacionadas con la contención y limitación de daños y las acciones involucradas en la etapa DESPUES son las que se refieren con la recuperación y restauración.

Cada organización por lo general tiene al menos un proceso crítico, que de verse interrumpido afectará su operación normal, provocando consecuencias negativas tales como pérdidas financieras, daño a su imagen, entre otras. En este contexto con la presente propuesta lo que se procura es que la organización priorice su gestión a los riesgos(crisis potenciales) que puedan afectar a los procesos críticos, reduciendo en gran medida el impacto sobre la empresa, por la materialización de alguno de esos riesgos.

CAPITULO 3

GESTION DE CRISIS ORGANIZACIONALES

3.1 FUNDAMENTOS DE GESTION DE CRISIS

Como se ha mencionado en la última sección del capitulo anterior, la presente investigación adoptará el término Gestión de Crisis(GC) para identificar a todas aquellas acciones o funciones necesarias para una adecuada gestión de crisis y continuidad del negocio. De igual manera en esta inconsistencia de terminologías, vale la pena mencionar que el término “crisis potenciales” es utilizado por Mitroff para identificar los “riesgos” a los que está expuesta una organización. En la presente investigación se utilizarán indistintamente y tendrán el mismo significado.

Para cumplir con el objeto planteado, tomaremos como referencia el modelo alternativo(Figura 2.16) definido por el investigador a partir del cual se desarrollará la propuesta del programa de gestión de crisis.

A continuación se describe las razones por las cuales una organización debería contar con un programa de GC y porqué la importancia de crear una cultura de prevención en las organizaciones.

3.1.1 ANTECEDENTES

En los últimos años, las crisis inducidas por el hombre han ido en aumento, una de las razones es la complejidad de las organizaciones y de los sistemas, que se han creado principalmente con la sistematización y globalización del comercio.

Existen coincidencias entre las crisis causadas por el hombre y los desastres naturales, pero también existen diferencias principalmente en que las primeras no

necesariamente suceden, es decir son evitables de ahí la necesidad de una gestión de crisis efectiva.[4]

Las crisis independientemente del tipo, aparecen de repente y son situaciones difíciles que pueden causar suspensiones de pagos, pérdida de imagen, huelgas, incendios, contaminaciones, fenómenos que podrían terminar con la vida de las empresas si no son gestionados adecuadamente.

Los tipos de crisis inducidos por el hombre rivalizan a los desastres naturales en alcance y magnitud, podemos citar algunos ejemplos al respecto:

El escape del mortífero gas metilisocianato de una planta de pesticidas de Unión Carbide en Bhopal, India, que causó daños y muertes a millares de empleados y personas que vivían en las inmediaciones.

La explosión del reactor nuclear de Chernobyl[57], que expandió la radiación mortífera por toda Europa y causó numerosas muertes inmediatas y un número desconocido de afectados en futuras generaciones.

La explosión del transbordador Challenger, tuvo como resultado la pérdida de siete vidas, demostró que los defectos de una organización, si se dejan sin corregir pueden producir múltiples crisis.

La quiebra de Enron[58] resultado de manipulaciones contables, implicó el despido de 5,600 personas e hizo evaporarse 68 mil millones de dólares de capitalización.

El escándalo de Parmalat[59], el mayor fraude empresarial en la historia del Viejo Continente. Al octavo grupo industrial italiano, Parmalat, se le descubrió un gigantesco hueco contable por el cual desaparecieron 10 mil millones de euros (casi 13 mil millones de dólares).

---

[4] Mitroff I. y C. Pearson. (2000). *Cómo Gestionar una Crisis*. Barcelona : Gestión 2000. pp 9-11.

[57] Stages of crisis management http://www.unu.edu/unupress/unupbooks/uu21le/uu21le0j.htm

[58] Bravo Patricia. (2003) "Lecciones de Responsabilidad Social Corporativa para la empresa del siglo XXI". http://www.uai.cl/profesores/pag/618.html

[59] Cano Miguel Antonio. Análisis del Caso Parmalat http://www.interamericanusa.com/articulos/Gob-Corp-Adm/Art-Parmalat.htm

Jhonson & Jhonson tuvo que retirar mas de cien mil botellas del mercado por la muerte de 8 personas en Chicago, debido a la colocación de cianuro en las cápsulas de Tylenol.

En nuestro país podemos citar el feriado bancario de 1999, que por el irresponsable manejo financiero, ciertas entidades cerraron, lo cual provocó que los clientes no puedan disponer de sus ahorros y que muchas empresas cerraran sus puertas por falta de liquidez dejando sin empleo a cientos de trabajadores.

El caso del Hospital de Chone, donde la falta de previsión hizo que salga a la luz, la insalubridad en el que los empleados realizaban sus labores, y que por versiones de los pacientes, eso fue la causa de la alta taza de mortalidad de los recién nacidos en dicho centro. En este caso vemos que resulta crítico contar con un portavoz oficial dentro de la institución, ya que al ser una entidad pública los medios de comunicación dieron una amplia cobertura, lo cual provocó graves daños a su imagen y reputación.

De igual manera los constantes derrames de petróleo en nuestra Amazonía han causado daños incalculables al ecosistema y a quienes lo habitan.

Un caso más reciente es el de la empresa de transporte aéreo, Air Madrid; que según los medios, era conocido sus problemas de insolvencia y no se tomó medidas a tiempo para evitar que miles de pasajeros de varios países resultaran afectados por su cierre repentino.

FIGURA 3.1 ATAQUE TERRORISTA NEW YORK, 9/11

Pero, sin duda el principal evento que ha marcado un mayor interés en el campo de la continuidad organizacional, principalmente en el medio estadounidense, es el ocurrido en New York el 11 de septiembre del 2001, donde a más de las vidas humanas, se perdieron información valiosa por lo que algunas compañías dejaron de funcionar. Por ello se afirma que," la preparación no es un lujo, es el costo de hacer negocios en el mundo post 9/11".[60]

Es a raíz del evento 9/11 cuando se reactiva el interés público por los planes de continuidad en el medio estadounidense y a nivel internacional se han dictado regulaciones en ese sentido.

Estudios realizados post ataque 9/11, como el de la Comisión 9/11, reportan la necesidad de que el gobierno trabaje en el proceso de reconocimiento de las responsabilidades del sector privado y en animarlos a tomar los adecuados mecanismos para proteger a la gente, a la propiedad y a las operaciones de los negocios. Se alienta a las organizaciones a asegurar e invertir en programas para mejorar su posición frente al incremento de riesgos, presentados por actos de violencia deliberados(The National Strategy 2003). En el National Response Plan(Enero 2005) y en el Management System (March 2004) se incluye explícitamente al sector privado en todas las fases de gestión de crisis y emergencias (concienciación, prevención, preparación, y en los planes y operaciones de respuesta y recuperación).

La misma Comisión 9/11 ha planteado la necesidad de elaborar un estándar nacional para la preparación del sector privado, el ANSI, a su vez ha sugerido que el Estándar de la NFPA(National Fire Protecction Association) NFPA1600 [61]que se refiere a Programas de continuidad del negocio y administración de emergencias y desastres, sea reconocido como el estándar nacional (ISHN2004).

---

[60] Looney Robert. (2002). Economic Costs to the United States Stemming From the 9/11 Attacks. http://www.ccc.nps.navy.mil/si/index.asp

[61] NFPA 1600. (2004). Standard on Disaster/Emergency Management and Business Continuity Programs. http://www.nfpa.org/assets/files/pdf/ nfpa1600.pdf#search=%22Que%20es%20el%20NFPA%201600%22

De igual manera, el acta The Intelligence Reform and Terrorism Prevention Act of 2004, firmado en la ley del 18 de diciembre del 2004, especifica en la sección 7305 – Private Sector Preparedness, que: "La preparación de los sectores públicos y privados en el rescate, reinicio y recuperación de operaciones debería incluir: un plan para evacuación, una adecuada capacidad de comunicación y un plan para la continuidad de operaciones(IRTPA 2004)". [62]

Las cuestiones de cuando, que tipo de crisis y cómo afectará a la organización, deben tener una respuesta fiable en un programa de Gestión de Crisis, la misma que le ayudará a superar la barrera psicológica de pensar sobre lo impensable, ayudando a prever y prepararse para lo peor.

No existe una receta para afrontar una situación de crisis en las organizaciones, sin embargo es posible elaborar un conjunto de planes y procedimientos de crisis apropiados. Las acciones emprendidas para su tratamiento pueden desencadenar una crisis mayor si los altos directivos no comprenden el contexto en que estas acciones tienen lugar.

Las regulaciones internacionales(Basilea II, Sarbanes Oxley) anteriormente descritas(sección 2.1.2) y las recomendaciones de mejores prácticas de gestión empresarial como la Responsabilidad Social Corporativa(sección 1.5) están produciendo diversos beneficios a las empresas, que van desde el ahorro de costes derivado de la gestión sostenible de recursos, hasta la mejora de las condiciones laborales en los centros de trabajo, consiguiendo una mayor implicación de los empleados con el proyecto empresarial. Los activos intangibles son cada vez más importantes para las empresas, aportando un valor a la marca que se refleja en sus balances.

A pesar de haber tocado en capítulos anteriores algunos aspectos relacionados y que influyen en la gestión de crisis, exponemos a continuación un resumen de

---

[62] www.nasttpo.org. NFPA 1600 Included in the Intelligence Reform and Terrorism Prevention Act of 2004. http://www.nasttpo.org/ NFPA1600.htm

algunos de ellos, que es necesario tomarlos en cuenta en la implementación de un programa de gestión efectivo.

3.1.2 GESTIÓN DE CRISIS Y CULTURA ORGANIZACIONAL

La cultura y los valores tienen una prueba de fuego en cada crisis que enfrenta la empresa. Es claro que una empresa que privilegie marcos de comportamiento basados en la confianza, la cooperación y la transparencia tendrá una mayor probabilidad de éxito.

El término resiliencia[63] ha sido introducido recientemente en el campo de la gestión empresarial. La resiliencia es una manera de ver los comportamientos humanos desde una perspectiva multidiciplinaria, que tiene como objetivo mejorar los procesos y resultados de los grupos humanos frente a la crisis.

En un evento de crisis, están presentes situaciones de incertidumbre, temor, desconfianza, apatía y negativismo, esto es una respuesta automática a los problemas y estímulos que vienen del ambiente (interno o externo) que de una u otra forma va a repercutir en el desempeño. Por este motivo, cuando los empleados se encuentran en una situación en donde el desgano, ha tomado cuerpo, es necesario una intervención motivacional para recuperar el estado anímico positivo.

En este sentido, el papel del líder es muy importante en el desarrollo de ambientes, en donde a pesar de la crisis, existen propósitos para mantener el ánimo y la actitud de competencia que las personas dentro de las empresas requieren para su mantenimiento y desarrollo.

---

[63] Horner Ken. (2006). Successful Business Continuity Strategies: How to Conduct Business as Usual.
http://www,wwpi.com/index.php?option=com_content&task=view&id=1379&Itemid=44

Aunque no existen fórmulas ni recetas que funcionen en la realidad, el conocimiento que surge del estudio del comportamiento de las personas dentro del trabajo, hace posible proponer algunas acciones, las cuales pueden ser valiosas, para aquellos que tienen como tarea, dirigir u orientar el trabajo de otros en condiciones críticas: [64]

- *Cumplir con las obligaciones*: el pago a tiempo y sueldo completo es importante, de ser posible pensar en acciones de incentivo que estimulen a las personas en ocasiones especiales.
- *Conformación de un verdadero equipo*: en circunstancias de amenaza los seres vivos tienden a integrarse en equipos, los que brindan la oportunidad de dar y recibir apoyo; esto permite sobrellevar en mejor forma los impactos emocionales que las crisis generan.
- *Reuniones, orientación, comunicación y apoyo constante*: el manejo de la información de la crisis dentro de las reuniones de trabajo, permite que las personas tengan "una válvula de escape" para los problemas que las situaciones diarias generen.
- *Prevenir el conflicto y eliminar las luchas de poder*: cuando las organizaciones se desgastan por la crisis, es importante prevenir los elementos internos que puedan erosionar el ánimo o minar la moral de sus miembros. En tal sentido, la creación de un clima de cooperación y de competencia sana, libre de luchas de poder o conflicto entre los miembros de la empresa es importante.
- *Incentivar y premiar los resultados*: parte de crear un clima de optimismo, viene de reconocer los logros a pesar del mal tiempo. En tales circunstancias, el reconocimiento en cualquiera de sus modalidades suele dar la pauta para mantener un ambiente optimista.
- *Preparación*: la responsabilidad de la conducción y dirección en tiempos de crisis, exige también contar con recursos nuevos por parte del gerente. Esto requiere que el líder se capacite, tanto en nuevos enfoques de negocio y gerencia, como en aspectos vinculados a la comprensión de las personas. Lo anterior supone, lecturas, asistencia a seminarios e intercambio de

[64] Alvarez José Angel.(2004). Optimismo en medio de la crisis: cómo lograrlo http://www.mujeresdeempresa.com/relaciones_humanas/relaciones040701.shtml

experiencias con otros ejecutivos que han manejado con éxito situaciones de crisis.

- *Actividades colectivas que incluyan acción*: el ejercicio y la actividad social compartida, suelen crear cohesión y mejorar el ánimo de las personas. Por tal razón, incluir éstas dentro de las acciones de soporte para la crisis, suelen mantener ágiles y dispuestas a las personas de la organización.

Las recomendaciones anteriores, utilizadas en forma individual o en conjunto, pueden servir como herramientas o guía, para que en una situación de crisis dentro de las organizaciones generen aprendizajes positivos en sus integrantes.

3.1.3 GESTIÓN DE CRISIS Y CULTURA DE PREVENCIÓN

"Todas las empresas deben enfrentarse, en algún momento, a situaciones financieras realmente conflictivas y traumáticas. Algunas logran superarlas: son las "ganadoras". Otras sucumben irremediablemente: son las "perdedoras". Sin embargo, todos los estudios coinciden en señalar que las organizaciones que han podido superar con éxito sus períodos de crisis son aquellas que han actuado con decisión ante sus primeros síntomas". [65]

Siempre existe la posibilidad de que cualquier empresa se enfrente a una situación adversa, independientemente del sector al que pertenezca, y tiene que prepararse con anterioridad si quiere hacerle frente con éxito.

En el campo de la salud y seguridad laboral, la cultura de prevención también ayuda a disminuir la siniestralidad, por eso se recomienda incluirlo en el programa de gestión integral de la empresa. Este aspecto no solo incide en los campos mencionados, sino que tienen una vinculación directa con la productividad empresarial, afectada por el tiempo perdido, los productos inutilizados, la revisión de maquinaria, y otros aspectos menos cuantificables como las sanciones y los

---

[65] Soriano Claudio L. (2006). Evalúe cuál es su nivel de riesgo.
http://www.microsoft.com/spain/empresas/marketing/empresas_crisis.mspx

efectos psíquicos en la plantilla ante un drama humano. En este sentido, “los empresarios están tomando conciencia en que la siniestralidad influye en la cuenta de resultados”.[66]

“La prevención en la empresa es una inversión. Siempre es menor la inversión necesaria en la prevención que el impacto económico, funcional y estructural de los costes derivados de la ocurrencia de un siniestro”.[67]

La formación es un aspecto clave para la adopción de conductas seguras y la utilización de los sistemas de prevención por parte de los empleados en sus actividades diarias, además deben ser participes en la gestión de la prevención. Cuanto mejor la organización pueda prever los aspectos de una crisis mejor podrá dominarla e inclusive tendrá más probabilidades de salir reforzado una vez superada.

La completa prevención de crisis es imposible, pero en principio las inducidas por el hombre son evitables. La gestión de la prevención es un aspecto esencial de la gestión empresarial de hoy y del futuro, debido a que a la empresa se le exige una mayor eficiencia en la utilización de los recursos para garantizar su sostenibilidad.

3.1.4 GESTIÓN DE CRISIS Y LA COMUNICACIÓN

Ninguna organización espera hacer frente a situaciones que causan una interrupción significativa del negocio, que estimule una cobertura de los medios. La difusión pública como resultado de una crisis, puede afectar las operaciones normales de la compañía y puede a menudo tener impacto financiero, legal y en la imagen corporativa de manera negativa si no es gestionada adecuadamente.

---

[66] Garcia Fernando. (2005). La prevención entra en una etapa de más calidad y mayores precios. http://www.fomenweb.com/revista/1250/

[67] Llongueras Pasqual. (2006). Prevención y rentabilidad, por fin. http://www.prevencionintegral.com/default.asp

Es necesario que los miembros de la organización conozcan que las únicas personas autorizadas a hablar en una situación de crisis al mundo exterior, son los miembros del equipo de GC, y específicamente su portavoz oficial. Además la(s) persona(s) responsable(s), debe estar debidamente preparada para enviar mensajes a todos los interesados[68] (audiencia interna y externa) de forma eficaz y hacer las puntualizaciones que considere pertinentes sobre imprecisiones o versiones infundadas de lo que ocurre, si no quiere sufrir un daño irreparable a la imagen del negocio.

3.2 IMPACTO FINANCIERO DE LA GESTIÓN DE CRISIS

"Un riesgo es un riesgo, ellos afectan el potencial de las ganancias, ya sea que provengan de fluctuaciones en los precios de los commodities(activos), del equipamiento contra incendio, del cambio en la legislación, o de la cobertura adversa de los medios. Finalmente, cómo usted reparte sus riesgos es la base de cómo usted ve la misión principal de su compañía y la razón de los inversionistas para invertir en ésta. Por lo tanto, conocer sus riesgos es conocerse a sí mismo. Anderson Bill Director Swiss New Markets."[69]

Como se ha manifestado, no es posible prepararse para todos los tipos de crisis, una de las razones es que la mayoría de las organizaciones no contarían con los suficientes recursos(humanos, financieros, infraestructura) para implementarlo.
Sin embargo, cabe recalcar que en cada organización, existen procesos críticos cuya interrupción puede causar grandes pérdidas económicas, razón por la cual su vigilancia es requerida.

---

[68] www.tinkle.es. (2006). Comunicación en tiempos de crisis.
http://www.tinkle.es/pages/desarrollo/desa.htm

[69] Entendiendo la administración del riesgo. (2006). Enterprise Risk Management, p.2
http://www.kpmg.cl/aci/pdf/ERM.pdf.

A continuación algunas estadísticas[70], que demuestran el impacto financiero que puede causar un evento de crisis(en este caso, a causa del aspecto tecnológico).

- El 20% de las compañías perdió más de un millón de libras, otro 20% perdió entre un millón y un cuarto de millón de libras, y el 43% perdió 10.000 libras (Coopers & Lybrand).
- Un tercio de todas las pérdidas comerciales cubiertas por seguros en el 2003 estuvieron relacionadas con ordenadores, y no incluyen los costes por interrupción de negocio o pérdida de datos (Association of British Insurers).
- El 78% de las compañías ha sufrido ataques por Internet, siendo el coste promedio de 30.000 libras (Department of Trade and Industry).

Sin duda el aspecto financiero es uno de los que más se ve perjudicado cuando un evento adverso se ha hecho presente, por ello es necesario tenerlo presente y balancear el presupuesto asignado a gestionar los riesgos.

3.3 DIAGNÓSTICO DE LA PREPARACIÓN ORGANIZACIONAL ANTE LA CRISIS [4]

Para el diagnóstico de la preparación organizacional, haremos uso de las herramientas de diagnóstico de Mitroff, el mismo que, luego de un profundo estudio de los factores de crisis que afectan a las organizaciones elaboró varios cuestionarios y el procedimiento para su representación gráfica así como su interpretación. Existe una herramienta para cada uno de los factores de crisis, esto nos permitirá determinar el nivel de preparación de la organización.

En la evaluación de la vulnerabilidad de una organización se debe procurar la participación de la mayor parte del personal y/o de quienes tengan mayor conocimiento de las diferentes áreas del negocio, para obtener distintas

---

[70] Office-Shadow - Business Continuity Software. (2006). Estadísticas sobre la Continuidad de Negocio. http://www.office-shadow.com/es/business-continuity-management/business-continuity-drivers-3.html

[4] Mitroff I. y C. Pearson. (2000). Cómo Gestionar una Crisis. Barcelona : Gestión 2000. pp. 47-94.

percepciones de la realidad. Las herramientas diagnósticas que se describen a continuación permitirán evaluar la actuación de la organización ante crisis potenciales actualmente.

a) Tipos de crisis

El par de cuestionarios que nos permiten determinar de manera general, donde la organización esta preparada y donde la organización es vulnerable, son la herramientas de diagnóstico “Tipos-crisis” y “Tipos-acciones preventivas”(ver Anexo 1). La primera recoge los diferentes tipos de crisis que pueden afectar a una organización, agrupados por categorías(A-H) que representan a las familias de crisis(ver Figura 2.15), vale la pena recalcar que cada ítem no debe ser interpretado textualmente sino que se debe dar la interpretación adecuada de acuerdo a la actividad de la empresa. La herramienta diagnóstica “tipo-acciones preventivas”, es un complemento a la anterior, en ésta se identifican que controles existen actualmente para contrarrestar potenciales crisis, de igual manera esta dividida en varias categorías(A-E) que representan a las familias de acciones preventivas(ver Figura 2.16).

b) Fases de crisis

Como se ha mencionado, el factor Fase se refiere a la temporalidad(Antes, Durante y Después), en este sentido, implícitamente están contenidas las sub-fases: detección de señales, preparación/prevención, contención/limitación de daños, recuperación y aprendizaje. La herramienta diagnóstica Fases(Ver Anexo1), nos permite identificar si existen o no implementados controles o procedimientos para cada fase, para la gestión de un evento de crisis considerando que, toda crisis pasa por las tres fases señaladas, por lo que es necesario implementar acciones a ser ejecutadas en cada una de ellas.

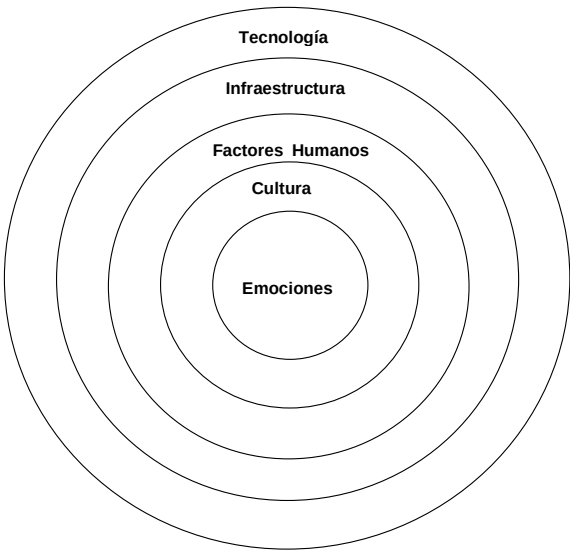
c) Sistemas de crisis

Las crisis ocurren a causa de la falla simultánea de sistemas técnicos, organizacionales y humanos, por lo que no es lógico analizar los sistemas que incluyen una tecnología central de la organización aisladamente de los sistemas humanos y organizacionales que lo implementan.

Las diferentes variables, componentes del factor Sistemas, Mitroff los interpreta como capas, según su mayor o menor visibilidad. (ver Figura 3.2). La figura representa una visión de conjunto, así como las complejas interacciones entre los factores técnicos, organizacionales y humanos individuales, que pueden causar e impedir las crisis. Los aspectos técnicos o las operaciones tecnológicas son las más fáciles de observar, éstos incluyen el equipo y la maquinaria que permiten que el trabajo se haga, así como los procesos necesarios para fabricar un producto o prestar un servicio.

Otra capa lo constituye la infraestructura de la organización, comprende el organigrama jerárquico que representa la estructura formal de poder. Algunas variables adicionales de esta capa y menos tangibles son: la comunicación formal, los premios y los sistemas presupuestarios. Los factores humanos constituyen la siguiente capa más interna, estos son menos visibles que las anteriores. Un ejemplo podría ser el “ajuste” entre el operario y la máquina.
Una capa más adentro está la cultura de una organización, la cual es prácticamente invisible o se da por supuesta.
Finalmente la última capa, la estructura emocional de la organización, la cual representa las respuestas emocionales.

