UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

PROGRAMA DE MAESTRÍA Y DOCTORADO EN INGENIERÍA
INGENIERÍA DE SISTEMAS – PLANEACIÓN

SISTEMA DE PLANEACIÓN PARA LA PREVENCIÓN DE CRISIS DE ORIGEN SOCIO-TÉCNICO EN ÁREAS DE GESTIÓN DE TIC

TESIS
QUE PARA OPTAR POR EL GRADO DE:
MAESTRO EN INGENIERÍA

PRESENTA:
ING. HERIBERTO GARCÍA LEDEZMA

DR. BENITO SÁNCHEZ LARA
FACULTAD DE INGENIERÍA

MÉXICO, D.F. NOVIEMBRE DE 2015

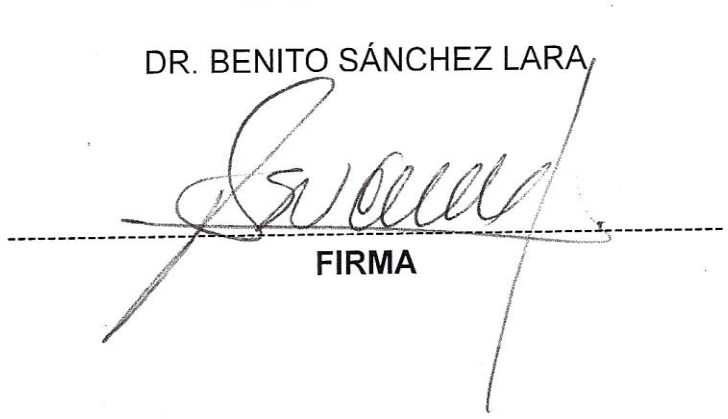
JURADO ASIGNADO:

Presidente:	M.I. ARTURO FUENTES ZENÓN
Secretario:	DR. MARIANO ANTONIO GARCÍA MARTÍNEZ
Vocal:	DR. BENITO SÁNCHEZ LARA
1 er. Suplente:	DR. TOMÁS BAUTISTA GODINEZ
2 do. Suplente:	DRA. NELLY RIGAUD TÉLLEZ

Ciudad Universitaria, México, D.F.

TUTOR DE TESIS:

DR. BENITO SÁNCHEZ LARA



FIRMA

Agradecimientos

Gracias por esta vida…

Dedico este trabajo a quien ha sido mi principal ejemplo de vida: mi madre Yolanda. Gracias por todo tu amor y apoyo. Gracias por nunca darte por vencida y por mostrarme que con esfuerzo y dedicación puedes conseguir lo que te propongas.

Yuri y a Abi, este trabajo también lo dedico a ustedes. Hermanos, su apoyo y cariño fue esencial para que pudiera alcanzar esta meta. Gracias pequeña Thayli por dar más alegría a mi vida.

Dr. Benito Sánchez Lara, profesor, tutor y amigo. Gracias por sus invaluables consejos y el tiempo dedicado en este proceso. Su guía excepcional fue importantísima para este logro.

Gracias a los expertos en gestión de TIC y a los sinodales que revisaron este trabajo por dedicar su valioso tiempo y por compartir parte de su experiencia profesional a través de sus respuestas y comentarios.

A mis amigos George, Neiha y Yaz, gracias por su apoyo en este tiempo que dediqué a la Maestría. Gracias Sally 🐾 por hacerme compañía a lo largo de tantas horas de redacción.

Mi gratitud también a Saynez, Koko, Yare, Mena, Char, Circe, Marco, Migue y demás amigos del laboratorio de cómputo del Departamento de Ingeniería en Computación. Sus comentarios, bromas, reuniones y *rides* me ayudaron mucho en la Maestría.

De igual manera agradezco a mis amigos del CENAPRED, que desde el momento en que supieron que estaba por estudiar la Maestría me dieron todo su apoyo.

A mis colegas *sistémicos* en esta aventura (Abraham, Gerard, Joss, Mexique, Oli, Robert y Víc), gracias por tantos momentos de compañerismo, de alegría, de dedicación, de profesionalismo y de esfuerzo. Ha sido una gran experiencia. Me siento muy afortunado por conocerlos y de tenerlos como mis amigos.

Gracias a Uriel, Javier, Daniel, Luis, Rosa, Marisol, Sra. Reyna, Dra. Mayra, Montserrat y a todas las demás personas que conocí en el laboratorio de planeación. Su apoyo y alegría fue muy importante para mí.

A mis compañeros de la generación 50 de la Maestría en Planeación, de la que me siento orgulloso de pertenecer, y a mis profesores de Maestría les agradezco por compartir sus conocimientos y experiencias.

Mi reconocimiento y agradecimiento a instituciones como la Facultad de Ingeniería, a la UNAM y al CONACYT, por apoyar en la formación profesional y científica de tantas personas que se esfuerzan cada día por mejorar.