FIGURA 3.2 CAPAS DE LOS SISTEMAS DE GC



Fuente: Ian Mitroff. Cómo Gestionar una Crisis. p.66

Mediante el uso de la herramienta de diagnóstico del Factor Sistemas(ver Anexo1), es posible evaluar la actuación de la organización respecto a este factor. Esta herramienta es básicamente un cuestionario sobre si se realizan ciertas tareas tales como: análisis de riesgos, mantenimiento periódico de equipos, auditorías de factores humanos, entre otras, o en si se establecen ciertas políticas tales como: incorporar la GC a las estrategias del negocio, implicar en su gestión a empleados de todos los niveles, valorar en la misma proporción la productividad y la seguridad, establecer canales de comunicación adecuados, entre otras.
Como vemos, existe una larga lista de aspectos que se deben tomar en cuenta respecto al factor Sistemas, sin embargo, es preciso señalar que esta lista debe adecuarse de acuerdo a la actividad de la empresa, ya que ciertos aspectos no son comunes para todas a las organizaciones.

d) Grupos de interés

Cuanto mayor y más compleja sea una crisis, más amplio es el conjunto de grupos de interés que pueden estar implicados.
Mediante el uso de la herramienta de diagnóstico Grupo de Interés(ver Anexo1), es posible evaluar la actuación de la organización respecto a este factor. Esta herramienta básicamente esta compuesta de dos partes: un listado de grupos de interés tomados en cuenta en los planes GC (de existir) o en las acciones de tratamiento de riesgos y, otra lista de quienes colaboran en la elaboración de los mismos planes.

En los últimos años el conjunto de stakeholders se ha extendido mas allá de los empleados, gerentes y sindicatos. Ahora se incluye a clientes, proveedores entre otros, por lo que la GC debe tomar en cuenta a todos los involucrados. En este sentido, la organización preparada, esta consciente de los stakeholders(grupos de interés) afectados, por lo tanto tiene una percepción diferente de la responsabilidad organizacional y de la relación con su entorno.

En resumen, las herramientas de diagnóstico ayudan a determinar el grado de preparación de la organización ante crisis, independientemente de sí tienen o no implementado un plan formal de GC, ya que como veremos más adelante existen

varias etapas de preparación ante crisis. Realizar el diagnóstico es muy beneficioso, en el sentido de que mediante el contenido de los cuestionarios es factible realizar un primer acercamiento a la gestión de crisis y evidenciar la amplitud de un programa de gestión de crisis efectiva. Cabe señalar, que los cuestionarios reflejan también las acciones consideradas como “buenas practicas” que llevadas a cabo por compañías exitosas.

3.4 ELABORACIÓN DEL PERFIL DE CRISIS [4]

Con los resultados obtenidos de la evaluación mediante las herramientas de diagnóstico, y una vez totalizado las respuestas afirmativas, se procede a elaborar la representación gráfica para cada factor de crisis, utilizando los respectivos Diagramas de Barras. En el diagrama el eje vertical representa el nivel de preparación y el horizontal representa a las variables(sub-factores) de los factores en el caso de la representación individual, mientras que, en la representación combinada el eje horizontal representa a los factores.

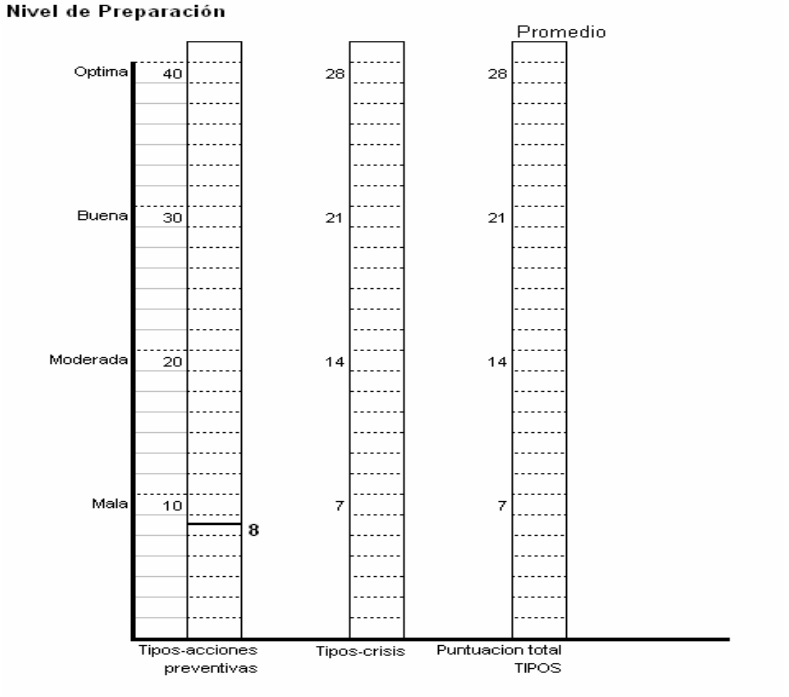
Mitroff ha dividido los niveles de preparación en cuatro segmentos identificados como: Mala, Moderada, Buena y Optima. Esta distribución se ha dado de manera simétrica de acuerdo al número de ítems de los cuestionarios para los sub-factores, a los cuales les corresponde una barra en la representación gráfica. Para el caso del Factor Tipos se representa mediante una barra por cada herramienta(crisis y acciones preventivas) y su escala corresponde al número de ítems de cada una (Figura 3.3). Es posible determinar el nivel de preparación en cada sub-factor al representar la puntuación en la barra correspondiente.

Como ejemplo, en la figura 3.3 se representa la puntuación de 8 (respuestas afirmativas), para el sub-factor “Tipos-acciones preventivas”, en ella, constatamos que la misma está por debajo del nivel Mala, lo cual indica que la organización poco o ningún esfuerzo esta realizando en cuanto a la GC.

---

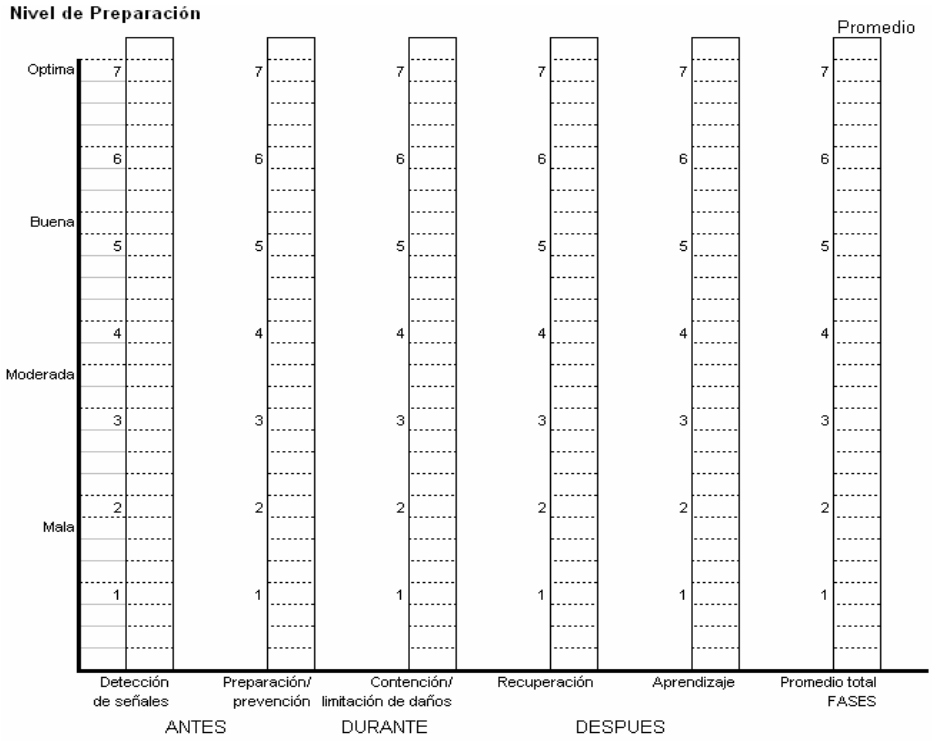
[4] Mitroff I. y C. Pearson. (2000). Cómo Gestionar una Crisis. Barcelona : Gestión 2000. pp. 95-97

FIGURA 3.3 DIAGRAMA DE BARRAS PARA TIPOS



Fuente: Ian Mitroff. Cómo Gestionar una Crisis. pp 50,53. Adaptado por el autor.

FIGURA 3.4 DIAGRAMA DE BARRAS PARA FASES

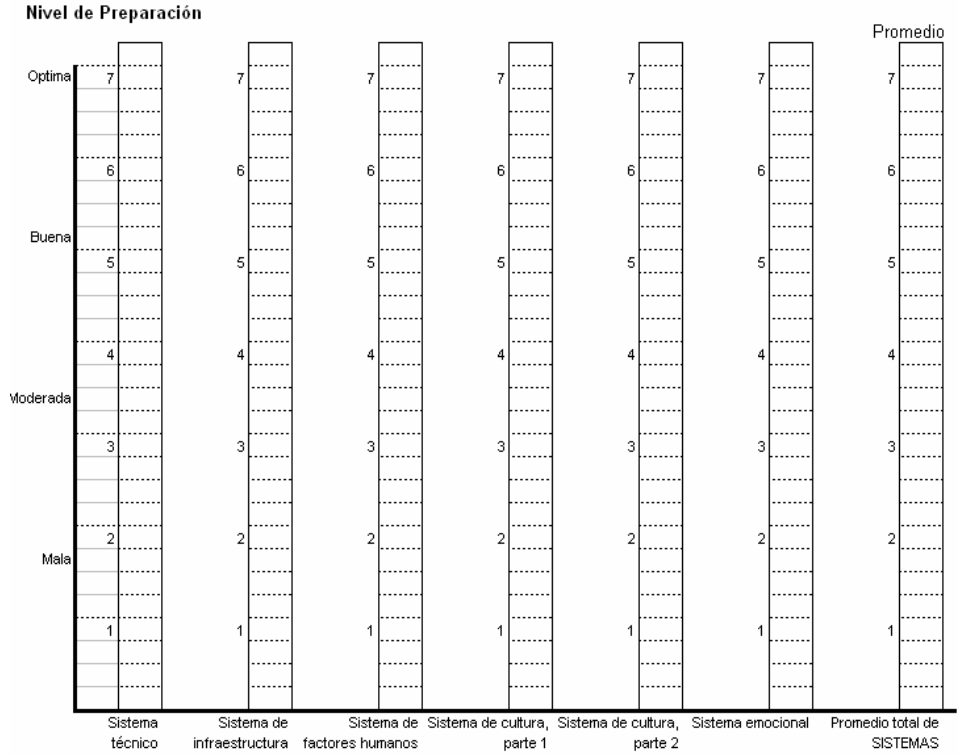


Fuente: Ian Mitroff. Cómo Gestionar una Crisis. p. 62. Adaptado por el autor.

Para el factor Fases de acuerdo a su herramienta de diagnóstico(Ver Anexo 1), se representa en una barra cada sub-fase (detección de señales, preparación/prevención, contención, recuperación y aprendizaje) y su escala corresponde al número de ítems de cada sub-fase(Figura 3.4). Las puntuaciones obtenidas para cada sub-factor se transforman a una escala semejante, para hallar el valor promedio del Factor el mismo que, es representado en la barra de resultado “Promedio”. Para el caso del Factor Tipos el resultado se representa en una escala de 1:4(segmentado de 1-28) y para los demás factores en la escala 1:1(segmentado de 1-7).

En el caso del factor Sistemas de acuerdo a su herramienta de diagnóstico (Ver Anexo 1), a cada agrupación de Sistemas(técnico, infraestructura, cultural, emocional) le corresponde una barra y su escala está dada por el rango de puntuación(1-7), como se indica en la Figura 3.5.

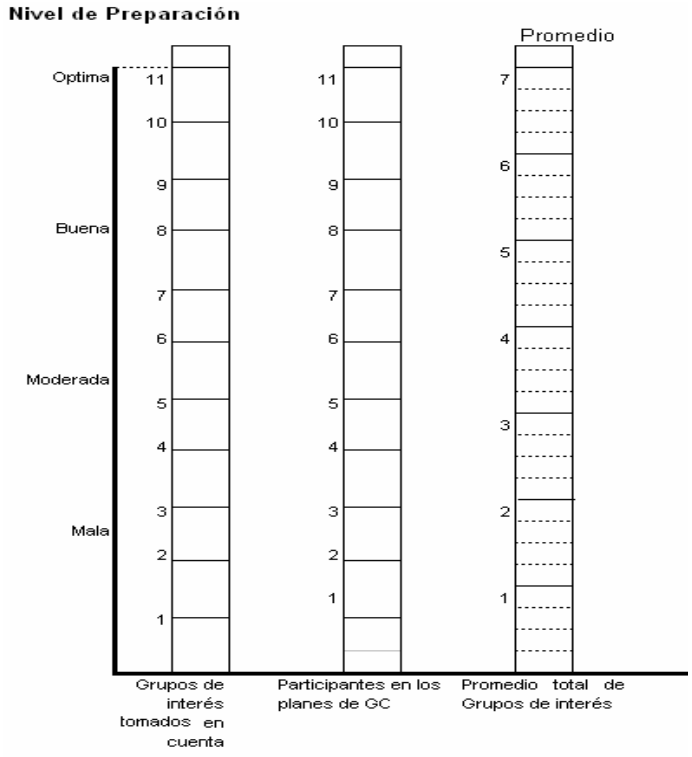
FIGURA 3.5 DIAGRAMA DE BARRAS PARA SISTEMAS



Fuente: Ian Mitroff. Cómo Gestionar una Crisis. p. 75.

En cambio el factor Grupo de interés, de acuerdo a su herramienta de diagnóstico(Ver Anexo 1), se representa en dos barras que corresponden a cada agrupación en la herramienta(Grupos de interés tomados en cuenta y los participantes en la preparación de planes de GC) y la escala está dada por el número de ítems de cada agrupación(Figura 3.6).

FIGURA 3.6 DIAGRAMA DE BARRAS PARA GRUPOS DE INTERES



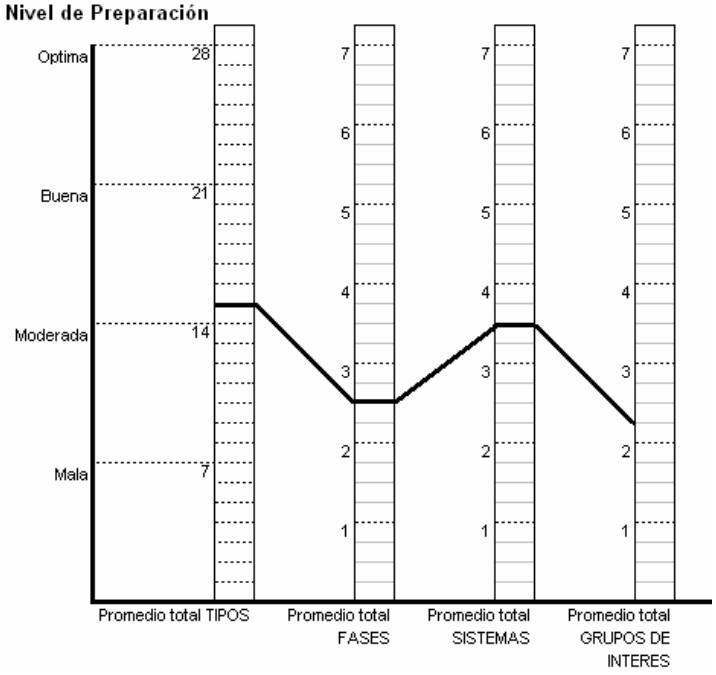
Fuente: Ian Mitroff. Cómo Gestionar una Crisis. p. 91.

Finalmente, los valores promedio obtenidos para cada Factor, se los representa en un diagrama de barras aparte, en escalas semejantes.

Con las puntuaciones promedio obtenidas para cada uno de los factores y representadas en sus respectivas barras, es posible trazar el perfil de crisis de una organización. Para ello, mediante una línea recta se unen las puntuaciones de las barras adjuntas, como se muestra en el Diagrama de Perfil de Gestión de Crisis(Figura 3.7). Esta es una manera rápida de ver los puntos débiles y fuertes de la organización ante una crisis respecto a los cuatro factores.

Según Mitroff, un factor se encuentran en la “zona de peligro” si las puntuaciones en el diagrama, están localizadas por debajo del nivel “Moderada”, lo cual es un aviso de que la organización debe prestar mayor atención y emprender las actividades necesarias para salir de esta zona. Los factores localizados dentro de las zonas buena y óptima son considerados fortalezas, caso contrario son debilidades. Finalmente, cabe mencionar que si cualquier variable de un factor entra en la zona de peligro, es una señal clara de que la organización es propensa a la crisis.

FIGURA 3.7 PERFIL DE GESTION DE CRISIS



Fuente: Ian Mitroff. Cómo Gestionar una Crisis. p. 91.

Si bien todos los factores son importantes, la variable *cultura* del factor Sistemas es aún muy crítica. En este sentido es muy importante conocer cuanto valora la organización las prácticas de seguridad, si existe discusión abierta de procedimientos de emergencia o de errores de seguridad, si se da buenos ejemplos de seguridad desde los niveles superiores.

3.4.1 LAS ETAPAS DE PREPARACIÓN ANTE LA CRISIS [4]

Según Mitroff, desde el punto de vista de la actuación organizacional sobre cada uno de los factores, es posible distinguir cinco etapas de preparación ante la crisis y que cada etapa subsiguiente incorpora las capacidades de GC de las etapas previas.

3.4.1.1 PRIMERA ETAPA

La primera etapa comprende el nivel más bajo de preparación, se restringe a precauciones tradicionales de seguridad. Es probable que sus procedimientos estén implementados de manera caótica, fragmentada a lo largo de la organización.

Los empleados no están familiarizados con sus papeles al implementar los planes. Es poco lo que se realiza en cuanto a ejercicios, prácticas o simulaciones, y el profesionalismo y entrenamiento de los que tienen la responsabilidad en caso de emergencia es baja. Las organizaciones de esta etapa tienden a negar sus debilidades. La implementación de planes para emergencias requieren poco esfuerzo por parte de la organización, de esta manera su preparación se limita a los tipos de crisis que reconocen.

Por lo general, las organizaciones son reactivas, debido a que prácticamente no existen programas de prevención, la planificación para la contención rara vez se da antes de que una crisis se haya desatado.

No tienen ninguna estructura organizacional para la GC, presupuesto o equipo formal. La GC lo ven como un gasto que no puede justificarse.

No perciben como los grupos de interés afectan a sus operaciones normales, peor aún como pueden resultar afectados o afectar al desarrollo de una crisis importante. Lo más probable es que exista un solo individuo de la jerarquía media que defienda la GC, de ahí que no sea una prioridad para la alta dirección.

---

[4] Mitroff I. y C. Pearson. (2000). Cómo Gestionar una Crisis. Barcelona : Gestión 2000. pp. 101-106

3.4.1.2 SEGUNDA ETAPA

Las organizaciones ya cuentan con un programa de gestión de desastres naturales y los causados por el hombre, pero es probable que no planifiquen ni se preparen para otros tipos de crisis.

Tienen una estructura organizacional y un presupuesto destinados a las funciones tradicionales de emergencias y seguridad. Aquí es mucho más probable que dispongan de mecanismos para contención y reanudación de actividades, pero no se preparan para lo que son ataques económicos, fugas de información, extorsión, etc.

Generalmente se concentran en los factores técnicos y no se dan cuenta de que la cultura organizacional también puede causar crisis importantes. De igual manera ignoran como los grupos de interés pueden afectar y resultar afectados, y se concentran básicamente en los internos. El interés de la GC ya se extiende a algunos miembros del equipo administrativo.

3.4.1.3 TERCERA ETAPA

Las organizaciones tienen procedimientos y planes mas detallados, abarcan, quién debe ser avisado y qué debe hacerse en ciertas circunstancias.

Todavía es poco probable que los planes estén integrados con otros procedimientos de crisis, como por ejemplo de otra área, de esta manera las lecciones aprendidas en una área no se comparten para beneficiar a la organización como un todo.

Aquí ya se toma en cuenta a los grupos de interés externos a la organización, aunque todavía no participan en la elaboración de planes. Algunos de los miembros de la alta dirección ya están conscientes de la importancia de la GC.

3.4.1.4 CUARTA ETAPA

Las organizaciones tienen integrado los planes. La gestión de crisis se restringe a pocos riesgos, generalmente a los del sector de industria.

Se realizan esfuerzos formales para las fases iniciales y posteriores de las crisis, además se planifica para la contención, prevención y recuperación.
Son identificados los grupos de interés externos que son críticos para la organización. Los altos directivos hacen suya la responsabilidad de la GC, por que se crea formalmente el equipo de gestión que tendrá la responsabilidad de facilitar y formalizar los esfuerzos.

3.4.1.5 QUINTA ETAPA

Las organizaciones muestran grandes capacidades de GC y son mucho más conscientes de su vulnerabilidad. Estas planifican y se preparan para al menos una crisis de cada familia y adoptan una acción preventiva para cada una de las familias de prevención.

Se presta mayor atención a cada una de las fases de la GC mediante acciones y procedimientos. Lo más probable es que las organizaciones desarrollen los planes y procedimientos tomando en cuenta explícitamente todos los sistemas críticos que participan en la causa y en la prevención de crisis.
Ven a los factores humanos, organizacionales y emocionales como fuentes de crisis. Tienen mayor conciencia de como contribuye la cultura organizacional, por lo que hay mayor participación de sus miembros en los simulacros, y por lo general, se incluyen a los grupos de interés externos en los esfuerzos de GC. En esta etapa la GC se valora como un activo.

3.5 ELABORACIÓN DEL PROGRAMA DE GESTIÓN DE CRISIS

Como se ha manifestado no existe una fórmula para llevar a cabo una gestión integral de los riesgos que sea aplicable a todas las organizaciones, dado que sus actividades y procesos son únicos, en tal virtud los riesgos a los que se encuentra expuesto son propios del ámbito en que se desarrolla su actividad de negocios. En este sentido un programa de GC para una organización en particular será personalizado.

En los casos más extremos, cuando una empresa entra en una crisis de supervivencia atrae la mirada de todos los grupos de interés, en ese momento cada nómina, cada declaración de impuestos, cada compra, la cuenta de servicios públicos, el pago del arrendamiento, en fin todo egreso se convierte en una pesadilla para la alta gerencia. El peor error es no aceptar la crisis, debido a que esto únicamente retarda la toma de decisiones para afrontarlo eficazmente, por ello es necesario anticiparse a las crisis mediante la concienciación y preparación lo cual es posible lograrlo mediante un adecuado programa para gestionarlo y en la medida de lo posible se evite entrar una crisis de cualquier tipo.

Los objetivos principales de elaborar un programa de GC son:
Minimizar las potenciales pérdidas económicas, disminuir las potenciales exposiciones, reducir la probabilidad de ocurrencia, reducirlas interrupciones a las operaciones, asegurar la estabilidad organizacional, facilitar una recuperación ordenada, minimizar el pago de seguros, reducir la dependencia en empleados claves, proteger los activos de la organización, asegurar la seguridad del personal y clientes, minimizar la toma de decisiones durante un evento desastroso, entre otros.

Basándome en lo descrito en la sección 1.1 del capitulo uno (Conceptos y Definiciones), de igual manera en los conceptos y el enfoque de Mitroff (sección 2.3.2.7) y en el modelo propuesto por el autor, me permito proponer, una metodología para emprender un tratamiento integral de los riesgos, sustentado en las siguientes premisas:

- Dado que en un evento de crisis están implicados cuatro factores interrelacionados(Tipos, Sistemas, Fases y Grupos de interés) es necesario un enfoque sistémico en su tratamiento y no de manera aislada.
- La gestión de la organización debe estar basada en procesos, lo cual facilita el tratamiento sistémico y la determinación de su cadena de valor y dentro de ésta el proceso crítico.
- La gestión de los riesgos es una actividad continua y como tal es factible alcanzar una nivel razonable de preparación ante eventos adversos de manera progresiva.

- Las acciones a considerar para el tratamiento de un riesgo en particular estará basado en su naturaleza y para determinar su impacto en el negocio podrán adoptarse métodos cuantitativos y/o cualitativos que más se ajuste a su realidad.

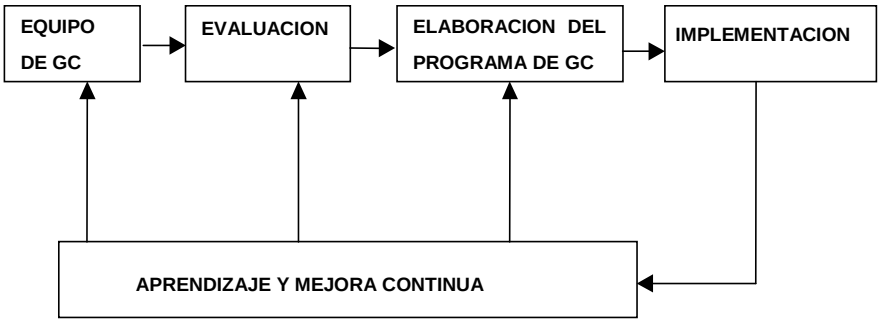
Basado en estas premisas, el objetivo a ser alcanzado en un tiempo prudente será el de asegurar la continuidad del negocio, al dar tratamiento en primera instancia a los riesgos de los procesos que son parte de la cadena de valor de la empresa, comenzando el tratamiento por el proceso más crítico de dicha cadena. Seguidamente se dará tratamiento a los demás procesos de la cadena de valor y a continuación a los procesos de apoyo hasta cubrir la totalidad de los procesos de la organización. Al ser la GC un proceso cíclico y permanente, las actividades aprendizaje y mejora continua, son muy importantes, debido a que a través de éstas se va perfeccionando el programa de gestión, ya sea capacitando periódicamente al personal, realizando pruebas de efectividad o dando tratamiento a nuevos riesgos detectados.

Con este procedimiento se espera lograr y mantener una gestión razonable de los riesgos, cuya efectividad real se comprobará únicamente cuando se haga presente un evento adverso. Si se presenta un escenario para el cual la organización no estuvo preparada, constituirá la oportunidad para mejorar el programa de GC. Para cumplir con este propósito será necesario:

- El apoyo decidido de la alta gerencia.
- Incorporar la GC en el proceso de planificación estratégica, incorporándolo en la declaración de la misión de la empresa.
- Generar la cultura de prevención en la organización mediante el involucramiento y la capacitación de todo el personal.
- Proveer de recursos para cumplir con este propósito.

En este contexto el proceso metodológico de planificación global de Gestión de Crisis, gráficamente se representa así:

FIGURA 3.8 PPROCESO DE PLANIFICACION DE GESTION DE CRISIS



Fuente: Deloitte & Touch. Business Continuity Management, p.12. Adaptado por el autor.

El ciclo de planificación de un programa de GC comprende las siguientes etapas:

Equipo de Gestión de Crisis

Alguien en la organización debe visualizar y ser el promotor de la necesidad de gestionar la continuidad organizacional, para que posteriormente se formalice adecuadamente sea un equipo o comité de gestión de crisis.

Evaluación

- Diagnóstico de la preparación organizacional.
- Evaluación de tipos de crisis potenciales.

Elaboración del programa de GC

- Definición de estrategias de prevención.
- Definición de estrategias de mitigación.
- Definición de estrategias de recuperación.

Implementación

- Plan de entrenamiento y pruebas.
- Plan de mantenimiento y control de cambios.

Aprendizaje y mejora continua

- Proceso que perfecciona el programa de GC.

Los altos directivos deben estar convencidos de la necesidad de la GC, antes de iniciar con el proceso, ello constituirá el mayor respaldo para que su implementación en la organización sea exitosa.

Es recomendable iniciar el proceso de gestión de crisis, con el tratamiento de los riesgos identificados como más críticos para la continuidad del negocio. De igual manera, se recomienda evolucionar progresivamente a los niveles superiores de preparación ante crisis(sección 3.4).

Analicemos a continuación cada una de las etapas del proceso metodológico:

3.5.1 EQUIPO DE GESTIÓN DE CRISIS

Uno de los aspectos más importantes en la planificación de un proceso de gestión de crisis, es la conformación del Equipo de Gestión de Crisis (EGC), que entre sus principales responsabilidades están: organizar esfuerzos más proactivos, intentar disminuir la probabilidad de crisis y desarrollar procesos de aprendizaje organizacional.

Lo ideal sería que la alta gerencia sea el promotor de la necesidad de una GC, sin embargo muchas veces esto no sucede, por lo que es muy posible que en un comienzo, empleados de los mandos medios y bajos sean los impulsores de esta necesidad, quienes tienen la labor de convencer a los altos directivos para obtener su apoyo.
La eficacia de un EGC, se potencia con un presupuesto, el desarrollo de políticas y procedimientos de gestión de crisis. La participación de los altos directivos es beneficiosa para la implementación de decisiones claves y para lograr recursos esenciales.

A continuación, un listado más amplio de las principales actividades que debe llevar a cabo el EGC:[4]

- Determinar el contexto y definir el objetivo de la GC.
- Elaborar un listado de crisis potenciales(riesgos)

---

[4] Mitroff I. y C. Pearson. (2000). Cómo Gestionar una Crisis. Barcelona : Gestión 2000. p. 121.

- Organizar esfuerzos de GC más proactivos para intentar disminuir la probabilidad de crisis.
- Desarrollar procesos de aprendizaje organizacional relativo a la GC.
- Elaborar un listado de contactos clave.
- Determinar las capacidades de emergencia en la organización y el vecindario
- Promover que el equipo sea multidiciplinario.
- Liderar y supervisar la implementación del programa de GC.
- Fomentar la cultura de prevención, entre otras.

El personal de la línea de producción debe ser partícipe en la implementación de los esfuerzos de GC, ya que están en mejor posición para percibir o contener una crisis, por lo que deben estar debidamente entrenados.

Cada miembro del EGC contribuirá con su habilidad y capacidad al equipo, lo cual mejorará a su vez la competencia y capacidad del grupo. La habilidad organizacional (trabajo en equipo, liderazgo, comunicación) es la base sobre la cual se construyen otras habilidades.

Cuando un evento de crisis se materialice, el EGC debe reunirse a la brevedad posible, esto presupone que los miembros del equipo puedan ser localizados a cualquier hora del día, los 365 días del año, y cada uno debe tener un suplente o reemplazo permanente. Una buena recomendación es tener un solo portavoz, su labor será la comunicación efectiva con los grupos de interés clave tanto internos como externos.

En las empresas pequeñas resulta complicado mantener una unidad de GC por el costo que esto implica, por lo que estas responsabilidades se incluyen en las de los empleados. En estos casos se forma un comité, que mediante reuniones periódicas deben vigilar el cumplimiento del programa de GC.

3.5.2 EVALUACIÓN

Las actividades involucradas son: El diagnóstico de la situación actual y la evaluación de los tipos de crisis potenciales(riesgos).

a) Diagnóstico de la preparación organizacional

Para llevar a cabo el proceso de diagnóstico, empleamos las herramientas descritas en la sección 3.3, que no son más que cuestionarios que nos permiten conocer la importancia que la organización da actualmente a la GC, y más específicamente respecto a cada uno de los factores. En base, a las respuestas (afirmativas) y las puntuaciones obtenidas se elaboran los diagramas de barras por factor para obtener un valor promedio de cada uno, los cuales a su vez nos permiten elaborar el perfil de crisis(sección 3.4), para determinar los puntos fuertes y débiles ante crisis, o dicho de otra manera nos muestra la preparación y la vulnerabilidad de la organización. También podemos averiguar en que etapa de preparación se encuentra actualmente la organización, según se cumpla o no con los requisitos mencionados en la sección 3.4.1.

b) Evaluación de los tipos de crisis potenciales

En este proceso están inmersos dos tareas principales: la identificación y la valoración.

Para la *identificación* de los tipos de crisis potenciales a los que se encuentra expuesta la organización, se sugiere hacer uso de los resultados obtenidos en la herramienta de Diagnóstico para Tipos (Ver Anexo1), mediante el cual es posible determinar los tipos de crisis potenciales a los cuales la organización podría estar expuesta.

Una vez identificados los tipos de crisis potenciales, es necesario realizar la *valoración* (priorizarlos), para dar tratamiento en primer lugar a los tipos que puedan afectar en mayor medida a los procesos críticos de la organización y poner en riesgo su continuidad. Este proceso es posible realizarlo de manera subjetiva en base a datos históricos registrados(por la empresa o el sector de la industria), o en base a un análisis de impacto al negocio.

La participación de los dueños de los procesos y/o aquellas personas que tengan un conocimiento global del negocio, puede facilitar el proceso de priorización de los riesgos; al conseguir su participación y distribuir la responsabilidad, se logra elaborar e implementar un programa de GC de mejor calidad, esto debido a que los mismos dueños de los procesos son quienes definen, documentan y prueban sus procedimientos de contingencia.

Como se habrá notado, no se hace mención al uso de ningún método en especial, en la identificación de los tipos de crisis potenciales. En lo que se refiere a la priorización de los riesgos, Mitroff, no facilita ninguna herramienta para su análisis, por lo que, se sugiere al lector complementar su estudio con la revisión de la sección Administración de Riesgos del capitulo dos y la bibliografía relacionada, en especial en el tema Evaluación (identificación y valoración) de riesgos, para obtener mejores resultados. La evaluación debe reforzarse con la revisión de las recomendaciones desarrollados en los diferentes estándares dependiendo de la naturaleza del riesgo.

3.5.3 ELABORACIÓN DEL PROGRAMA DE GC

Luego de identificar los tipos de crisis potenciales que pueden afectar la organización, se determina las acciones a tomar para prevenir, mitigar y restaurar el/los proceso(s) afectado(s), mediante el desarrollo de procedimientos que cubran todas las fases por las cuales un tipo de crisis específico atraviesa.

Para la fase ANTES(PRE-CRISIS) se definen las acciones preventivas a ser ejecutadas para evitar que un tipo de crisis potencial se materialice.

Una herramienta valiosa para llevar a cabo esta tarea es la herramienta de diagnóstico “Tipos-acciones preventivas” (Ver Anexo 1). Esta herramienta, pone en evidencia las acciones preventivas que están siendo o no tomadas en cuenta actualmente por la organización. Con ello se procede a elaborar las acciones necesarias para el tratamiento de los tipos de crisis potenciales identificados, con el afán de disminuir su vulnerabilidad o en su defecto reducir el impacto.

Dada la extensión de las responsabilidades de un auditor en la actualidad, la auditoría es de gran ayuda para identificar posibles fallas en los controles implementados y para la identificación temprana de posibles fuentes de crisis.

Para la fase DURANTE(CRISIS)[4] se define las acciones reactivas para el tratamiento oportuno de un tipo de crisis en curso, con ello se pretende contener y minimizar los efectos causados por un evento que se ha materializado.
Durante la crisis, diversas actividades deben desarrollarse de manera simultanea, así las principales actividades de los responsables de su gestión, será la de recoger la información, realizar el análisis, controlar los daños y realizar una comunicación eficiente.

- Recogida de datos, la finalidad es evaluar los daños, el medio ambiente, las instalaciones del negocio.
- Análisis, es necesario descubrir la causa de la crisis, para ello se debe averiguar:
  ¿Fue la crisis debida a un defecto en las tecnologías centrales?.
  ¿Por falta de información?
  ¿Por error humano?
  ¿Que papel jugaron los factores humanos?
  ¿Contribuyó la estructura de la organización a la crisis por una falla en la comunicación, los roles, la autoridad o las estructuras de gratificación?
- Debe descubrirse cual es la crisis y que la ocasionó, caso contrario los mecanismos de *contención de daños* puede activarse y originar nuevas crisis.
- Comunicación, el EGC debe ser comunicado y reunido para tratar la crisis ante las primeras señales, esto presupone que los miembros estarán disponibles a toda hora y podrán ser localizados fácilmente. También pueden ser avisados otros grupos de interés dependiendo de la naturaleza de la crisis.

[4] Mitroff I. y C. Pearson. (2000). Cómo Gestionar una Crisis. Barcelona : Gestión 2000. pp. 107-110.

Es recomendable que haya un sólo portavoz quien debe comunicarse de manera efectiva con los grupos de interés clave. La credibilidad del portavoz es muy importante más que conocer los datos o la verdad en medio de cualquier crisis.

Para la fase DESPUES(POST-CRISIS) se define las acciones de recuperación y restauración que posibiliten la continuidad del negocio, posterior a un evento de crisis. En general, para esta fase se elaboran los procedimientos necesarios para restablecer el proceso afectado luego de una interrupción.
Para ejemplificar podemos mencionar, el caso de la interrupción de un equipo de servidor de archivos, que mientras no se restablezca, los usuarios estarán inhabilitados de aplicar dichos archivos. Si la organización estuvo preparada para este tipo de crisis, tomará las acciones pertinentes de manera inmediata para restablecerlo en el menor tiempo posible, siguiendo el procedimiento elaborado para el efecto.

No esta por demás manifestar, que será de utilidad la revisión de la sección Continuidad del Negocio del capitulo dos, para complementar el conocimiento acerca de las actividades involucradas en este proceso.
Luego que un evento de crisis ha sido mitigado y se ha recuperado la normalidad, es necesario cerrarlo mediante el registro en un documento, el tratamiento brindado y toda la información relacionada. La documentación de estos hechos contribuye al aprendizaje de la organización, ya sea, para mejorar la intervención en crisis futuras o tratar de evitarlas.

Como hemos mencionado, es posible alcanzar un grado aceptable de preparación ante la crisis, partiendo de la gestión de los tipos que pueden afectar a los procesos críticos de la organización. Sin embargo, vale la pena recordar la recomendación de Mitroff, de que para distribuir de forma regular el riesgo y la preparación de la organización, se planifique al menos una crisis potencial de cada familia y se adopte al menos una acción preventiva de cada familia de acciones preventivas.

Aún cuando los parámetros RTO y RPO descritos en la sección 2.2.3, son actualmente más utilizados en la recuperación de sistemas informáticos, no quita la posibilidad de ser considerados en la gestión de otros eventos de crisis, por lo que deben ser tomados en cuenta al definir las estrategias, ya que en cierta medida ellos determinan el margen de tiempo en que un proceso puede permanecer interrumpido sin sufrir graves daños.
Al final de este proceso se debe tener identificado las acciones y los recursos necesarios para dar tratamiento a los riesgos potenciales en sus diferentes fases.

3.5.4 IMPLEMENTACIÓN DEL PROGRAMA DE GC

Los responsables de llevar a efecto esta tarea son las mismas personas que participaron en la elaboración de los planes con la coordinación y supervisión del comité o equipo de GC.

Primero, es necesario emprender un plan de capacitación respecto a la implementación del programa, difundiendo los objetivos que se procura alcanzar, de manera que todos los miembros de la organización se encuentren comprometidos con este propósito.

Los principales actores en este proceso, son las personas claves involucradas con los procesos que permitieron identificar un tipo de crisis potencial.
Mediante el entrenamiento continuo, se crea conciencia respecto a la importancia de la cultura de prevención, para que se incorpore a la cultura corporativa. De igual manera hay que definir los mecanismos de seguimiento y control al programa de GC implementado. Una vez implementado el programa se debe realizar todas las pruebas necesarias, para determinar su efectividad.

Se recomienda tener un documento principal para el registro de información clave y común para los tipos de crisis y hacer referencia de las acciones de tratamiento de riesgos individuales, esto facilitará su mantenimiento. Se sugiere usar el documento Planificación de la Gestión de Crisis y Continuidad del Negocio(ver Anexo1), como documento principal, publicado por el U.S. Department Homeland

Security[71] (Departamento de Seguridad Nacional), para resaltar precisamente la amplitud de un programa de continuidad organizacional. El documento se puede comenzar a llenar en la etapa de elaboración del programa de GC con los datos disponibles y terminarlo en la etapa de implementación.

Analizando brevemente el contenido del documento, observamos que en su primer bloque contiene información relevante de la compañía, el lugar de operación normal, datos del lugar alternativo en caso de algún desastre así como las personas responsables de gestionar una crisis. A continuación encontramos información de contactos en caso de emergencia tales como 911, policía, bomberos, etc. En otro bloque se observa un cuadro destinado para registrar los riesgos potenciales(naturales y causados por el hombre) que pueden afectar al negocio.

Seguidamente hay un espacio para registrar los miembros del EGC, personas de negocios vecinos, proveedores principales y alternativos. Se registra también un plan de evacuación, la manera en que serán contactados los empleados en caso de desastres, la localización de copias de seguridad de archivos y documentos importantes, y la periodicidad de revisión del plan.

3.5.5 APRENDIZAJE Y MEJORA CONTINUA

El proceso de aprendizaje está presente en todas las fases, por lo tanto es de esperar que con el tiempo, las habilidades del EGC y el de toda la organización mejore. El aprender de experiencias ajenas especialmente de empresas que tienen un objetivo semejante(empresas del mismo sector) es muy importante.

Se conseguirá la mejora continua siempre y cuando se realice un adecuado seguimiento y control a este proceso de gestión; la efectividad de la labor realizada cuando el negocio estuvo en su estado de normalidad se lo comprueba cuando tenga que hacer frente a un evento adverso.

---

[71] www.ready.gov. Sample Business Continuity and Disaster Preparedness Plan, p.1-7 http://www.ready.gov/america/_downloads/sampleplan.pdf

Una de las principales actividades en esta etapa es la revisión y actualización del programa de gestión de crisis de acuerdo a los cambios en el entorno organizacional, tales como nueva legislación vigente, requerimientos regulatorios, cambios tecnológicos, rotación de personal, resultados de pruebas, etc.

La entidad individual u organizacional responsable del liderazgo y gestión de un programa de GC, requerirá de ciertas competencias (conocimientos, habilidades) y soporte de continuidad organizacional para asumir esas responsabilidades; algunas de ellas se han descrito en el capítulo uno. Conforme la organización vaya mejorando sus habilidades relacionadas a la GC, se incorporarán nuevos tipos de crisis para su gestión, y así el programa actual irá perfeccionándose progresivamente.

Se concluye la presente propuesta realizando una comparación de algunos aspectos, respecto a la propuesta de Mitroff.

CUADRO 3.1 CUADRO COMPARATIVO

Propuesta de Mitroff	**Propuesta del Autor**
Enfasis en elaborar el programa de GC a partir de las familias de crisis y de las familias de prevención.	Enfasis en elaborar un programa de GC a partir de identificar el proceso crítico dentro de la cadena de valor.
Un programa de GC se considera razonablemente efectivo, si da tratamiento al menos a un riesgo de cada familia y se elabore al menos una acción preventiva de cada familia.	Un programa de GC se considera razonablemente efectivo, si se elabora progresivamente hasta llegar a dar tratamiento a todos los riesgos considerados críticos para la empresa.
Orientado a dar atención a la mayor cantidad de tipos de crisis posibles.	Orientado a garantizar en cierta medida la continuidad del negocio.
Modelo gráfico no incluye la continuidad.	Modelo gráfico incluye la continuidad.

Hay que tener presente que el proceso de GC no termina con la implementación, más bien es el comienzo de la verdadera gestión.

CAPITULO 4

CASO PRACTICO

4.1 ANTECEDENTES

Por motivos de confidencialidad y debido a que el tratamiento y divulgación de ciertos aspectos podría afectar negativamente a la organización, el nombre de la compañía no será revelado, y para referirnos a ella se utilizará el nombre genérico de empresa “Tecnológica”. En razón de que la finalidad del caso práctico, es demostrar la aplicabilidad del modelo de GC propuesto, nos concentraremos en el proceso considerado como el más crítico para la compañía.

La organización a la cual se aplicará el modelo de GC propuesto, es una empresa de servicios cuyo negocio gira alrededor de las tecnologías de la información. La misma esta radicada en la ciudad de Quito desde 1993, su actividad principal se concentra en el desarrollo, diseño, integración y comercialización de Sistemas Inteligentes al servicio del sector de la transportación y afines (ITS). Algunos aspectos que caracterizan a este tipo de empresas hemos descrito en las secciones 1.4 y 1.6.

Vale la pena señalar también que la empresa posee una certificación ISO 9001:2000 obtenida en el 2003, de cuyo Manual de Calidad extraeremos la información referente a los procesos.

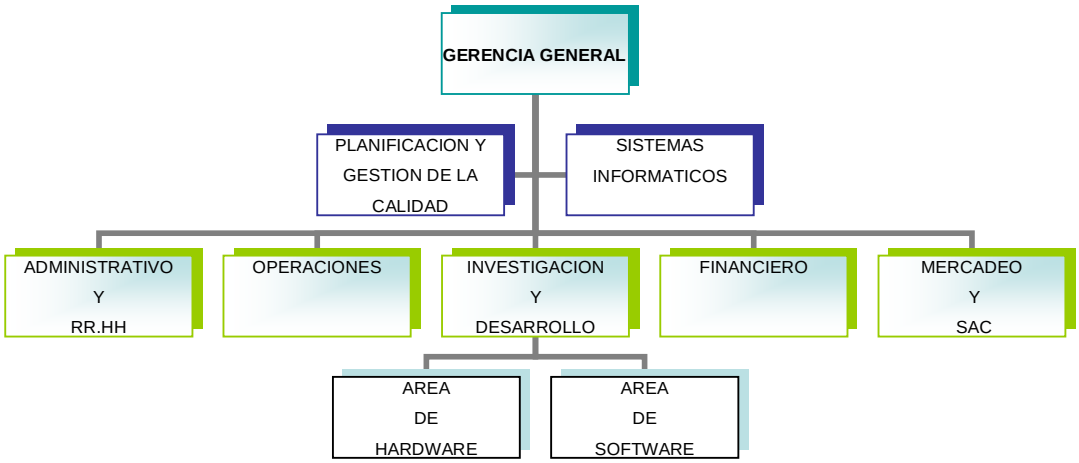
A continuación se describe la misión de la empresa:

Misión

Proveer soluciones, servicio y asesoría al sector de la transportación y áreas afines mediante la investigación y desarrollo de tecnologías basada en el estudio de mercado y bajo esquemas de mutuo beneficios.

ORGANIGRAMA

FIGURA 4.1 ORGANIGRAMA EMPRESA TECNOLOGICA



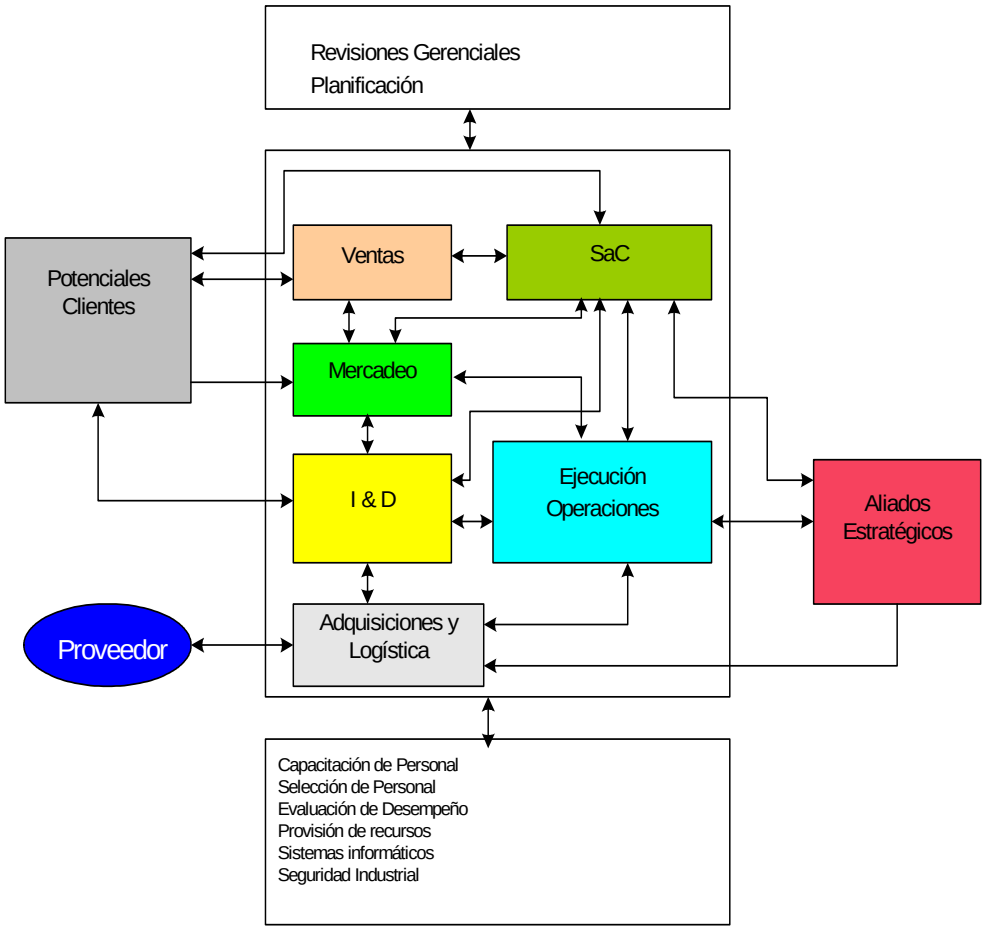
Este organigrama es un aproximado a lo que es en la realidad, por tanto válido para nuestro caso de estudio, en él podemos apreciar a más de las unidades que son comunes a la mayoría de las organizaciones, la unidad de Investigación y Desarrollo(I&D) la cual esta compuesta de dos áreas claramente identificados como Area de Software y Area de Hardware, que tiene la finalidad de denotar las habilidades más destacables de cada una o su nivel de especialización, ya que en la práctica estas son complementarias en esta organización.

De manera general podemos mencionar que el negocio de la empresa gira en torno al proceso I&D y a los productos que éste desarrolla, da mantenimiento y brinda soporte de último nivel a los demás departamentos. Este departamento está conformado por profesionales Ingenieros en Sistemas y Electrónicos.

Los riesgos que amenazan a la empresa, son propios de este tipo de organizaciones(innovadoras), donde su factor de producción radica en las habilidades y conocimiento de sus empleados. Al mismo tiempo, es altamente dependiente de la tecnología, por lo que se requiere frecuentemente la capacitación en nuevas tecnologías(dependencia del conocimiento).

En el gráfico a continuación, observamos el diagrama de procesos que es también parte del Manual de Calidad:

FIGURA 4.2 DIAGRAMA DE PROCESOS DE LA COMPAÑÍA TECNOLOGICA



En el gráfico podemos observar los procesos que son considerados parte de la cadena de valor: Negocios(Mercadeo y Ventas), Servicio al cliente, Operaciones, I&D y Adquisiciones y logística. En la parte inferior se encuentran algunos procesos de soporte. Algunas de las tareas más críticas de la empresa están asignadas al área de Investigación y Desarrollo, la que tiene a su cargo el diseño y desarrollo de los productos tecnológicos(software, hardware y/o su integración),

el mantenimiento del sistema de fidelidad de clientes y el monitoreo del centro de cómputo. Las responsabilidades están distribuidas entre sus miembros.

Productos y Servicios

- Sistema de fidelidad.
- Aplicación para la facturación automática en estaciones de servicios.
- Oros.

Podemos decir que el principal servicio que ofrece la compañía es el Sistema de fidelidad, el cual permite gestionar el abastecimiento de combustible de flotas de vehículos, en una red de estaciones de servicio que están distribuidas estratégicamente en la ciudad de Quito. Para obtener el beneficio los vehículos, cuentan con un dispositivo electrónico el cual permite llevar el control de cada carga de combustible. Terminado el abastecimiento, la transacción se registra en una base de datos en la estación. Diariamente la información recopilada en las estaciones es centralizada en la compañía, para el monitoreo de los cupos asignados a cada vehículo y para permitir el acceso a los clientes a consultar el estado de los vehículos de su flota, a través del Internet.

En este proceso están presentes varios componentes tecnológicos: los dispositivos de comunicación, la red local, las aplicaciones de software, entre otros, de los cuales se espera su disponibilidad continua para brindar el servicio contratado por los clientes. La falla de uno de los componentes o sus partes pondría en grandes apuros a la operación del sistema.

De igual manera, para su administración se requiere que los responsables de este proceso tengan amplios conocimientos de administración de base de datos, de comunicaciones y configuración de equipos, para tomar acciones de prevención y llevar adelante el monitoreo constante de la disponibilidad del sistema.

4.1.1 CONFORMACIÓN DEL EGC

Como se manifestó en el capitulo anterior, el éxito del desarrollo de un programa de GC y su implementación depende en gran medida del apoyo y la participación de la alta gerencia de la organización. En nuestro caso por la relación laboral que el autor de la presente investigación mantiene con la empresa en estudio, se consiguió la apertura de la gerencia administrativa.

Para comenzar se dispuso la conformación de un Comité de GC, que inicialmente estuvo conformado por representantes de la parte administrativa y de la parte técnica. Estas personas compartirán sus responsabilidades diarias con las del comité.

Conforme el proceso metodológico propuesto para elaborar un programa de GC; se procedió a definir el objetivo:
El objetivo general de emprender la elaboración de un programa Gestión de Crisis en la empresa, es el de determinar y dar tratamiento integral a los principales riesgos a los que se encuentra expuesto la organización, que permita garantizar en cierta medida la continuidad del negocio.

En este sentido, se ha sugerido modificar el enunciado de la misión empresarial, de la siguiente manera:

Misión (modificada)
Proveer soluciones, servicio y asesoría continua al sector de la transportación y áreas afines mediante la investigación y desarrollo de tecnologías basada en el estudio de mercado y bajo esquemas de mutuo beneficios que garanticen la sostenibilidad de la empresa.

4.2 DIAGNÓSTICO DE LA PREPARACIÓN ORGANIZACIONAL ANTE LA CRISIS

El desarrollo de este punto, es parte de la etapa Evaluación, dentro del proceso de Planificación de GC, una vez conformado el equipo o comité.

En este proceso realizamos el diagnóstico de toda la empresa, para lo cual utilizamos las herramientas de diagnóstico para cada uno de los factores(Tipos, Fases, Sistemas y Grupos de interés) mencionadas en la sección 3.3 del capitulo anterior. Esto nos va a permitir tener una idea general en cuanto a su preparación y de los esfuerzos que en este sentido realiza la organización actualmente.

Para los fines del presente trabajo, esta actividad se llevó a cabo con la participación de los representantes de las áreas más representativas de la compañía, ellos son: un representante del área administrativa y dos del área técnica(hardware, software), cuyos criterios tienen mayor peso dentro de la compañía, la misma que esta conformada por menos de 20 personas. Estos representantes tienen un amplio conocimiento del negocio y son los que tienen mayor experiencia en sus respectivas áreas y han colaborado en el llenado de los formularios que comprenden las herramientas de diagnóstico.

A continuación los resultados obtenidos del diagnóstico. Comenzamos analizando los resultados del Factor Tipos, sobre la base del siguiente cuestionario:

HERRAMIENTA DE DIAGNOSTICO PARA TIPOS-CRISIS

¿Planifica su organización los siguientes puntos?

		SI	NO
A	**Ataques económicos externos**		
	Extorsión		X
	Soborno		X
	Boicot		X
	Opas(Oferta pública de acciones)		X
B	**Ataques informativos externos**		
	Violación de copyright	X	
	Perdida de información	X	
	Falsificación		X
	Rumores dañinos		X
C	**Averías**		
	Avisos y reclamaciones	X	
	Fallos en el producto	X	
	Fallos en las plantas		X
	Averías informáticas	X	
	Operario deficiente/errores de operario		X
	Seguridad deficiente		X
D	**Catástrofes**		
	Daños medioambientales		X
	Accidentes importantes		X
E	**Psicopatología**		
	Terrorismo		X
	Imitadores		X
	Alteración/sabotaje in situ		X
	Alteración/sabotaje externo		X
	Rapto de ejecutivos		X
	Acoso sexual		X
	Rumores dañinos		X
F	**Factores Sanitarios**		
	Enfermedades ocupacionales	X	
G	**Factores de Imagen**		
	Daños a la reputación		X
	Rumores	X	
H	**Factores de Recursos Humanos**		
	Sustitución de ejecutivos		X
	Moral deficiente		X
NUMERO TOTAL DE RESPUESTAS SI Y NO		**7**	**21**

En este caso vemos que la compañía no ha tomado conciencia de las potenciales crisis de la categoría A (Ataques económicos externos). Por la actividad de la empresa observamos que si ha puesto atención en cambio en la seguridad de la información y la propiedad intelectual.

En lo que respecta a la categoría C, vemos que existen los procedimientos para dar tratamiento a las reclamaciones, a las fallas en los productos o a los errores de operarios.

En cuanto a los tipos de crisis de la categoría de D, la empresa no ha planificado para enfrentar desastres naturales, únicamente existe una limitada preparación para enfrentar un siniestro importante(incendio). La empresa no ha considerado o desconoce las crisis potenciales de la categoría E(Psicopatología).

En cambio, si ha prestado atención a las enfermedades ocupacionales(categoría F). En cuanto a los factores de imagen existe cierto descuido ya que no existen procedimientos formales para enfrentarlo.

Se ha descuidado al recurso humano al no planificar formalmente la sustitución o abandono de personal clave, de igual manera no se realiza un diagnóstico periódico de la moral de los empleados.

Finalmente se totaliza las respuestas afirmativas y negativas; más adelante el valor obtenido por las respuestas afirmativas se representará en un diagrama de barras.

En general, en cuanto al Factor Tipos vemos que la organización no ha sido consciente de la existencia de otros tipos de riesgos(extorsión, rumores, daños a la reputación, moral deficiente, etc.) que pueden afectar de manera negativa sus actividades diarias.

Enseguida, veamos los resultados del cuestionario Tipos-acciones preventivas.

HERRAMIENTA DIAGNÓSTICA TIPOS-ACCIONES PREVENTIVAS

	SI	NO
A Actividades estratégicas		
La filosofía corporativa apoya la GC		X
La GC está integrada en las nociones y declaraciones de excelencia corporativa		X
La GC está integrada en procesos de planificación estratégica		X
Se incluye a personas de fuera de la organización en el equipo de GC		X
Entrenamiento y cursillos de GC		X
Simulaciones de crisis		X
Estrategias de diversificación y de cartera para la GC.	X	
SUBTOTAL	1	6
B Actividades técnicas y estructurales		
Creación de un equipo o unidad de GC		X
Creación de un presupuesto para la GC		X
Actualización y desarrollo continuo de manuales y políticas de emergencia	X	
Inventario informatizados de empleados, plantas, productos y aptitudes	X	
Creación de una sala o unas instalaciones estratégicas de emergencia		X
Reducción de productos, servicios y procesos de producción peligrosos	X	
Mejoras en el diseño y en la seguridad global del producto y de la producción	X	
Redundancia tecnológica(copias de seguridad informáticas)	X	
Contratación de expertos y servicios de GC externos		X
SUBTOTAL	5	4
C Actividades de evaluación y diagnóstico		
Auditorias legales y financieras de amenazas y responsabilidades		X
Modificaciones en la cobertura del seguro		X
Auditorías de impacto medioambiental		X
Priorización de las actividades más críticas necesarias para la operaciones diarias	X	

Detección de señales de advertencia temprana, revisiones, gestión de problemas		X
Investigación exclusiva de peligros potenciales ocultos		X
Seguimiento crítico de crisis pasadas		X
Programas estrictos de inspección y mantenimiento		X
SUBTOTAL	1	7

D **Actividades de comunicación**

Entrenamiento los medios de comunicación para la GC		X
Esfuerzos importantes en relaciones públicas	X	
Aumento de la información a la población local		X
Potenciación de las relaciones con grupos de interés(policía, medios)		X
Potenciación de la colaboración entre grupos de interés	X	
Uso de los nuevos canales y tecnologías de comunicación	X	
Números de teléfono dedicados a avisos y reclamaciones de los clientes	X	
SUBTOTAL	4	3

En este caso observamos, que prácticamente la organización no ha tomado conciencia todavía de la necesidad de incorporar la GC a los procesos de planificación estratégica.

La empresa cumple con ciertas actividades de la categoría B(Actividades técnicas y estructurales), sin embargo, se ha dado más por la exigencia de formalizar ciertos procesos relacionados con el Sistema de Gestión de Calidad ISO 9001, y no porque exista una responsabilidad formal asignada para este propósito, como un equipo o comité de GC; tampoco existe un presupuesto asignado para lo que es la gestión de la continuidad organizacional.

En cuanto a los ítems de la categoría C(Actividades de evaluación y diagnóstico), si bien existen ciertos procedimientos de evaluación y diagnóstico, éstos no son formales. En cuanto a las actividades de comunicación(categoría D), se han establecido procedimientos para las relaciones con los proveedores y clientes

principalmente, pero hay que trabajar más en las relaciones con otros grupos de interés. Respecto a la categoría E(actividades psicológicas y culturales), al no existir conciencia, de la GC sobre todo por su desconocimiento, no se ha prestado atención a los impactos emocionales que pueden causar o afectar una situación de crisis.

Revisemos a continuación los resultados de la herramienta de diagnóstico para el factor Fases, el cual se lo puede encontrar en el Anexo 2(Herramientas de diagnóstico FASES), sobre el cual realizamos un breve análisis.
Observamos que en la sub-fase detección de señales tempranas, existe poca preparación, únicamente a través de procedimientos no formales, debido básicamente a la falta de conciencia, por tal motivo, los procedimientos implementados en la preparación/prevención son escasos y poco efectivos al no aplicarlos regularmente.

En cuanto a la contención y limitación de daños, se depende del conocimiento y la habilidad de los dueños de los procesos, ya que no existen procedimientos formales y tampoco se ha emprendido una capacitación en este sentido.
En la sub-fase de recuperación, actualmente se centra básicamente en la recuperación de la información de base de datos, para ello se cuenta con backups de los mismos, sin embargo este procedimiento esta incompleto ya que no se lleva a cabo pruebas y simulacros de recuperación de manera periódica.
Existe cierta conciencia individual acerca de crisis pasadas, mas no una conciencia organizacional, principalmente por falta de conocimiento sobre la GC como se ha manifestado.

De manera general, podemos citar que prácticamente la cultura de prevención es inexistente. Al no contar formalmente con un equipo o comité de gestión crisis, no se han elaborado planes para enfrentar una situación adversa en cada una de sus fases(antes, durante y después), sólo existen esporádicos procedimientos independientes, de prevención y recuperación del servicio principal.

Los resultados del cuestionario de diagnóstico del Factor Sistemas podemos revisarlo en el Anexo 2(Herramienta diagnóstica SISTEMAS), del cual realizamos un análisis a continuación.

Observamos que al no ser la GC formalmente parte de las estrategias del negocio, se ha descuidado diferentes actividades que podrían contribuir en la gestión de crisis potenciales.
Así tenemos que en la categoría A(Sistema técnico), existen procedimientos básicos para el mantenimiento de los equipos de cómputo pero no existe un procedimiento formal de análisis de riesgos. Al no existir conciencia en cuanto a la GC la mayoría de las actividades comprendidas dentro de la categoría B(Sistemas de infraestructura) son esporádicas o inexistentes.

Dentro de la categoría C(Sistemas de factores humanos), aun cuando ciertas actividades no están formalizados como parte de un programa de continuidad organizacional, si lo están dentro del sistema de gestión de calidad, por eso vemos que la mayoría de las actividades se están llevando a cabo, aunque no ha plenitud. En cuanto a la categoría D(Sistema de cultura parte 1), se observa que la comunicación entre los diferentes niveles se da de buena manera, las prácticas de seguridad se concentran en la parte tecnológica y se descuida la parte humana al no evaluar periódicamente la moral de los empleados.
Respecto al Sistema emocional(categoría F), al haber sido la GC un tema desconocido en la organización, no se ha prestado atención al hecho de que la crisis influye en la parte emocional de los empleados y que debe ser tratado adecuadamente, esto se ve reflejado en la baja puntuación.

Finalmente, tenemos los resultados del diagnóstico del Factor Grupos de Interés en el Anexo 2(Herramienta diagnóstica para grupos de interés), del cual podemos decir que, evidentemente por la ausencia de políticas de GC en la compañía en estudio, la composición de los stakeholders (grupos de interés) reconocidos se reduce únicamente a los clientes, proveedores y empleados. De igual manera son pocos los stakeholders que de una u otra manera han colaborado en la elaboración de acciones de tratamiento de ciertos riesgos.

En este contexto la preparación de la organización ante la crisis, se encuentra en la etapa más baja, por lo que hay mucho esfuerzo por realizar en este tema, empezando por crear interés en todos sus miembros.

4.3 ELABORACIÓN DEL PERFIL DE CRISIS

Para elaborar el perfil de crisis, hacemos uso de las herramientas gráficas descritas en la sección 3.4**,** los cuales nos permiten representar en las barras correspondientes, las puntuaciones obtenidas en los cuestionarios de cada uno los factores. Esto es un complemento al análisis de los resultados del diagnóstico, el cual facilita una interpretación gráfica de la preparación de la organización. Para el efecto, cada factor se representa en su propia escala y luego el promedio de cada uno será llevado a una escala semejante para obtener el perfil de crisis de la organización.

Comencemos revisando la representación gráfica de diagnóstico del Factor Tipos(Figura 4.4), ésta tiene una barra para cada cuestionario de Tipos(crisis y acciones preventivas), en el diagrama observamos más claramente las deficiencias encontradas y descritas en la sección anterior. Debido a que su puntuación promedio esta situada por debajo del nivel Moderada, lo cual según Mitroff, significa que la organización está en la zona de peligro en cuanto a la preparación ante crisis, respecto a este factor.

En la Figura 4.5, tenemos la representación gráfica de diagnóstico del Factor Fases, observamos que las sub-fases: detección de señales y recuperación, tienen una puntuación superior, debido a que existen ciertas actividades encaminadas con esos propósitos, sin embargo de aquello no es suficiente para llevar una adecuada gestión de crisis, esto se refleja en que la puntuación está por debajo del nivel de preparación Moderada, lo cual significa que se encuentra en la zona de peligro, en lo que respecta este factor.

FIGURA 4.4 DIAGRAMA DE BARRAS PARA TIPOS

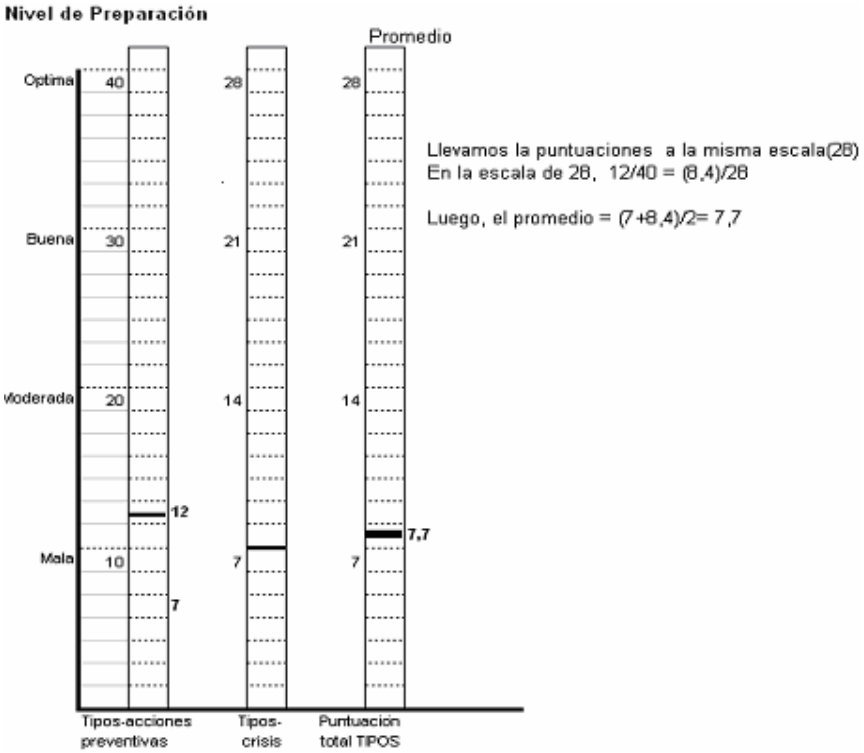
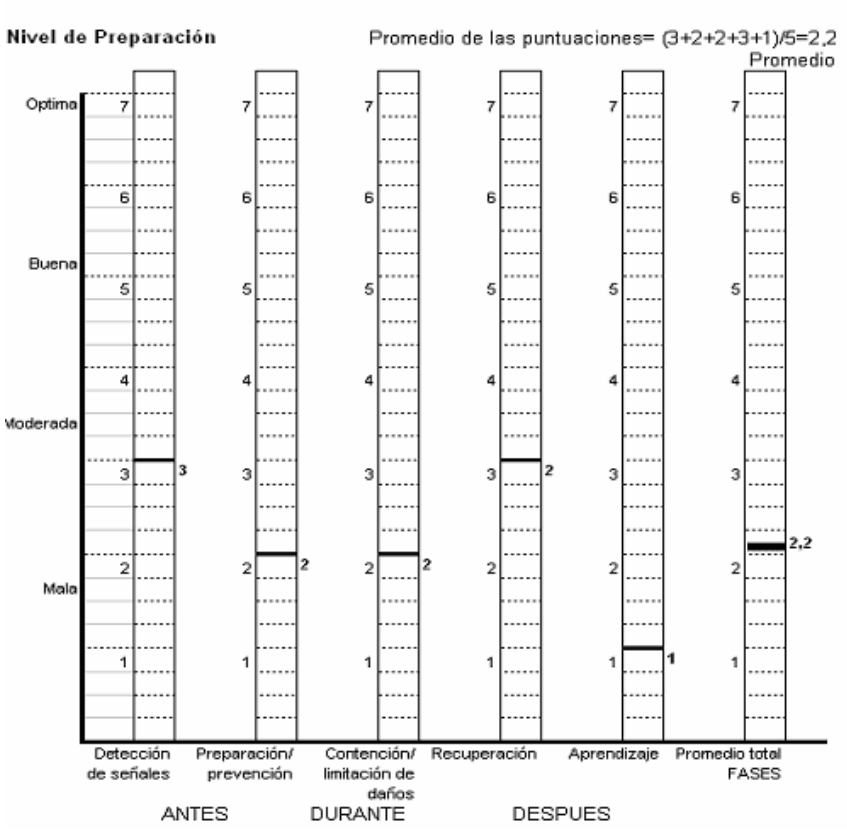
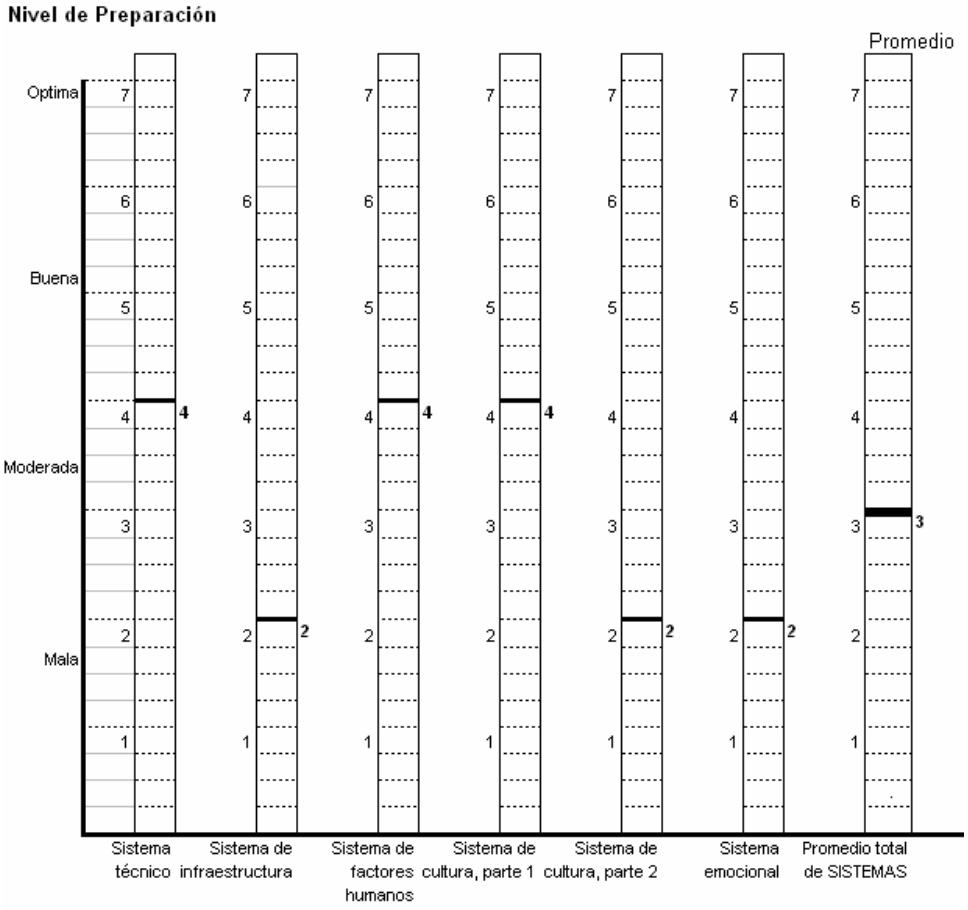


FIGURA 4.5 DIAGRAMA DE BARRAS PARA FASES



En la representación gráfica del diagnóstico del Factor Sistemas(Figura 4.6), observamos que en las categorías de Sistemas: técnico, de factores humanos y de cultura(parte1), sus puntuaciones han sobrepasado el nivel Moderado levemente, pero aun están por debajo del nivel Bueno. Las demás categorías como podemos apreciar están cerca del nivel de preparación Mala, por lo que su promedio esta por debajo del nivel de preparación Moderada, es decir en la zona de peligro.

FIGURA 4.6 DIAGRAMA DE BARRAS PARA SISTEMAS

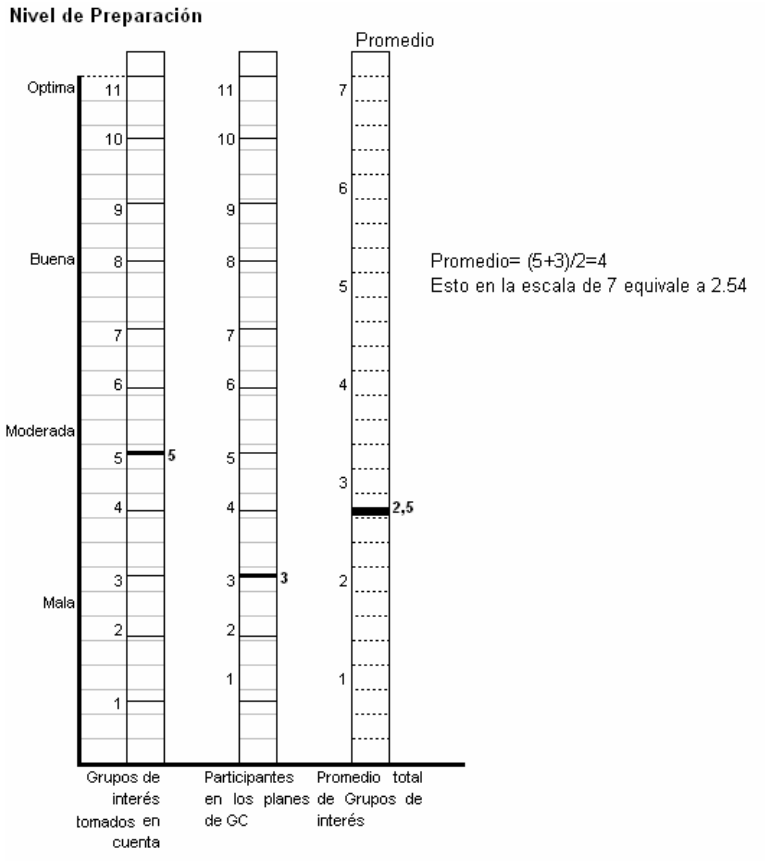


Promedio de puntuaciones: (4+2+4+4+2+2)/6=3

En la representación gráfica para el factor Grupos de interés(Figura 4.7), observamos que las puntuaciones de las categorías: Grupos de interés tomados en cuenta y Participantes en la elaboración de la GC, están por debajo del nivel

de preparación Moderada, al igual que su Promedio, en este sentido la preparación de la organización respecto a este factor se encuentra también en la zona de peligro.

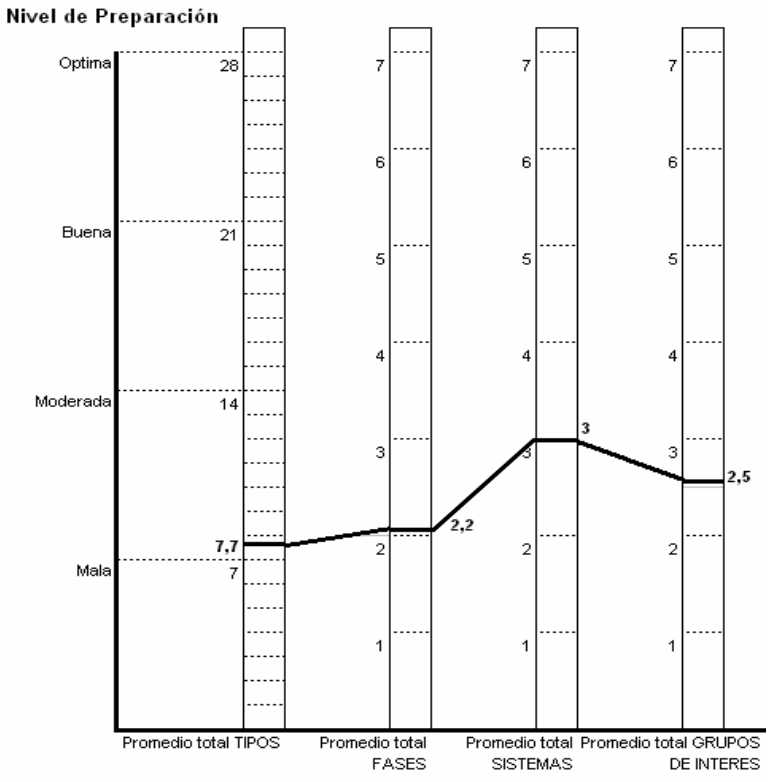
FIGURA 4.7 DIAGRAMA DE BARRAS PARA GRUPOS DE INTERES



Ahora los valores promedio de los factores, los trasladamos a la gráfica de barras en escalas semejantes(Figura 4.8). Al unir las puntuaciones de los factores, obtenemos como resultado una gráfica lineal, a esta representación Mitroff lo ha denominado “Perfil de crisis” de la organización, el cual nos permite realizar una interpretación de la preparación respecto a los cuatro factores.

En nuestro caso mediante el diagrama, podemos deducir lo siguiente: los factores menos atendidos son Tipos y Fases, y los más atendidos Sistemas y Grupos de Interés, sin embargo, no alcanzan el nivel de preparación Moderada.

FIGURA 4.8 PERFIL DE GESTION DE CRISIS



Para el presente caso podemos concluir manifestando, que las puntuaciones se encuentran localizados en una zona de peligro(Bajo la preparación Moderada), esto significa que la organización no se encuentra lo suficientemente preparada para afrontar de manera adecuada una situación adversa que se pudiera presentar, lo cual le puede acarrear grandes pérdidas(económicas, de imagen, etc.) si no se toman acciones para remediarlo.

La empresa, por su actividad relacionada con la tecnología de la información, ha tomado conciencia en cierta medida, únicamente de ciertos riesgos tecnológicos de manera parcial, pero ha descuidando otros aspectos tales como la gestión del conocimiento, la moral de los empleados, la reputación, entre otros.

La aseveración anterior podría justificarse, debido a que no ha existido anteriormente conciencia respecto al tema ni una responsabilidad asignada, por tal motivo existen esfuerzos aislados para enfrentar riesgos específicos, que generalmente son los más visibles. Por ello es necesario identificar y gestionar los

diversos tipos de crisis(riesgos) que podrían afectar la normal operación de la organización o poner en peligro su existencia.

Como se habrá notado, no hemos encontrado esfuerzos para gestionar la continuidad organizacional, básicamente por su desconocimiento, por tal motivo recomendamos emprender jornadas de capacitación antes de la implementación, para conseguir involucrar a todo el personal en este proceso y obtener mejores resultados.

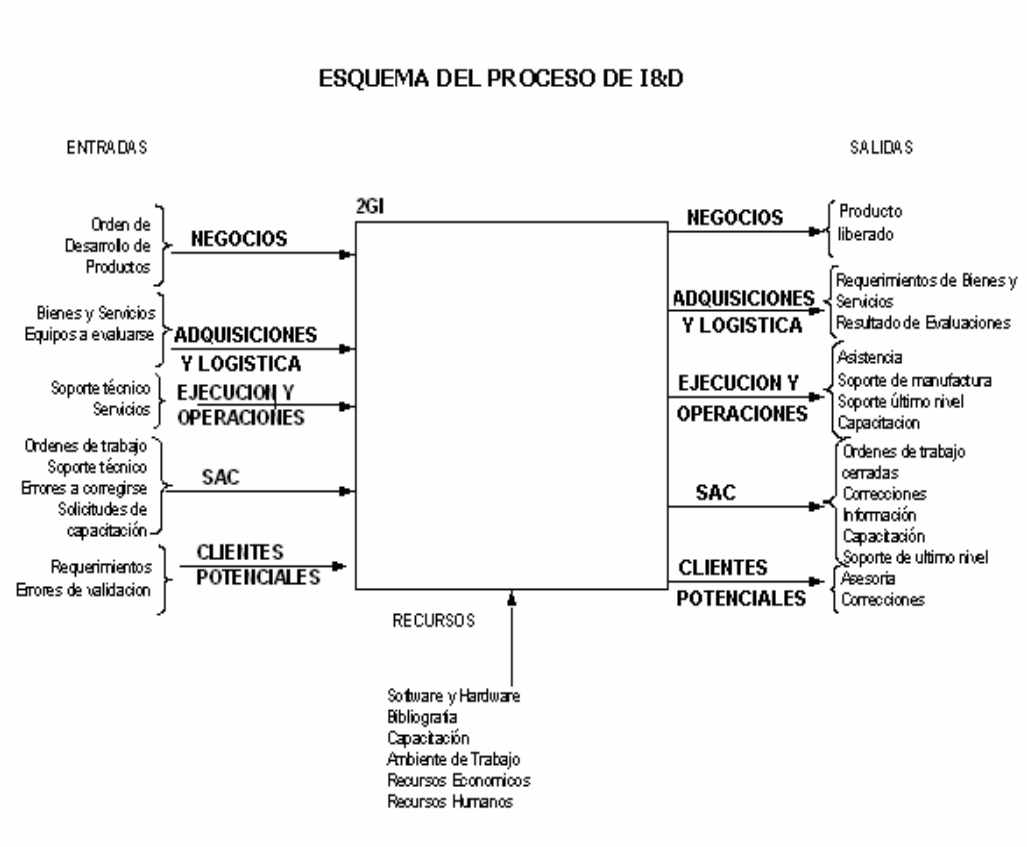
4.4 ELABORACIÓN DEL PROGRAMA DE GESTIÓN DE CRISIS

Según el proceso de planificación general, hemos desarrollado anteriormente las etapas de conformación del EGC y una parte de la Evaluación(Diagnóstico de la preparación), entonces nos resta desarrollar la evaluación de los tipos de crisis potenciales antes de proceder a elaborar el programa.

Una vez realizado el diagnóstico y haber palpado la falencia en la gestión de riesgos en la empresa, procedimos al análisis de su cadena de valor, que básicamente esta conformada por los siguientes procesos: Negocios, I+D, Operaciones, Adquisiciones y Servicio al cliente, de los cuales el proceso de I+D se ha identificado como el más crítico debido, a que a su cargo se encuentra entre otras tareas la gestión tecnológica que da soporte al Sistema de fidelidad y el desarrollo y mantenimiento de aplicaciones de software/hardware personalizadas, los cuales son comercializados.

Para tener una idea más clara, tenemos a continuación el proceso de I+D y sus interrrelaciones:

FIGURA 4.3 ESQUEMA DEL PROCESO DE I&D



Podemos observar una representación aproximada del proceso(I&D), el cual tiene varios elementos de entrada que provienen de otros procesos de la organización(Negocios, Servicio al Cliente, Ejecución y Operaciones, Adquisiciones/Logística, y Clientes Potenciales), entre los cuales podemos citar: orden de desarrollo de productos, requerimientos de soporte técnico, errores en aplicaciones de software a corregirse, solicitudes de capacitación.

De la misma manera tenemos varios elementos de salida, entre los cuales podemos citar: el producto liberado, requerimientos de bienes, resultados de evaluaciones, capacitación, asesoría.

La empresa es básicamente dependiente de su producto tecnológico “Sistema de fidelidad”, el cual facilita a los clientes dueños de flotas vehiculares la gestión permanente del aprovisionamiento de combustible en una red de estaciones de servicio. Como recompensa por la administración de toda la información generada

en las estaciones de servicio por las flotas, la empresa recibe una valor fijo mensual, que constituye aproximadamente el 50% del total de sus ingresos. En este sentido la entrega del servicio continuo es muy importante para afianzar la fidelidad de los clientes a este sistema y ser un buen referente para captar más mercado, lo cual contribuiría a la obtención de mayores ingresos fijos.

Para nuestro caso, dentro de este proceso vamos analizar el subproceso que garantiza el aprovisionamiento continuo de combustible y el acceso a través de la pagina web, a la información de las flotas de manera permanente. En este sentido garantizar la continuidad de este servicio implica contar con la infraestructura tecnológica adecuada en pleno funcionamiento, así como también, con el personal idóneo para llevar a cabo su gestión.

La implementación de sistemas tecnológicos de alta disponibilidad que existen en el mercado, mediante redundancia de equipos o sus partes, no es viable actualmente en la empresa, por su costo muy elevado. En estas condiciones debemos preveer otras alternativas para enfrentar una eventualidad que afecte la disponibilidad del principal servicio del cual depende la empresa.

4.4.1 EVALUACIÓN DE CRISIS POTENCIALES

Enseguida, procedemos a realizar los tipos de riesgos a los que esta expuesto nuestro proceso considerado crítico.

Identificación.- Para llevar adelante este proceso podemos hacer uso de los resultados obtenidos en la herramienta de diagnóstico Tipos, lo que nos permite identificar los tipos de crisis potenciales que no han sido tomados en cuenta por la organización en la prevención, tratamiento o recuperación de crisis, así como aquellos que habiendo sido tomados en cuenta no están siendo gestionados de manera integral, y en nuestro caso lo relacionado al proceso crítico.

En este sentido, vamos a identificar los tipos de crisis potenciales que podrían amenazar el proceso crítico de la organización, que como lo manifestamos

anteriormente están bajo la responsabilidad de I & D. Podríamos advertir que por la actividad de la empresa estos riesgos serían principalmente de carácter tecnológico, pero no se descarta ni se los considera menos críticos otros tipos de riesgos. Para los fines del presente trabajo señalaremos solamente algunos.

CUADRO 4.1 IDENTIFICACION DE CRISIS POTENCIALES

Identificación de tipos de crisis potenciales				
Objetivo del proceso:	**Causas**	**Riesgo(crisis potenciales)**	**Descripción**	**Efectos (consecuencias)**
Proveer la información del consumo de combustible a los usuarios y clientes	Sobrecarga de conexiones y aparatos electrónicos. Material inflamable Descuido en el mantenimiento de la red eléctrica. No hay regulación de temperatura.	Incendios	La alta concentración de calor por la disposición de varios equipos electrónicos en un espacio reducido y el funcionamiento continuo de los mismos, puede provocar un incendio.	Improductividad Daño a la imagen Posibles pérdidas materiales, humanas o de información.
Proveer la información del consumo de combustible a los usuarios y clientes	Descuido en la seguridad física. Inseguridad en el país.	Robo	Los bienes tecnológicos son un atractivo para la delincuencia	Posibles pérdidas materiales, humanas o de información importante para el negocio.
Proveer la información del consumo de combustible a los usuarios y clientes	Defectos físicos en el disco por: Alto nivel de uso. Variaciones de voltaje. Tiempo de vida útil.	Daño disco duro Servidor	Equipo servidor de base de datos no disponible.	Improductividad Reclamos de los clientes. Daño a la imagen de la empresa.
Proveer soporte técnico y desarrollar productos.	Inconformidad	Salida empleado clave	Conocimiento critico para la operación del negocio se va con el empleado.	Interrupción del proceso a su cargo.

En el cuadro anterior podemos evidenciar también, como diferentes variables pueden intervenir en el origen de una crisis y como su ocurrencia puede determinar varios efectos o consecuencias.

Valoración.- Después de haber identificado los posibles riesgos a los que se enfrenta la organización, construimos la tabla de probabilidad y vulnerabilidad, en base a datos históricos de ocurrencia y del análisis de los controles existentes actualmente en la organización.

A continuación un análisis de las consideraciones tomadas para definir su probabilidad y vulnerabilidad de cada uno de los riesgos.

- Para el caso del incendio, no se ha registrado antes un evento de este tipo, sin embargo las condiciones de alta combustibilidad de los muebles de oficina y el piso flotante, sumados a la poca ventilación especialmente en el espacio de los servidores, no se descarta la probabilidad de que este riesgo se materialice, por lo que se le ha asignado una probabilidad media. Al no existir procedimientos ni actividades de entrenamiento para enfrentar este tipo de riesgo, se ha considerado una vulnerabilidad alta para este evento.

- En lo que respecta al riesgo robo, se han registrado anteriormente intentos de robo de los bienes de la empresa; fuera de la empresa se ha materializado este riesgo. El sector en donde se encuentra localizado la empresa se considera susceptible de que se materialice este tipo de evento. Por estas razones se ha considerado asignarle una probabilidad alta. No existen procedimientos formales para contrarrestar este tipo de riesgo lo cual le hace altamente vulnerable.

- En cuanto al daño en el disco duro, se han registrado anteriormente eventos de este tipo, además es conocido en el sector de la industria como un evento común, sea por la obsolescencia que alcanza luego de un tiempo determinado, o por la intensidad de uso del mismo, por ello se le ha asignado una alta probabilidad. Existen ciertos procedimientos enfocados básicamente a respaldar la información del disco periódicamente, pero no existen procedimientos de recuperación, por tal motivo se lo considera de alta vulnerabilidad.

- En cuanto al evento salida de empleado clave, se ha registrado anteriormente este tipo de evento y los efectos fueron la interrupción y retraso de una actividad importante para el negocio, por ello se ha asignado una probabilidad alta. No se tiene implementado procedimiento de traspaso de información clave entre la persona que abandona un puesto y su reemplazo, por esta razón se lo considera de alta vulnerabilidad.

Las consideraciones anteriores están reflejadas en la siguiente tabla:

CUADRO 4.2 TABLA DE PROBABILIDAD Y VULNERABILIDAD

Posibles Amenazas	**Probabilidad (entorno, datos históricos)**			**Vulnerabilidad (controles existentes)**			**Riesgos detectados**
	Baja	Media	Alta	Baja	Media	Alta	
Incendios		✔				✔	✔
Robo			✔			✔	✔
Daño disco duro Servidor			✔			✔	✔
Salida empleado clave			✔			✔	✔

De lo anterior observamos que la mayoría de los tipos de crisis(riesgos) identificados tienen una alta probabilidad de ocurrencia. La vulnerabilidad también es alta, debido a que los escasos controles existentes son poco efectivos o simplemente no existen.

Basándonos en los cuadros(4.1 y 4.2)decidimos que hacer con los riesgos (reducir, eliminar, transferir o aceptar).
Las decisiones tomadas son las siguientes:

Incendios: Se ha optado reducir el riesgo, ya que esto beneficiará de forma determinante a la empresa, debido a que actualmente carece de: un sistema de alarma contra incendios, señalamiento de las rutas de evacuación, sistemas de irrigación, detectores de humo, mantenimiento de extintores y personal capacitado.
Para cumplir con este objetivo se va elaborar un conjunto de acciones a ser ejecutadas en cada fase del evento de crisis(incendio).

Robo: Se optó por reducir el riesgo, tomando en cuenta que no se tiene personal de vigilancia en el día y el entorno social de inseguridad actual en el país no favorece al normal desarrollo de las operaciones diarias. Muchas veces nos preocupamos más por el bien tangible(equipo), cuando resulta ser más valioso la información contenida en él.
Para cumplir con este objetivo se va elaborar un conjunto de acciones a ser ejecutadas en cada fase del evento de crisis(robo).

Daño disco duro Servidor: Se ha optado por reducir el riesgo, debido a que actualmente por el factor costo, no se ha implementado un sistema de redundancia más sofisticado. Vale la pena mencionar que la probabilidad de daño físico de este elemento en un equipo servidor siempre es alta, y está determinada por varios factores tales como: cantidad de usuarios que acceden a la información, sobrecargas, vida útil, etc.
Para cumplir con este objetivo se va elaborar un conjunto de acciones a ser ejecutadas en cada fase del evento de crisis(daño disco duro).

Salida de empleado clave: Se ha decidido aceptar el riesgo y tomar las debidas precauciones para reducir el impacto. En estos tiempos existe alta movilidad de personal especialmente del área tecnológica, por lo que en cualquier momento un empleado responsable de un proceso clave podría abandonar la organización, lo cual significaría una interrupción de este proceso.
Para cumplir con el objetivo se va elaborar un conjunto de acciones a ser ejecutadas en cada fase del evento de crisis(salida empleado clave).

4.4.2 ELABORACIÓN DEL PROGRAMA DE GC

Hemos constatado que existen una variedad de riesgos que amenazan a la organización en estudio(en especial al proceso crítico I & D), todos ellos con su grado de probabilidad de llegar a concretarse dependiendo de algunos factores internos o externos. El tratamiento de ellos va a demandar la inversión de una gran cantidad de recursos. Para cumplir con el objetivo del presente trabajo, se ha

seleccionado solo algunos riesgos que tienen un origen diferente, a fin de ejemplificar la elaboración del programa de GC.
En nuestro caso, el objetivo del programa es preparar a la organización y específicamente a los miembros del proceso crítico(I&D) para afrontar eventos que pueden causar una interrupción de las operaciones del negocio, una pérdida económica, un daño a la imagen, a la propiedad o al ser humano.

Conforme el procedimiento descrito en la sección 3.5 del capitulo anterior, procedemos a elaborar el programa, el cual básicamente contendrá las estrategias o acciones de prevención, de mitigación y las de recuperación para dar tratamiento a los riesgos(crisis potenciales) identificados en la sección anterior, para el efecto se considerarán ciertas suposiciones y condiciones bajo las cuales se desarrolla el evento.

A continuación detallamos el desarrollo de las acciones estratégicas para cada uno de los riesgos.

4.4.2.1 ACCIONES PARA LA GESTIÓN DE INCENDIO

Para la gestión de este riesgo partimos del supuesto de que el incendio se produce dentro de las horas laborables.

Acciones preventivas (ANTES)

- Contar con extintores en buenas condiciones y en lugares estratégicos
- Contar con salidas de emergencias señalizadas.
- Contar con números telefónicos donde se pueda reportar cualquier emergencia.
- Evitar sobrecargar las líneas eléctricas, no conectando más de un aparato en cada toma corriente.
- Desconectar los equipos electrónicos al término de su jornada.
- No utilizar para limpieza productos inflamables como gasolina, reporte a quienes lo usen.
- Reportar cualquier olor a quemado, gas, gasolina o productos aromáticos inflamables.

- No fumar en áreas restringidas(señalización).
- Identificar las posibles fuentes de incendio de su entorno de trabajo.
- Familiarizar con la ubicación y el uso de los extintores de su área de trabajo.
- Reportar las obstrucciones a los accesos de extintores.

Acciones reactivas (DURANTE)

- Intentar sofocarlo con el extintor más cercano.
- Implementar reglas de no fumar.
- Desconectar los aparatos electrónicos a su alcance.
- Retirarse del lugar, cerrando puertas y ventanas.
- Considerar que es inminente el desalojo del lugar; para lo cual debe estar preparado para actuar con rapidez, procurando conservar la calma.
- Si no es su piso, considerar actuar por decisión propia y abandonar el lugar.
- En cualquiera de los casos, siga las instrucciones de quien este coordinando las acciones.

Acciones de recuperación(DESPUES)

- Al tener bajo control la emergencia, cuando sea necesario, los encargados de área afectada, participarán en la investigación de las causas que originaron el siniestro, informando por escrito al Comité.
- Los encargados del/las área(s) afectada(s) deben elaborar un reporte a sus superiores, que contengan: descripción cronológica de los hechos, gravedad de los daños humanos y materiales, posibles causas, lugar de la emergencia, forma en que se recibió el reporte, medios utilizados para combatir al fuego y eficiencia en las acciones tomadas, así como fallas de organización, humanos o de equipos que se observaron, además de las recomendaciones o sugerencias.
- Con el resultado de la evaluación de los daños proceder a ejecutar las acciones de recuperación de los procesos, en estas actividades participarán los dueños de los procesos bajo la coordinación y supervisión del Comité de GC.
- Los encargados de área que como resultado del siniestro tengan información que consideren de utilidad, deben dirigirla por escrito al comité, con el fin de emplear esas experiencias en la actualización de los procedimientos

establecidos adecuándolos para casos futuros, llevando un control hasta su cabal cumplimento.

4.4.2.2 ACCIONES PARA LA GESTIÓN DE UN ROBO

Para la gestión de este riesgo partimos del supuesto de que el robo se realiza en horas laborables.

Acciones preventivas (ANTES)

- Tener capacitación sobre como actuar en caso de que este riesgo se materialice.
- Tener al alcance números telefónicos de emergencias.
- Situar alarmas en lugares estratégicos y que sólo el personal conozca su ubicación.
- Evitar llevar dinero en exceso u objetos de valor.
- Cuide que nadie lo siga. Si alguien lo sigue, busque vías de escape.
- Localizar personal de vigilancia apto para responder ante este suceso
- Si se percata de la presencia de sujetos evidentemente sospechosos (estén o no armados), informar al encargado del área y al personal de vigilancia, en caso de existir.

Acciones reactivas (DURANTE)

- Si es víctima de un acto ilícito procure conservar la calma, no intente impedir el delito, puede estar en peligro su integridad física.
- Si es posible y sin exponerse, observe con detalle las características del individuo que esté relacionado con el delito.
- Si es testigo, sólo si es posible y sin exponerse, con discreción solicitar ayuda.
- Esperar hasta que el delincuente(s) se aleje y pase el peligro.

Acciones de recuperación (DESPUES)

- Conservar la calma.
- Evaluar lo sucedido o el perjuicio ocasionado, y comunicar al comité de GC, el cual tomará las acciones necesarias para remediarlo.
- Evaluar la actuación en el acontecimiento y recoger sugerencias para mejorarlo en el futuro.

4.4.2.3 ACCIONES PARA LA GESTIÓN DE DAÑO DEL DISCO DURO

Para la gestión de este riesgo partimos del supuesto de que el equipo servidor no tiene ninguna configuración de recuperación automática, y que el resto de elementos del equipo están en buenas condiciones.

Acciones preventivas (ANTES)

- Determinar las características del hardware y en especial del disco duro(su capacidad y tipo de tecnología) instalado en el servidor.
- Periódicamente realizar un chequeo de la superficie del disco con programas utilitarios, en caso de anomalías informar al jefe inmediato.
- Periódicamente respaldar la información contenida en el/los disco(s) duro(s).
- Llevar el registro de la fecha de respaldo y la localización de los respaldos.
- Tener en stock un disco duro de respaldo.
- Realizar un mantenimiento periódico del Servidor(s), si nota alguna anomalía informar inmediatamente a su superior.
- Mantener a la mano los manuales y software originales del equipo servidor.
- Mantener a la mano los números telefónicos del proveedor y el soporte técnico especializado.
- Tener identificado las aplicaciones instaladas en el disco, así como su documentación para una eventual reinstalación.
- Capacitar al personal técnico en el mantenimiento y recuperación (Hardware/Software) del servidor.
- Realizar simulacros periódicamente.

Acciones reactivas (DURANTE)

- Aislar el equipo de la red
- Comunicar a todo el personal y/o clientes(usuarios del servidor) la no disponibilidad de los datos.

Acciones de recuperación (DESPUES)

- Reemplazar el disco duro.
- Configuración del disco en el equipo servidor.
- Instalación y configuración de todo el software del disco original(sistema operativo, administrador de base de datos, utilitarios, etc.).
- Restauración de los datos desde los respaldos.

- Comunicar a todos los usuarios de la disponibilidad del servidor.
- Verificar con los usuarios la integridad de la información recuperada.
- Evaluación y recepción de sugerencias para mejorar el procedimiento de recuperación.

4.4.2.4 ACCIONES PARA LA GESTIÓN DE SALIDA DE EMPLEADO CLAVE

Para la gestión de este riesgo partimos del supuesto de que un empleado clave decide abandonar la empresa voluntariamente.

Acciones preventivas (ANTES)

- Identificar la información clave por puesto para la operación de la empresa.
- Realizar intercambio de funciones entre pares, de ser posible.
- Concienciar la importancia de compartir la información en beneficio de la empresa.
- Documentar la información clave por puesto.
- Documentar el perfil y las habilidades requeridas para el puesto.
- Formalizar el traspaso de la información.
- Auditar la documentación generada por el puesto.
- Auditar periódicamente la moral de los empleados.

Acciones reactivas (DURANTE)

- Mantener buena comunicación con el empleado saliente.
- Recoger información sobre las razones o causas de su abandono, sus recomendaciones.
- Designar al receptor de la información(empleado reemplazo o un par).
- Ejecutar el traspaso formal de información.

Acciones de recuperación (DESPUES)

- Análisis y validación de la información recolectada del empleado saliente.
- Realizar un seguimiento de la recuperación a estado normal del proceso involucrado.
- Brindar apoyo y hacer un seguimiento de la moral del empleado reemplazo.

- Evaluar, documentar, modificar o actualizar los procedimientos elaborados y ejecutados en la gestión de la continuidad del conocimiento, responsabilidad del comité de GC.

A continuación describimos los Grupos de interés(stakeholdres) identificados y a ser tomados en cuenta en la gestión de crisis de la empresa, en nuestro caso son: los funcionarios de otros departamentos(clientes internos), la alta dirección, los clientes y los proveedores de servicios públicos locales: policía, bomberos.

Se sugiere realizar una capacitación al personal involucrado para resaltar la importancia de realizar la gestión de crisis en la organización antes de la implementación, muy en especial a los del proceso crítico, con ello se contribuye a crear una cultura de prevención y concienciación necesaria para llevar adelante esta gestión, para lo cual el apoyo incondicional de la alta dirección es imprescindible.

Para el presente caso el parámetro RTO esta dado por el tiempo que nuestros clientes internos y externos pueden tolerar la interrupción del proceso principal. Tomando en cuenta, que se tiene implementado ciertos procedimientos para contrarrestar algún evento adverso que afecte a los sistemas informáticos, se ha establecido que el tiempo máximo de inhabilitación del proceso en estudio no debe sobrepasar los 7 días.

Para el caso del RPO este parámetro dependerá del riesgo, por lo que de manera general podemos manifestar que para el caso de interrupción de los sistemas informáticos el tiempo esta dado por la periodicidad de respaldo de la información, en nuestro caso es de dos días.

Para el caso del riesgo salida del empleado clave, este tiempo depende de varios factores tales como: el nivel de conocimiento, habilidad y experiencia del empleado reemplazo, y de cuan efectiva haya sido la gestión de la continuidad del conocimiento para ese cargo. Sin embargo para nuestro caso se ha determinado que no debe exceder de 15 días.

En resumen, todas las consideraciones planteadas y las estrategias descritas a ejecutarse en cada fase, para cada una de los riesgos identificados vienen a conformar un Programa de Gestión de Crisis.

Cabe mencionar, que la elaboración de las acciones descritas en el Programa de GC para el presente caso, no tienen la intención de ser una receta, ya que como se ha mencionado a lo largo del presente trabajo las circunstancias que rodean a cada organización son distintas y cambiantes, por lo cual cada organización le corresponderá elaborar su propia programa, ya que nuestra intención ha sido demostrar la aplicabilidad del modelo propuesto.

De igual manera, los riesgos tecnológicos aquí tratados son los más visibles y sencillos, sin duda existen entornos de cómputos muy sofisticados cuya gestión de los riesgos asociados demandará de muchos recursos(económico, conocimiento y tiempo).

4.5 DOCUMENTACIÓN

Toda la documentación del programa de GC (continuidad organizacional) debe estar sustentado en un formato estándar y de fácil comprensión para la mayoría en la organización, esto es primordial para su puesta en práctica.

Como se mencionó en el capítulo anterior, es recomendable tener un documento principal para el registro de la información clave y común para todos los tipos de crisis(riesgos), y hacer referencia en éste al documento que contiene las acciones de tratamiento de riesgos individuales, esto facilitará su mantenimiento. Este documento puede empezar a llenarse en la etapa de elaboración del programa de GC, por ello a continuación presentamos a manera de ejemplo, el documento con algunos ítems ya llenos, los demás deberán ser completados en la etapa de implementación.

4.5.1 DOCUMENTO DE PLANIFICACION DE LA GESTION DE CRISIS Y CONTINUIDAD DEL NEGOCIO

Este es el formato del documento que podríamos utilizarlo en la gestión de la continuidad organizacional.

Lugar de operación normal	**Lugar de operación alternativo**
Nombre de la Compañía: *Tecnológica Cía. Ltda.* Dirección: *Av. 12 Octubre 235* Ciudad, Provincia: *Quito, Pichincha* Número de Teléfono: *2563241*	Nombre de la Compañía: _____ Dirección: _____ Ciudad, Provincia: _____ Número de Teléfono: _____

La siguiente persona estará a cargo de gestionar la crisis y será el portavoz de la compañía en caso de emergencia.

- Contacto Primario de Emergencia: *Gustavo B.*
- Número de Teléfono: *2356245*
- Número Alternativo: *099686900*
- Correo electrónico: *gustavob@tecnologica.com*

En ausencia de la persona principal estará a cargo de gestionar la crisis esta persona.
Contacto Secundario de Emergencia _____
Número de Teléfono _____
Número Alternativo _____
Correo electrónico _____

INFORMACION DE CONTACTOS DE EMERGENCIA

- Marque 9-1-1 en caso de emergencia
- Policía/Bomberos - No Emergencias

101 / 102

- Proveedor de Seguros

_____

MANTÉNGANSE INFORMADO

Los siguientes RIESGOS naturales y causados por el hombre podrían afectar nuestro negocio:

Riesgos	**Plan de acción**	**Archivo**
Incendio	Acciones para la gestión de incendio	GC_incendio.doc
Robo	Acciones para la gestión de Robos	GC_robo.doc
Daño disco duro Servidor	Acciones para la gestión de Daño disco	GC_daño_disco.doc
Salida empleado clave	Acciones para la gestión de Salida empleado clave	GC_salida_empleado.doc

EQUIPO DE GESTION DE CRISIS

Las siguientes personas participarán en la planificación de emergencias y la gestión de crisis:

Nombre	**Area**	**Ext.**	**Número teléfono**
Juan Pérez	Administración	217	2357641
Willian Gualotuña	Investigación y Desarrollo	213	*2356245*

Las siguientes personas de los negocios vecinos participarán en nuestro equipo de GC:

_____

_____

Comunicaremos nuestros planes de emergencia con compañeros de trabajo de la siguiente forma:

_____

_____

En caso de desastre, nos comunicaremos con los empleados de la siguiente forma:

En días laborables marcando su número de extensión.

En fines de semana o feriados marcando a su domicilio ó a su celular.

PROVEEDORES

Nombre de la Compañía: _____

Dirección: _____

Ciudad: _____ Provincia: _____

Código Postal: _____

Teléfono: Fax: Correo electrónico: _____

Nombre de Contacto: Número de Cuenta: _____

Materiales/Servicios Proporcionados: _____

Si esta compañía sufre un desastre, obtendremos los suministros/materiales de la siguiente:

Nombre de la Compañía: _____

Dirección: _____

Ciudad: _____ Estado: _____

Código Postal: _____

Teléfono: Fax: Correo electrónico: _____

Nombre de Contacto: Número de Cuenta: _____

Materiales/Servicios Proporcionados: _____

PLAN DE EVACUACION PARA LAS INSTALACIONES

Hemos elaborado estos planes en colaboración con los negocios vecinos y los propietarios del edificio para evitar confusión.

Hemos encontrado, copiado y publicado mapas del edificio y de las instalaciones.

Las salidas están claramente marcadas.

Practicaremos los procedimientos de evacuación _____veces por año.

Si debemos abandonar rápidamente el lugar de trabajo:

_____

1. Sistema de advertencia.

_____ Probaremos el sistema de advertencia y registraremos los resultados _____ veces por año.

2. Lugar de reunión

_____

3. Persona responsable/coordinador para el lugar de reunión:

_____

a. Algunas responsabilidades:

_____

4. _____ es responsable de emitir la orden de "todo despejado".

COPIA DE SEGURIDAD DE LOS ARCHIVOS

- *El administrador de red (Juan Pérez)* es responsable de hacer copias de seguridad de nuestros archivos cruciales, incluidos los sistemas de nómina del personal y de contabilidad.
- Las copias de seguridad, incluyendo una copia de este plan, mapas del sitio, pólizas de seguro, registros bancarios y copias de seguridad informáticas están en nuestras instalaciones en *La caja fuerte*
- Otro juego de copias de seguridad está guardado en este lugar fuera de las instalaciones: *Bóveda del Banco del Pichincha*

Si nuestros registros de contabilidad y nómina de personal resultan destruidos, mantendremos la continuidad de la siguiente forma:

_____

_____

INFORMACION DE CONTACTO EN EMERGENCIA DE LOS EMPLEADOS

La siguiente es una lista de nuestros compañeros de trabajo y su información de contacto de emergencia individual:

Nombre	**Número teléfono**	**Número alternativo(cel.)**
Arteaga Marco	2264897	098652354
Gualotuña Willian	2548698	095648254
Melo Mónica	2648354	097568425

REVISION ANUAL

Revisaremos y actualizaremos este plan de continuidad del negocio y de desastres en *las oficinas de la compañía la primera semana de año.*

COMITÉ DE GC DE LA COMPAÑÍA TECNOLOGICA.

Hasta aquí comprende el documento principal, los ítems que todavía no están llenos serán completados en la etapa de implementación.

Es importante distribuir la responsabilidad del mantenimiento de la documentación entre los dueños de los procesos del negocio y el comité de GC, éste a la vez actuará coordinando, dando guías, y estandarizando el trabajo de toda la organización. Es responsabilidad del comité, divulgar la última versión de la documentación.
De la misma forma que se respalda los datos del negocio de la empresa, toda la documentación surgida como resultado de la elaboración y mantenimiento del programa de GC debe ser debidamente respaldada.

Para alcanzar el éxito en la implementación del programa de GC, se recomienda adecuar la estructura organizacional al de una empresa innovadora, es decir una estructura plana para generar el compromiso y la colaboración necesaria de los empleados, de igual manera considerar que en este tipo de empresas su valor radica en el uso intensivo del capital intelectual y no en los activos tangibles por lo que es necesario gestionarlo adecuadamente.

Finalmente, se debe tener presente que los planes ¡no son el objetivo! son un medio más para lograr la continuidad del negocio, por lo que:
No hay que preocuparse en escribir el mejor plan del mundo, sino en realizar las pruebas necesarias para comprobar su efectividad

Con todo lo expuesto en el presente trabajo se ha dado cumplimiento a los objetivos planteados en el plan de tesis.

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- En el presente estudio se ha podido determinar que no existe todavía una terminología universalmente aceptada para nombrar a un programa de continuidad organizacional, ya que se ha venido utilizando indistintamente los términos Gestión de Crisis(GC) ó Gestión de la Continuidad de Negocio, entre otras, y muchas veces la terminología utilizada es la que determina su alcance. La falta de un estándar universalmente aceptado ha sido quizá la causa de que en las organizaciones de los países subdesarrollados no se haya tomado interés, de la necesidad de una gestión sistémica de los riesgos en todas las fases(antes, durante y después).

- Los procesos que se deben llevar a cabo para la creación de un programa de Gestión de Crisis(continuidad organizacional) se pueden dividir en varias etapas. Primeramente se procede a la identificación y análisis de cuáles son aquellos puntos en el negocio que, en caso de fallo o interrupción, pueden provocar problemas a la organización. A continuación se desarrollan las estrategias de prevención, respuesta y recuperación para dar tratamiento a los riesgos identificados en sus diferentes fases en el tiempo. Se debe implementar dicho plan realizando las adquisiciones y la formación necesaria para que todo esté preparado si el riesgo llega a materializarse. Por último, y probablemente lo más importante, se debe realizar una prueba total de dicho plan para comprobar su efectividad y tomar correctivos de ser necesario.

- Las organizaciones preparadas ante crisis se diferencian de aquellas que son propensas, en que las primeras tienen una visión global e integrada, la ven como una necesidad estratégica y no como un coste. Este cambio en la filosofía corporativa hace que los ejecutivos consideren a sus empresas no

solamente como sistemas productivos sino también como potencialmente destructivos, ya que no sólo discuten los puntos relacionados con el crecimiento productivo sino también con los potenciales fracasos o fallas, teniendo presente de que las crisis originadas por el hombre o por la organización pueden ser evitadas. La integración de la GC en la filosofía de excelencia corporativa es primordial, ya que el no hacerlo puede llegar a ser un obstáculo para el desarrollo de un programa de GC efectivo. En este sentido ciertas excusas como: “Un programa formal no es necesario para una compañía excelente. Solo las compañías malas necesitan gestión de crisis para cubrir sus deficiencias”, crean excesiva autoconfianza, lo que influye negativamente en la gestión de crisis.

- Son consideradas buenas prácticas de organizaciones preparadas ante crisis, el implementar procesos de evaluación tales como auditorías (legales, financieras, etc.), el evaluar el número de días que pueden mantener las actividades diarias sin personal, sin efectivo, sin tecnología o sin datos, el determinar grupos de interés o mercados que deben servir ineludiblemente, el establecimiento de prioridades en las actividades para las operaciones diarias. De igual manera, las organizaciones preparadas delegan a los responsables de los procesos, investigar en sus áreas eventos de crisis relacionados y comunicar al equipo o comité de GC eventos no considerados para su tratamiento, averiguan los efectos que producirían los cambios en las regulaciones o la innovación en la tecnología, ven en el análisis de crisis pasadas una oportunidad de aprender y mejorar los esfuerzos futuros, y comprenden que la gestión de crisis requiere tanto acciones técnicas como humanas.

- El propósito de la GC de crisis no es exclusivamente volver lo antes posible a hacer negocios, sino que además la organización debe tomar conciencia de su responsabilidad moral y social con los stakeholders internos y externos, con la sociedad e incluso con el medio ambiente. Por ello la organización preparada debe integrar esta responsabilidad a su filosofía y estrategias de negocio, con la finalidad de obtener ventajas competitivas.

5.2 RECOMENDACIONES

- El objetivo primordial de un programa de continuidad organizacional(GC) es el de preservar la integridad física del personal, las instalaciones, la seguridad del equipo de computo y el medio ambiente; así como, recuperar las operaciones del negocio en el menor tiempo para reducir o evitar posibles pérdidas y garantizar su continuidad.

- Un ambiente adecuado que propicie una buena comunicación organizacional contribuye al desarrollo con mayor facilidad de un plan o programa de GC, el cual es de gran utilidad en la prevención, mitigación y restauración de eventos no previstos para fortalecer los puntos débiles de la empresa. De igual manera se consigue, una menor resistencia a la prueba del plan y una mayor participación de la gente involucrada en las mejoras posteriores.

- Cualquier programa de continuidad organizacional debe buscar establecer cómo la organización puede continuar sus operaciones en caso que se produzca una interrupción. La responsabilidad de que este plan de continuidad exista, que esté bien dimensionado y que cuente con los recursos necesarios para llevarse a cabo recae en la alta gerencia, debido a que las consecuencias de dicha interrupción del servicio por un tiempo prolongado pueden llevar a un gran perjuicio económico para la empresa y en algunos casos, a la desaparición de la misma.

- Desarrollar una cultura interna donde se fomente la discusión de malas noticias. Para ello se debe implementar sistemas de bonificación y reconocimiento para empleados que descubren peligros ocultos, funcionamiento defectuoso o defectos en el producto. La experiencia de un desastre trae consigo serios problemas psicológicos, por ello algunas empresas preparadas, emplean servicios de los equipos de intervención postcrisis, formados por psicoterapeutas, trabajadores sociales y médicos.

REFERENCIAS BIBLIOGRAFICAS

LIBROS

- Beazley H., Boenisch J y David Harden, Continuity Management, New York: Jhon Wiley & Sons Inc., 2002.
- Bennis W., Spreitzer G. y T. Cummings, Las claves del Liderazgo, Barcelona: Ediciones Deusto, 2006.
- Chiavenato Idalberto, Gestión del talento humano, Bogotá: Mc Graw-Hill Interamericana, 2002.
- David Fred R, Conceptos de Administración Estratégica, México: Prentice-Hall. Quinta edición, 1997.
- Friedman Mark, Everyday Crisis Management, Naperville:First Decision Press, 2002.
- Hoffman D., Bateson J., Fundamentos de Marketing de servicios, México: Printice Hall, 2002
- Lincango Miguel Angel, Administración por procesos, Universidad Central: Quito, 2006.
- Marín Hoyos Alvaro, Como recuperar su empresa: el método C, Bogotá: Editorial Norma S.A., 2002.
- Mintzberg H., Quinn J. y J. Voyer, El Proceso Estratégico, México: Printice Hall. Primera edición, 2002.
- Mitroff I. y C. Pearson, Cómo Gestionar una Crisis, Barcelona : Gestión 2000, 1999.

INTERNET

- Albaladejo Juan Carlos. (2006). Que es la prevención de riesgos laborales: Objetivos y Definiciones. www.prevention-world.com.
- Alvarez José Angel. (2004). Optimismo en medio de la crisis: cómo lograrlo http://www.mujeresdeempresa.com
- Aporte Grupo Kaizen. (2006). Moviendo la frontera de la estrategia. http://www.gestiopolis.com

- Aramajo Armando. (2006). Diseñando la Estrategia Empresarial. http://www.secretosenred/
- Arroyo Eduardo. Universidad Metropolitana. (2006). Fundamentos de procesos: Definiciones y clasificaciones. http://www.suagm.educ_new_web/
- ASIS GDL BC. (2005). Business Continuity Guideline: A practical approach for emergency preparedness, crisis management and disaster recovery. http://www.asisonline.org
- Bravo Patricia. (2003). "Lecciones de Responsabilidad Social Corporativa para la empresa del siglo XXI". http://www.uai.cl/
- Buezo Luis. (2004). ¿Garantizan las empresas la Continuidad de su Negocio? http://www.computing.es
- Bustamante Alejandro. (2006). UCEMA-MAG Evaluación de riesgo agropecuario: Simulación Montecarlo. http://www.cema.edu.ar/
- Cano Miguel Antonio. (2006). Análisis del Caso Parmalat http://www.interamericanusa.com/
- Civil Aviation Authority of New Zealand. (2006). Rule Development Process: Risk Management Methodology. http://www.caa.govt.nz
- Chatzkel Jay. (2005). Measuring and Valuing Intellectual Capital: From Knowledge Management To Knowledge Measurement. http://www.tlainc.com/
- Daccach José Camilo. (2002). Continuidad y Contingencia http://www.deltaasesores.com/
- De la Fuente. (2002). Liderazgo en tiempos de crisis. http://www.inun.edu.ar/
- Deloitte & Touche. (2003). Business Continuity Management.. http://sfisaca.org/download/C10BusContinuityMgmt.pdf
- Departamento Administrativo de la Función Pública. Colombia. (2006). Guía Administración del Riesgo. http://procesos.univalle.edu.co
- Dora Price. (2006). Continuidad viva del negocio http://www_tecnologiaempresarial_info
- Ernst&Young. (2006). Evaluación del Riesgo empresarial. http:/www.ey.com/
- Espiñeira, Sheldon y Asociados. Firma miembro de PricewaterhouseCoopers. (2006). Planificación de la continuidad de operaciones. http://www.pc-news.com/

- Estrategia Empresarial. (2006). Las nuevas organizaciones empresariales en la Nueva Economía: La industria de la información en la Economía del Conocimiento. http://publicaciones.estrategia.net/
- Faulín Javier. (2006). Simulación de Montecarlo con Excel. http://www.abcbolsa.com/
- Fernández José Manuel. (2006). BS 25999 Gestión de la Continuidad de Negocio. http://iso9001-iso27001-gestion.blogspot.com/
- Gallego Mery. (2003). SA 8000 - Social Accontability. http://redalyc.uaemex.mx/
- García Fernando. (2005). La prevención entra en una etapa de más calidad y mayores precios. http:/www.fomenweb.com
- Gestióndelconocimiento.com. (2006). Aprendizaje Organizativo. http://www.gestiondelconocimiento.com/
- Gordon R. Sullivan, Michael V. Harper. Liderar el cambio: Tomado del libro: La esperanza no es un método. http://www.lafamilia.info
- Gregory Shaw. (2004). The competencies required for executive level business Crisis and Continuity Managers. http://www.gwu.edu/
- Horner Ken. (2006). Successful Business Continuity Strategies: How to Conduct Business as Usual. http://www.wwpi.com/
- Ivorra José. (2002). La gerencia de riesgos - factor crítico de éxito http://www.willydev.net/
- Koprinarov Bratoy. (2005). El riesgo empresarial y su gestión. http://www.analitica.com/
- Landaluce Gonzalo. (2005). Como estar preparado ante un desastre: Planificación de la continuidad de negocios. http://www.borrmatt.es/
- Llongueras Pasqual. (2006). Prevención y rentabilidad, por fin. http://www.prevencionintegral.com/
- Looney Robert. (2002). Economic Costs to the United States Stemming From the 9/11 Attacks. http://www.ccc.nps.navy.mil/
- Martínez Juan Gaspar. (2006). Análisis de impacto. http://www.iee.es/
- Medina César y Mónica Espinosa. (1996). El aprendizaje organizacional: el estado del arte hacia el tercer milenio. http://www.azc.uam.mx/

- Miller Kevin. (2006). Business impact analysis. What is business impact analysis - a definition from Whatis_com.http://searchstorage.techtarget.com/
- Muzard Joël. (2006). El Desarrollo del Capital Intelectual y la Administración de Conocimientos. http://www.a-i-a.com
- NFPA 1600. (2004). Standard on Disaster/Emergency Management and Business Continuity Programs. http://www.nfpa.org
- Office-Shadow - Business Continuity Software. (2006). Estadísticas sobre la Continuidad de Negocio. http://www.office-shadow.com
- Pavisich Luis. (2006). Las Nuevas Herramientas de la Administración Moderna. http://www.monografias.com
- Pool Roberto J. (2006). La Responsabilidad Social Empresarial: El Reto del Siglo XXI. http://www.mes-d.net/
- http://portal.surrey.ac.uk. (2007). Key elements of the Turnbull Report
- Romero Cuevas y Ramón Salvador. (2005). Gestión del Conocimiento y del Capital Intelectual en una PYME del sector textil.
  https: https://upcommons.upc.edu
- Saavedra Patricia. (2005). Riesgo y los Acuerdos de Basilea II.
  http://laberintos.itam.mx/
- Shaw Gregory. (2004). Crisis Management and Business Continuity. http://www.gwu.edu/~icdrm/publications/ShawTextbook011105.pdf
- Smith David. (2002). Business Continuity Institute. Business Continuity Management Good Practice Guidelines. http://www.auckland.ac.nz/
- Smith Peter A. (2006). Systemic Knowledge Management: Managing Organizational Assets For Competitive Advantage. http://www.tlainc.com/
- Soriano Claudio L. (2006). Evalúe cuál es su nivel de riesgo.
  http://www.microsoft.com/
- Touraj Nasseri. (2006). Knowledge Leverage : The Ultimate Advantage.
  http://www.brint.com/
- www.brsltd.org. (2006). HACCP MS e ISO 22000. Requisitos Sistemas de Gestión en Seguridad Alimentaria.
- www.consultoras.org (2006). BS 25999-1 Code of Practice for Business Continuity Management Just Published.

- www.deloitte.com. The 2004 Deloitte Research Study.
- www.gestiopolis.com. (2007). Cadena de valor.
- www.grupokaizen.com. (2006). Procesos de negocios.
- www.globalcrossing.com.(2006). Continuidad del Negocio.
- www.bcn.cl. Norma ISO 26000 Directrices sobre Responsabilidad Social.
- www.iso27000.es. (2006). ISO 27000.
- www.iso27001security.com ISO 27000 SERIES
- www.kpmg.cl. (2006). Enterprise Risk Management: Entendiendo la administración del riesgo.
- www.nasttpo.org. (2004). NFPA 1600 Included in the Intelligence Reform and Terrorism Prevention Act of 2004.
- www.office-shadow.com. Qué es la Continuidad de Negocio
- www.ready.gov. (2006). Department Homeland Security: Sample Business Continuity and Disaster Preparedness Plan.
- www.tinkle.es. (2006). Comunicación en tiempos de crisis.
- www.unu.edu. (2007). Stages of crisis management.
- http://www.gwu.edu Gregory Shaw. (2004). The competencies required for executive level business Crisis and Continuity Managers. http://www.gwu.edu/~icdrm/publications/PDF/Dissertation_Shaw.pdf
- Thomas Rosamund. (2005). Etica Empresarial Gobierno y Reputación Corporativa. http://www.inn.cl/iso26000/ÉticaEmpresarialGobierno%20ReputaciónCorporativa.pdf
- Izquierdo Fernando. Administración de riesgos TI. http://www.felaban.com/pdf/fernando_izquierdo_%20Administracion_de_riesgos.ppt
- Getronics. (2006). Gestion de Continuidad. http://www.getronics.com/es/es-es/solutions/servicios_infraestructura/Gestion_y_Mantenimiento/gm_gestcont.htm
- Editorial Borrmart. (2005). Introducción al Plan de Continuidad del negocio: Conceptos Básicos. http://www.borrmart.es/articulo_redseguridad.php?id=566&numero=18

ANEXO Nº 1

HERRAMIENTAS DE DIAGNOSTICO DE:

TIPOS DE CRISIS

FASES

SISTEMAS

GRUPOS DE INTERES

DOCUMENTO GUIA:

PLANIFICACION DE LA GESTION DE CRISIS Y CONTINUIDAD DEL NEGOCIO

HERRAMIENTA DIAGNÓSTICA PARA TIPOS - CRISIS

Fuente: Como Gestionar una Crisis, Ian Mitroff

¿Planifica su organización los siguientes puntos?

		SI	NO
A	**Ataques económicos externos**		
	Extorsión	☐	☐
	Soborno	☐	☐
	Boicot	☐	☐
	Opas(Oferta pública de acciones)	☐	☐
B	**Ataques informativos externos**		
	Violación de copyright	☐	☐
	Perdida de información	☐	☐
	Falsificación	☐	☐
	Rumores dañinos	☐	☐
C	**Averías**		
	Avisos y reclamaciones	☐	☐
	Fallos en el producto	☐	☐
	Fallos en las plantas	☐	☐
	Averías informáticas	☐	☐
	Operario deficiente/errores de operario	☐	☐
	Seguridad deficiente	☐	☐
D	**Catástrofes**		
	Daños medioambientales	☐	☐
	Accidentes importantes	☐	☐
E	**Psicopatología**		
	Terrorismo	☐	☐
	Imitadores	☐	☐
	Alteración/sabotaje in situ	☐	☐
	Alteración/sabotaje externo	☐	☐
	Rapto de ejecutivos	☐	☐
	Acoso sexual	☐	☐
	Rumores dañinos	☐	☐

F	**Factores sanitarios**	**SI**	**NO**
	Enfermedades ocupacionales	☐	☐
G	**Factores de imagen**		
	Daños a la reputación	☐	☐
	Rumores	☐	☐
H	**factores de recursos humanos**		
	Sustitución de ejecutivos	☐	☐
	Moral deficiente	☐	☐
	Número total de respuestas SI y NO	_____	_____

HERRAMIENTA DE DIAGNOSTICO TIPOS-ACCIONES PREVENTIVAS

Fuente: Como Gestionar una Crisis, Ian Mitroff, adaptada por el autor

	SI	NO
A Actividades estratégicas		
La filosofía corporativa apoya la GC		
La GC está integrada en las nociones y declaraciones de excelencia corporativa		
La GC está integrada en procesos de planificación estratégica		
Se incluye a personas de fuera de la organización en el equipo de GC		
Entrenamiento y cursillos de GC		
Simulaciones de crisis		
Estrategias de diversificación y de cartera para la GC.		
SUBTOTAL		
B Actividades técnicas y estructurales		
Creación de un equipo o unidad de GC		
Creación de un presupuesto para la GC		
Actualización y desarrollo continuo de manuales y políticas de emergencia		
Inventario informatizados de empleados, plantas, productos y aptitudes		
Creación de una sala o unas instalaciones estratégicas de emergencia		
Reducción de productos, servicios y procesos de producción peligrosos		
Mejoras en el diseño y en la seguridad global del producto y de la producción		
Redundancia técnologica(copias de seguridad informáticas)		
Contratación de expertos y servicios de GC externos		
SUBTOTAL		
C Actividades de evaluación y diagnóstico		
Auditorias legales y financieras de amenazas y responsabilidades		
Modificaciones en la cobertura del seguro		
Auditorías de impacto medioambiental		
Priorización de las actividades más críticas necesarias para la operaciones diarias		
Detección de señales de advertencia temprana, revisiones, gestión de problemas		
Investigación exclusiva de peligros potenciales ocultos		
Seguimiento crítico de crisis pasadas		
Programas estrictos de inspección y mantenimiento		
SUBTOTAL		

	SI	NO
D Actividades de comunicación		
Entrenamiento de los medios de comunicación para la GC		
Esfuerzos importantes en relaciones públicas		
Aumento de la información a la población local		
Potenciación de las relaciones con grupos de interés que intervienen(policias, medios)		
Potenciación de la colaboración entre grupos de interés		
Uso de los nuevos canales y tecnologías de comunicación		
Números de teléfono dedicados a avisos y reclamaciones de los clientes		
SUBTOTAL		

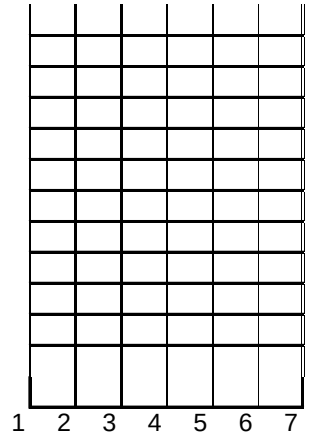
	SI	NO
E Actividades psicológicas y culturales		
Fuerte compromiso de la alta dirección con la GC		
Potenciación de las relaciones con grupos activistas		
Mejor aceptación de los alarmistas		
Más trasparencia acerca de los impactos humanos y emocionales de las crisis		
Apoyo psicológico a los empleados		
Gestión de la tensión de la ansiedad		
Conmemoración simbólica y memoria corporativa de crisis y peligros pasados		
Seguimiento de percepciones culturales en grupos de empleados		
SUBTOTAL		
TOTAL APARTADOS A-E		

HERRAMIENTA DIAGNOSTICA FASES
Fuente: Como Gestionar una Crisis, Ian Mitroff adaptada por el autor

En la escala de 1 a 7, puntuar lo bien o mal que su organización gestiona las sub-fases de la GC
Puntuar la opinión que le merece cada uno de los items en la linea de la derecha

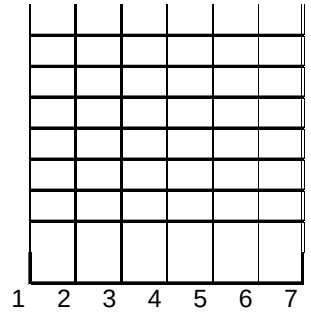
No existe este programa **El programa da una total cobertura**

Sub-fase 1: detección de señales
Mecanismos de detección de señales(MDS) para cualquier crisis
MDS para la crisis mas probable
MDS para una amplia gama de crisis
MDS basados en base de datos existentes
Equipo interno dedicado a probar los procedimientos
Reconocimiento y gratificaciones a la gente que usa MDS
Descripciones formales de trabajo que incluyen el uso de MDS
Estructura informativa centrada en la GC
Punto central de recepción de señales detectadas
Recopilación de estadísticas sobre crisis y casi-crisis
Apoyo cultural a la detección de señales



Puntuación media estimada:

Sub-fase 2: preparación/prevención
Sondeos obligatorios para descubrir crisis
Mantenimiento e inspección regular de todas las instalaciones
Procedimientos y manuales técnicos formales que usan herramientas de GC(análisis de riesgos)
Análisis de factores humanos del equipo crítico
Control de la cantidad de trabajo para evitar excesos
Gestión de la complejidad del sistema para evitar excesos
Incorporación de aprendizaje organizacional a medida que avanzan los sistemas y las tecnologías

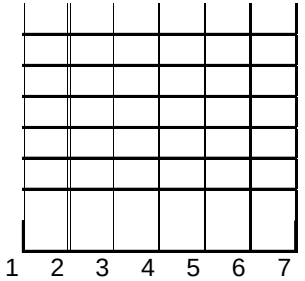


Puntuación media estimada:

Sub-fase 3: contención/limitación de daños

Mantenimiento de información de contención
Actualización de capacidades de contención
Prueba de capacidades de contención
Implementación de mecanismos de contención
Reconocimiento y gratificación de la contención de daños
Asignación de responsabilidades de contención de daños

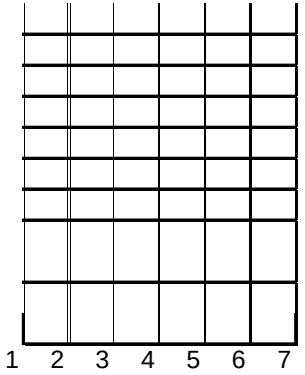
Puntuación media estimada:



Sub-fase 4: recuperación

Identificación de grupos de interés mas importantes para la recuperación
Identificación de tareas, servicios y productos mínimos necesarios para mantener la actividad
Obtención de recursos necesarios para apoyar la reanudación mínima
Identificación de necesidades in situ y externas
Identificación de medios de autosuficiencia si la crisis causa aislamiento del resto de la compañía
Priorización de necesidades mínimas
Establecimiento de las redundancias mas críticas para la reanudación de la actividad
Asesoramiento de interacciones potenciales entre solicitudes tecnológicas y humanas en los planes de recuperación

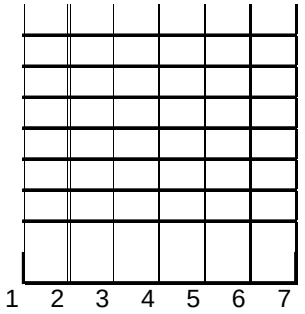
Puntuación media estimada:



Sub-fase 5: aprendizaje

Revisión de crisis o casi-crisis
Revisión de la gestión de crisis, sin culpas
Contraste de cosas bien hechas con cosas hechas de manera deficiente
Generalización de aprendizaje a otras crisis potenciales
Reconocimiento formal de las lecciones aprendidas
Tormenta de ideas y creatividad dentro de los equipos de revisión de GC
Recuerdo y reconocimiento formal de los aniversarios de las crisis

Puntuación media estimada:



HERRAMIENTA DIAGNOSTICA SISTEMAS
Fuente: Como Gestionar una Crisis, Ian Mitroff, adaptada por el autor

Describa su organización como un todo, indicando su grado de identificación, en la escala de 1(muy en desacuerdo) al 7(muy de acuerdo), con las siguientes afirmaciones:

A **Sistema técnico**

Se realizan análisis de riesgo y avería de las instalaciones y equipos importantes
Existen manuales y listas técnicas de comprobación para instalaciones y equipos importantes
Se realizan regularmente revisiones de mantenimiento
Los sistemas técnicos importantes estan integrados mediante ingeniería de sistemas
El análisis de riesgo se realiza regularmente
Los sistemas de advertencia son fáciles de reconocer
Hay sistemas de advertencia instalados para alertar a los operarios de que se ha producido un error
Es fácil diferenciar entre distintos sistemas de advertencia
Hay sistemas de control y manejo centralizados para sistemas técnicos criticos

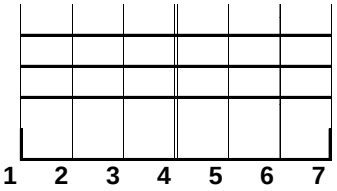
Puntuacion promedio estimada:

B **Sistemas de infraestructura**

Los sistemas de comunicación estan integrados para la GC
Los sistemas de gratificación incorporan la GC
Las estrategias de negocio incorporan la GC
Las descripciones/instrucciones de trabajo incorporan la responsabilidad de GC
Existe un equipo de crisis (EGC)
Nuestro EGC se reúne regularmente
Se llevan acabo simulaciones de crisis regularmente
Nuestros planes de crisis implican a empleados de todos los niveles.
Tenemos entrenamiento de tensión para la GC
Tenemos ayuda empocional para la GC
Premiamos a la gente que informa de noticias potencialmente malas, aún cuando no dan soluciones
Premiamos a la gente que tiene un buen historial de seguridad
Premiamos a la gente que tiene un buen historial de mantenimiento
Tenemos un punto receptor central para recoger información sobre crisis y casi-crisis

Si una planta o división necesita recursos por razones de seguridad, se los damos
Hay recursos disponibles para analizar los planes para impedir averías
Nuestra organización tiene recursos humanos suficientes para que el trabajo se realice sin problemas

Puntuación promedio estimada:

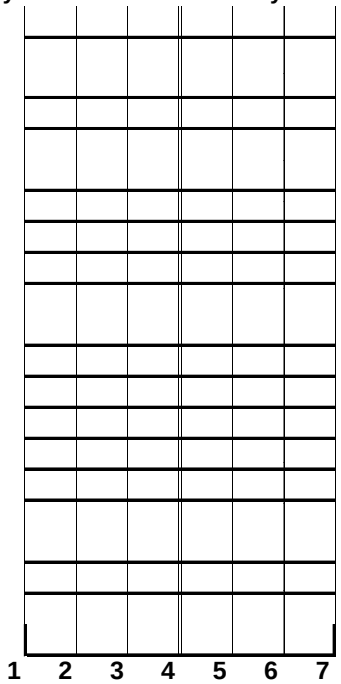


C Sistemas de factores humanos

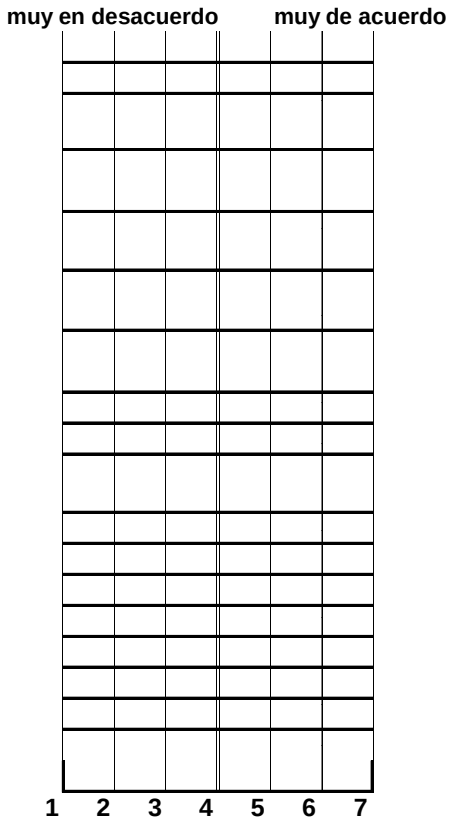
muy en desacuerdo **muy de acuerdo**

Se llevan a cabo auditorías de factores humanos en los departamentos y plantas importantes
Nuestros sistemas de control se diseñan y se registran para que sean de fácil uso y acceso por parte de los operarios
Investigamos problemas o errores de diseño apuntados por nuestros operarios
La cantidad de información que necesita un operario para manejar los equipos clave se tiene en cuenta en el diseño de sistemas clave
Se evalúan los requerimientos físicos para manejar el equipo de una forma efectiva
Se evalúa la tensión física y emocional que conlleva usar el equipo
La complejidad de los equipos y sistemas no ha aumentado significativamente en los ultimos años
Nuestro entrenamiento mantiene a la gente al día sobre cómo manejar nuestros equipos y sistemas más nuevos.
Las actividades normales no sobrecargan la capacidad de manejar información de los gerentes
Las actividades normales no sobrecargan la capacidad de los operarios para llevar a cabo sus tareas
Existe la responsabilidad formal de mantener al dia los manuales de procedimiento
Los manuales de procedimientos son fáciles de comprender
Hay botones de pare para operaciones críticas
Si el trabajo está informatizado o automatizado, los operarios saben cómo evitar al sistema en caso necesario
Los nuevos trabajadores reciben un entrenamiento adecuado antes de quedarse solos en el puesto

Puntuación promedio estimada:



D **Sistema de cultura, parte 1**



En nuestra organización se valora mucho las prácticas de seguridad
No valoramos más la productividad que la seguridad
Se les da la oportunidad a gerentes, ingenieros y operarios de discutir procedimientos operativos normales
Se les da la oportunidad a gerentes, ingenieros y operarios de discutir procedimientos operativos de emergencia.

Después de un accidente, se les pide a las personas implicadas que discutan las lecciones aprendidas

Hay una línea abierta de comunicación entre la dirección y los trabajadores sobre el asuntos de seguridad
La gente de nuestra organización consigue recursos suficientes para hacer el trabajo bien hecho la primera vez
La moral de la organización es correcta
Los empleados comprenden la comunicación proveniente de los nieveles más altos

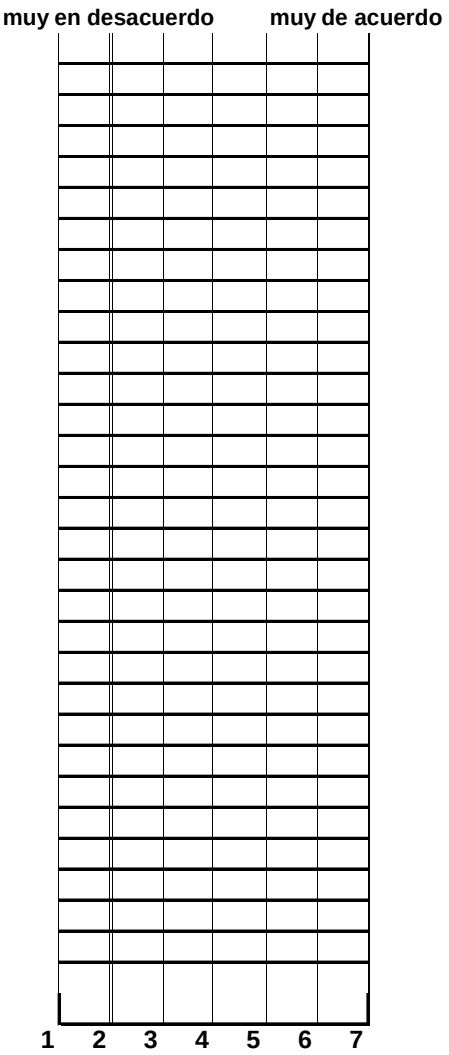
La gente del nivel superior de la organización consigue información importante de los niveles inferiores
Los empleados de las diferentes áreas funcionales hablan entre ellos
Los empleados de las diferentes áreas geográficas hablan entre ellos
Mantenemos informados a nuestros grupos de interés externos
Nuestros grupos de interés externos nos mantienen informados
Los empleados comprenden los valores que imperan en la organización
Los valores que aplicamos día a día son los mismos valores que nosotros predicamos
La gente de nivel superior pone buenos ejemplos para la seguridad

Puntuación promedio estimada:

E **Sistema de cultura parte 2**

El tamaño de nuestra organización nos protegera de crisis importantes
Nuestra especial ubicación nos protegerá
Las compañías excelentes y bien administradas no tienen crisis
Las crisis no requieren de procedimeintos especiales
Basta con reaccionar a una crisis cuando ésta se haya producido
La gestión de crisis es un lujo
Los empleados portadores de malas noticias merecen ser castigados
Los fines deseables para el negocio justifican medios de alto riesgo
La dedicación de nuestros empleados es tanta que podemos confiar en ellos
Si sucede una crisis importante, alguien nos rescatará
La GC es responsabilidad de otros
El medio ambiente es benigno
No ha ocurrido nada nuevo que justifique un cambio en nuestros procedimientos
No es una crisis si no nos sucede o nos perjudica a nosotros
Los posibles delitos perpetrados por nuestros empleados son un coste de hacer negocios
La mayoria de las crisis resultan no ser muy importantes
Cada crisis es única, así que no es posible prepararse para las crisis
Las crisis son únicamente negativas en su impacto
Las crisis son aisladas
La mayoría de las crisis pueden resolverse con la tecnología
Basta con dar una atención técnica y financiera, y una solución rápida a los problemas
La mayoría de las crisis se resuelven solas
La mayoría de las crisis son culpa de un único individuo malvado
La GC son como los seguros solo necesita cubrirse hasta cierto punto
En una crisis simplemente tenemos que remitirnos a nuestros manuales de GC
Somos un equipo que funcionará bien durante una crisis
Solo los altos ejecutivos necesitan estar enterados de nuestros planes de GC
La única cosa importante es asegurar que nuestras operaciones internas permanecen intactas
Nosotros somos suficientemente duros para reaccionar de forma objetiva y racional
Sabemos cómo manipular a los medios

Puntuación promedio estimada:



F **Sistema emocional**

Se permite a la gente expresar sus sentimientos
La gente es conciente de que las crisis dejan secuelas emocionales
Se le da a la gente preparación para los aspectos emocionales y traumáticos de las crisis
Nuestro programa de ayuda a los empleados incluye asistencia emocional para crisis
Después de una crisis o casi-crisis organizacional se entrevista a la gente para evaluar el alcance del impacto psicológico

Después de una crisis o casi crisis los implicados reciben asesoria emocional y para los traumas.
Es bien recibido que alguien pida consejo o terapia psicológica para problemas emocionales
Es bien recibido quien comparte y expresa honestamente sus emociones

Puntuacion promedio estimada:

HERRAMIENTA DIAGNÓSTICA PARA GRUPOS DE INTERÉS

Fuente: Como Gestionar una Crisis, Ian Mitroff, pág. 90, Adaptada por el autor

¿Cuales de estos grupos de interés son los tenidos en cuenta en los planes de GC de su organización? Marque las categorías que procedan

Clientes	☐
Competidores	☐
Grupos de especial interés	☐
Reguladores	☐
Alta dirección	☐
Mandos intermedios	☐
Trabajadores	☐
Sindicato	☐
Medios de comunicación	☐
Junta directiva	☐

Total **----------**

¿Cuales de estos grupos de interés colaboran en la elaboración de planes de GC?

Consejero delegado	☐
Oficina central de predicción	☐
Consejero legal	☐
Representante de relaciones publicas	☐
Representante de seguridad	☐
Representante de recursos humanos	☐
Representante de operaciones	☐
Representante de ventas	☐
Representante de seguridad/asuntos medioambientales	☐
Representante de los mandos intermedios	☐
Representante de los trabajadores	☐

Total **----------**

PLANIFICACION DE LA GESTION DE CRISIS Y CONTINUIDAD DEL NEGOCIO

Fuente: US. Department Homeland Security. Ejemplo de Plan para la Continuidad del Negocio y Preparación para Desastres. Adaptada por el autor.

Lugar de operación normal	**Lugar de operación alternativo**
Nombre de la Compañía _____ Dirección _____ Ciudad, Provincia _____ Número de Teléfono _____	Nombre de la Compañía _____ Dirección _____ Ciudad, Provincia _____ Número de Teléfono _____

La siguiente persona estará a cargo de gestionar la crisis y será el portavoz de la compañía en caso de emergencia.

_____

Contacto Primario de Emergencia

_____

Número de Teléfono

_____

Número Alternativo

_____

Correo electrónico

En ausencia de la persona principal estará a cargo de gestionar la crisis esta persona.

_____

Contacto Secundario de Emergencia

_____

Número de Teléfono

_____

Número Alternativo

_____

Correo electrónico

INFORMACION DE CONTACTOS DE EMERGENCIA

Marque 9-1-1 en caso de emergencia

_____

Policía/Bomberos - No Emergencias

_____

Proveedor de Seguros

MANTÉNGANSE INFORMADO

Los siguientes RIESGOS naturales y causados por el hombre podrían afectar nuestro negocio:

Riesgos	**Plan de acción**	**Archivo**

EQUIPO DE GESTION DE CRISIS

Las siguientes personas participarán en la planificación de emergencias y la gestión de crisis:

Nombre	**Area**	**Ext.**	**Número teléfono**

Las siguientes personas de los negocios vecinos participarán en nuestro equipo de GC:

_____

_____

_____

_____

Comunicaremos nuestros planes de emergencia con compañeros de trabajo de la siguiente forma:

_____

_____

En caso de desastre, nos comunicaremos con los empleados de la siguiente forma:

_____

_____

PROVEEDORES

Nombre de la Compañía: _____

Dirección: _____Ciudad: _____

Provincia: _____Código Postal: _____

Teléfono: Fax: Correo electrónico: _____

Nombre de Contacto: Número de Cuenta: _____

Materiales/Servicios Proporcionados: _____

Si esta compañía sufre un desastre, obtendremos los suministros/materiales de la siguiente:

Nombre de la Compañía: _____

Dirección: _____Ciudad: _____

Provincia: _____Código Postal: _____

Teléfono: Fax: Correo electrónico: _____

Nombre de Contacto: Número de Cuenta: _____

Materiales/Servicios Proporcionados: _____

PLAN DE EVACUACION PARA LAS INSTALACIONES

Hemos elaborado estos planes en colaboración con los negocios vecinos y los propietarios del edificio para evitar confusión.

Hemos encontrado, copiado y publicado mapas del edificio y de las instalaciones.

Las salidas están claramente marcadas.

Practicaremos los procedimientos de evacuación _____veces por año.

Si debemos abandonar rápidamente el lugar de trabajo:

_____

_____

1. Sistema de advertencia

_____

Probaremos el sistema de advertencia y registraremos los resultados _____ veces por año.

2. Lugar de reunión:

_____

4. Persona responsable/coordinador para el lugar de reunión:

_____

a. Algunas responsabilidades:

_____

_____

4. _____ es responsable de emitir la orden de "todo despejado".

COPIA DE SEGURIDAD DE LOS ARCHIVOS

_____ es responsable de hacer copias de seguridad de nuestros archivos cruciales, incluidos los sistemas de nómina del personal y de contabilidad.

Las copias de seguridad, incluyendo una copia de este plan, mapas del sitio, pólizas de seguro, registros bancarios y copias de seguridad informáticas están en nuestras instalaciones en

_____.

Otro juego de copias de seguridad está guardado en este lugar fuera de las instalaciones:

_____

Si nuestros registros de contabilidad y nómina de personal resultan destruidos, mantendremos la continuidad de la siguiente forma:

_____

_____

INFORMACION DE CONTACTO EN EMERGENCIA DE LOS EMPLEADOS

La siguiente es una lista de nuestros compañeros de trabajo y su información de contacto de emergencia individual:

Nombre	**Número teléfono**	**Número alternativo(cel)**

REVISION ANUAL

Revisaremos y actualizaremos este plan de continuidad del negocio y de desastres en _____.

COMITÉ DE GC DE LA COMPAÑIA

ANEXO Nº 2

RESULTADOS DEL CASO PRACTICO:

RESULTADOS DEL DIAGNOSTICO DE FASES

RESULTADOS DEL DIAGNOSTICO DE SISTEMAS

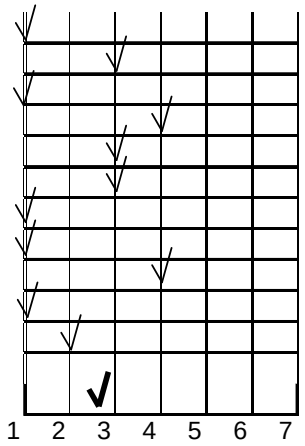
RESULTADOS DEL DIAGNOSTICO DE GRUPOS DE INTERES

HERRAMIENTA DIAGNOSTICA FASES
Caso Práctico : Empresa Tecnológica

En la escala de 1 a 7, puntuar lo bien o mal que su organización gestiona las sub-fases de la GC
Puntuar la opinión que le merece cada uno de los items en la linea de la derecha

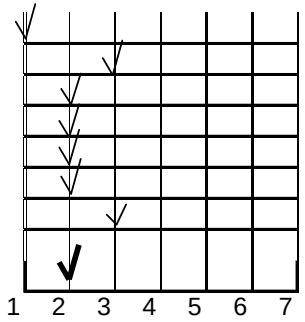
No existe este programa **El programa da una total cobertura**

Sub-fase 1: detección de señales
Mecanismos de detección de señales(MDS) para cualquier crisis
MDS para la crisis más probable
MDS para una amplia gama de crisis
MDS basados en base de datos existentes
Equipo interno dedicado a probar los procedimientos
Reconocimiento y gratificaciones a la gente que usa MDS
Descripciones formales de trabajo que incluyen el uso de MDS
Estructura informativa centrada en la GC
Punto central de recepción de señales detectadas
Recopilación de estadísticas sobre crisis y casi-crisis
Apoyo cultural a la detección de señales



Puntuación media estimada:

Sub-fase 2: preparación/prevención
Sondeos obligatorios para descubrir crisis
Mantenimiento e inspección regular de todas las instalaciones
Procedimientos y manuales técnicos formales que usan herramientas de GC(análisis de riesgos)
Análisis de factores humanos del equipo crítico
Control de la cantidad de trabajo para evitar excesos
Gestión de la complejidad del sistema para evitar excesos
Incorporación de aprendizaje organizacional a medida que avanzan los sistemas y las tecnologías

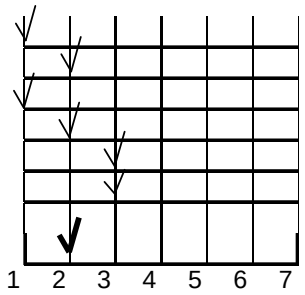


Puntuación media estimada:

Sub-fase 3: contención/limitación de daños

Mantenimiento de información de contención
Actualización de capacidades de contención
Prueba de capacidades de contención
Implementación de mecanismos de contención
Reconocimiento y gratificación de la contención de daños
Asignación de responsabilidades de contención de daños

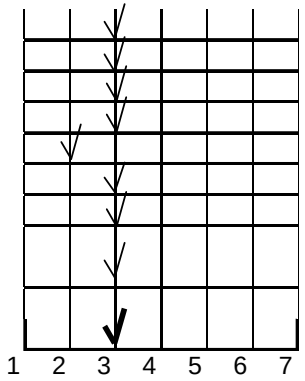
Puntuación media estimada:



Sub-fase 4: recuperación

Identificación de grupos de interés mas importantes para la recuperación
Identificación de tareas, servicios y productos mínimos necesarios para mantener la actividad
Obtención de recursos necesarios para apoyar la reanudación mínima
Identificación de necesidades in situ y externas
Identificación de medios de autosuficiencia si la crisis causa aislamiento del resto de la compañía
Priorización de necesidades mínimas
Establecimiento de las redundancias mas críticas para la reanudación de la actividad
Asesoramiento de interacciones potenciales entre solicitudes tecnológicas y humanas en los planes de recuperación

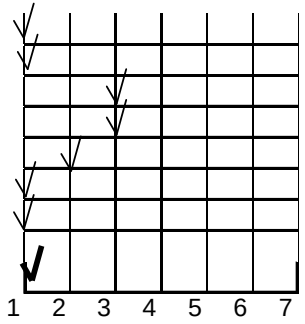
Puntuación media estimada:



Sub-fase 5: aprendizaje

Revisión de crisis o casi-crisis
Revisión de la gestión de crisis, sin culpas
Contraste de cosas bien hechas con cosas hechas de manera deficiente
Generalización de aprendizaje a otras crisis potenciales
Reconocimiento formal de las lecciones aprendidas
Lluvia de ideas y creatividad dentro de los equipos de revisión de GC
Recuerdo y reconocimiento formal de los aniversarios de las crisis

Puntuación media estimada:



HERRAMIENTA DIAGNOSTICA SISTEMAS
Caso Practico : Empresa Tecnológica

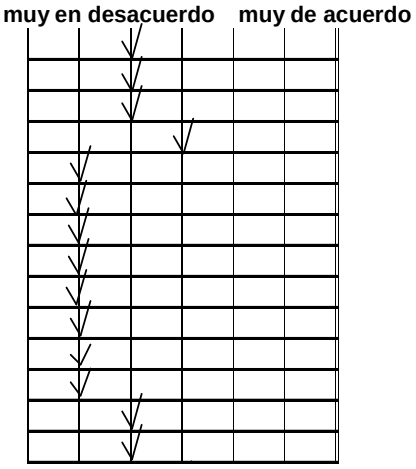
Describa su organización como un todo, indicando su grado de identificación, en la escala de 1(muy en desacuerdo) al 7(muy de acuerdo), con las siguientes afirmaciones:

A Sistema técnico

Se realizan análisis de riesgo de las instalaciones y equipos importantes
Existen manuales y listas técnicas de comprobación para instalaciones y equipos importantes
Se realizan regularmente revisiones de mantenimiento
Los sistemas técnicos importantes estan integrados mediante ingeniería de sistemas
El análisis de riesgo se realiza regularmente
Los sistemas de advertencia son fáciles de reconocer
Hay sistemas de advertencia instalados para alertar a los operarios de que se ha producido un error
Es fácil diferenciar entre distintos sistemas de advertencia
Hay sistemas de control y manejo centralizados para sistemas técnicos criticos

Puntuacion promedio estimada:

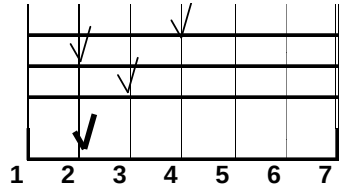
B Sistemas de infraestructura



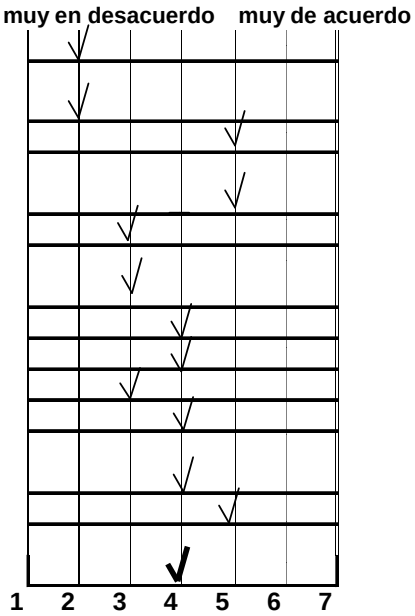
Los sistemas de comunicación estan integrados para la GC
Los sistemas de gratificación incorporan la GC
Las estrategias de negocio incorporan la GC
Las descripciones/instrucciones de trabajo incorporan la responsabilidad de GC
Existe un equipo de crisis (EGC)
Nuestro EGC se reúne regularmente
Se llevan acabo simulaciones de crisis regularmente
Nuestros planes de crisis implican a empleados de todos los niveles.
Tenemos entrenamiento de tensión para la GC
Tenemos ayuda empocional para la GC
Premiamos a la gente que informa de noticias potencialmente malas, aún cuando no dan soluciones
Premiamos a la gente que tiene un buen historial de seguridad
Premiamos a la gente que tiene un buen historial de mantenimiento
Tenemos un punto receptor central para recoger información sobre crisis y casi-crisis

Si una planta o división necesita recursos por razones de seguridad, se los damos
Hay recursos disponibles para analizar los planes para impedir fallas
Nuestra organización tiene recursos humanos suficientes para que el trabajo se realice sin problemas

Puntuación promedio estimada:



C Sistemas de factores humanos



Se llevan a cabo auditorías de factores humanos en los departamentos
Nuestros sistemas de control se diseñan y se registran para que sean de fácil uso y acceso por parte de los operarios
Investigamos problemas o errores de diseño apuntados por nuestros operarios
La cantidad de información que necesita un operario para manejar los equipos clave se tiene en cuenta en el diseño de sistemas clave
La complejidad de los equipos y sistemas no ha aumentado significativamente en los ultimos años
Nuestro entrenamiento mantiene a la gente al día sobre cómo manejar nuestros equipos y sistemas más nuevos.
Las actividades normales no sobrecargan la capacidad de manejar información de los gerentes
Las actividades normales no sobrecargan la capacidad de los operarios para llevar a cabo sus tareas
Existe la responsabilidad formal de mantener al dia los manuales de procedimiento
Los manuales de procedimientos son fáciles de comprender
Si el trabajo está informatizado o automatizado, los operarios saben cómo evitar al sistema en caso necesario
Los nuevos trabajadores reciben un entrenamiento adecuado antes de quedarse solos en el puesto

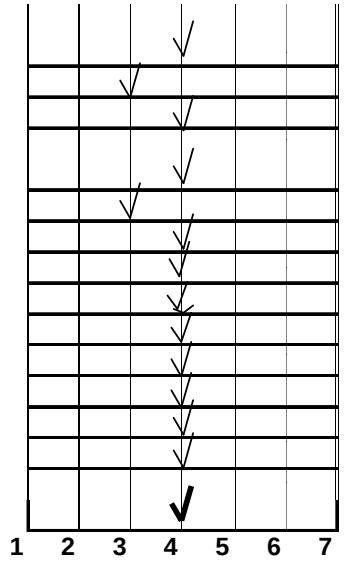
Puntuación promedio estimada:

D Sistema de cultura, parte 1

En nuestra organización se valora mucho las prácticas de seguridad
No valoramos más la productividad que la seguridad
Se les da la oportunidad a gerentes, ingenieros y operarios de discutir procedimientos operativos normales

Se les da la oportunidad a gerentes, ingenieros y operarios de discutir procedimientos operativos de emergencia.
Después de un accidente, las personas implicadas que discuten las lecciones aprendidas.
Hay una línea abierta de comunicación entre la dirección y los trabajadores sobre el asuntos de seguridad
La gente de nuestra organización consigue recursos suficientes para hacer el trabajo bien hecho la primera vez
La moral de la organización es correcta
Los empleados comprenden la comunicación proveniente de los nieveles más altos
La gente del nivel superior de la organización consigue información importante de los niveles inferiores
Los empleados de las diferentes áreas funcionales hablan entre ellos
Mantenemos informados a nuestros grupos de interés externos
Nuestros grupos de interés externos nos mantienen informados
Los empleados comprenden los valores que imperan en la organización
Los valores que aplicamos día a día son los mismos valores que nosotros predicamos
La gente de nivel superior pone buenos ejemplos para la seguridad

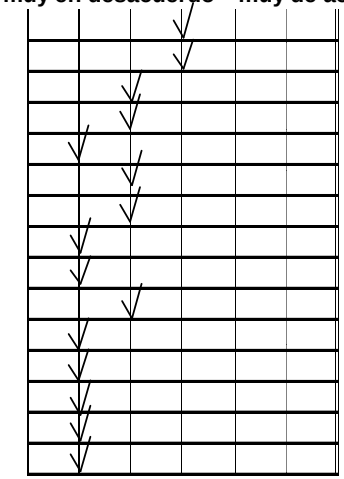
Puntuación promedio estimada:



E Sistema de cultura parte 2

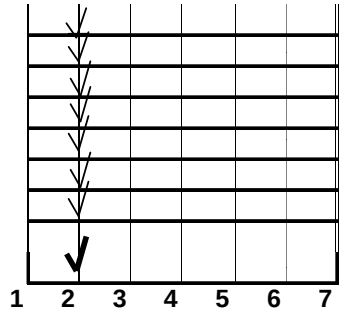
muy en desacuerdo **muy de acuerdo**

El tamaño de nuestra organización nos protegera de crisis importantes
Las compañías excelentes y bien administradas no tienen crisis
Basta con reaccionar a una crisis cuando ésta se haya producido
La gestión de crisis es un lujo
Los empleados portadores de malas noticias merecen ser castigados
Los fines deseables para el negocio justifican medios de alto riesgo
La dedicación de nuestros empleados es tanta que podemos confiar en ellos
Si sucede una crisis importante, alguien nos rescatará
El medio ambiente es benigno
No ha ocurrido nada nuevo que justifique un cambio en nuestros procedimientos
Los posibles delitos perpetrados por nuestros empleados son un coste de hacer negocios
Cada crisis es única, así que no es posible prepararse para las crisis
Las crisis son aisladas
La mayoría de las crisis pueden resolverse con la tecnología
Basta con dar una atención técnica y financiera, y una solución rápida a los problemas



La mayoría de las crisis se resuelven solas
En una crisis simplemente tenemos que remitirnos a nuestros manuales de GC
Somos un equipo que funcionará bien durante una crisis
Solo los altos ejecutivos necesitan estar enterados de nuestros planes de GC
La única cosa importante es asegurar que nuestras operaciones internas permanecen intactas
Nosotros estamos suficientemente preparados para reaccionar de forma objetiva y racional
Sabemos cómo manipular a los medios

Puntuación promedio estimada:



F Sistema emocional

Se permite a la gente expresar sus sentimientos
La gente es conciente de que las crisis dejan secuelas emocionales
Se le da a la gente preparación para los aspectos emocionales y traumáticos de las crisis
Nuestro programa de ayuda a los empleados incluye asistencia emocional para crisis
Después de una crisis o casi-crisis organizacional se entrevista a la gente para evaluar el alcance del impacto psicológico
Después de una crisis o casi crisis los implicados reciben asesoria emocional y para los traumas.
Es bien recibido que alguien pida consejo o terapia psicológica para problemas emocionales
Es bien recibido quien comparte y expresa honestamente sus emociones

Puntuacion promedio estimada:

HERRAMIENTA DIAGNÓSTICA PARA GRUPOS DE INTERÉS

¿Cuales de estos grupos de interés son los tenidos en cuenta en los planes de GC de su organización? Marque las categorías que procedan

Clientes	☑
Competidores	☑
Grupos de especial interés(proveedores)	☐
Reguladores(estado)	☑
Alta dirección	☐
Mandos intermedios	☑
Trabajadores	☑
Sindicato	☐
Medios de comunicación	☐
Junta directiva	☐

Total **------- 5 ---------**

¿Cuales de estos grupos de interés colaboran en la elaboración de planes de GC?

Consejero delegado	☐
Oficina central de predicción	☐
Consejero legal	☐
Representante de relaciones publicas	☐
Representante de seguridad	☐
Representante de recursos humanos	☐
Representante de operaciones	☑
Representante de ventas	☐
Representante de seguridad/asuntos medioambientales	☐
Representante de los mandos intermedios	☑
Representante de los trabajadores	☑

Total **-------- 3 ---------**