Son tantas las personas a las que tengo que agradecer por el apoyo que me brindaron para realizar este trabajo y tantas las formas en que lo hicieron que sin duda llenaría varias páginas más. A todos ustedes que me ayudaron y contribuyeron en este proceso con consejos, opiniones, pláticas, su tiempo al escucharme o de cualquier otra forma: Gracias.

“Hola mundo =]”

“Sé puro, sé noble; surge”
Siddhārtha Gautamá

“Se incendió mi casa:
ahora nada me obstruye
la visión de la luna”
Mizuta Masahide

“Vivimos en el mundo cuando amamos.
Sólo una vida vivida para los demás merece la pena ser vivida”
Albert Einstein

“Luna de nieve
matizando de azul
la noche oscura”
Kawabata Bosha

ÍNDICE

RESUMEN

Las Tecnologías de la Información y Comunicación (TIC) tienen presencia en el sector público y en el sector privado debido a que facilitan y mejoran el desempeño de sus actividades. En algunos casos sólo se utilizan como una herramienta de ayuda en los procesos administrativos o productivos, pero en otros casos son un elemento fundamental para el cumplimiento de los objetivos de las organizaciones. Como otras áreas de las instituciones, las áreas de gestión de TIC son propensas a sufrir eventos que alteran su funcionamiento desde niveles mínimos hasta niveles severos lo cual afecta el desempeño del resto de la organización. Ante este tipo de situaciones se tienen planes de contingencia que una vez que sucede un evento perturbador que afecta el desempeño del área de TIC, buscan el restablecimiento de las operaciones esenciales y después se ocupan de regresar a la normalidad el resto de las funciones. La conveniencia de este tipo de planes es irrefutable; sin embargo, sus acciones tienen un punto cuestionable por definición: su carácter reactivo ante un suceso no deseado. Lo que se propone en este trabajo es atender las crisis en áreas de gestión de TIC desde un punto de vista proactivo, en el que se identifiquen elementos que pueden causar dichas situaciones y generar planes para eliminar o disminuir sus efectos. Por ser un área técnica, la mayoría de los planes de atención a crisis existentes para los departamentos de gestión de TIC se enfocan en crisis de tipo técnico y se desatiende otro factor igual de importante: el organizacional.

Este trabajo se enfoca en estas 2 perspectivas y las combina para proponer un *Sistema de Planeación para la prevención de crisis de origen socio-técnico*. Dicho sistema tiene como objetivo establecer directrices para la formulación de planes de atención que consideren el aspecto social y técnico de las áreas de gestión de TIC como causa de riesgo y también como base para la propuesta de soluciones. El fundamento teórico que se ocupa para la formulación de este *Sistema de Planeación* es el enfoque socio-técnico desarrollado inicialmente en el Instituto Tavistock por Emery y Trist (Jackson, 2000), además del desarrollo organizacional (Lalonde, 2011).

Para el desarrollo del *Sistema de Planeación* se tomaron en cuenta modelos respecto a la prevención de crisis en general y modelos que tratan la atención de desastres socio-técnicos técnicos (Aini & Fakhrul-Razi, 2010; Ibrahim M. Shaluf, Ahmadun, Said, Mustapha, & Sharif, 2002; Tarn, Wen, & Shih,

2008). Se ocupó como método planeación el *Subsistema de Planeación* propuesto en Gelman & Negroe (1982), que apoya en el proceso de conducción que lleva a cabo un sistema conducente sobre uno conducido; además para generar el *Sistema de Planeación* se ocupó la *construcción por descomposición* desde la perspectiva indicada también en Gelman & Negroe (1982).

Una vez definido el *Sistema de Planeación* fue necesario buscar una validación de la correspondencia inicial con la realidad de acuerdo con lo indicado en Sagasti & Mitroff (1973) y saber qué tan útil, compatible y factible es llevarlo a cabo para áreas de gestión de TIC. Para esto se diseñó un cuestionario de validación que se aplicó a once expertos en el tema y a través del cual se registraron sus opiniones una vez que se les explicaron los objetivos y el funcionamiento con base en el modelo del sistema generado.

Como resultado de este trabajo se observa que el aspecto organizacional y social determina de forma importante el desempeño de los departamentos de gestión de TIC y que esto es un tema que los administradores de esas áreas reconocen y están interesados en atender. Las opiniones expresadas por los expertos consultados indican que el *Sistema de Planeación* propuesto es útil por el enfoque preventivo y por el tipo de riesgos al que se refiere. Se concluye también que su factibilidad de aplicación depende de varios factores en los que está envuelta el área de TIC, desde aspectos financieros, recursos humanos, formas arraigadas de realizar las actividades, y procedimientos y políticas de la organización.

Este Sistema de Planeación no pretende indicar una solución definitiva al problema de las crisis con origen socio-técnico en áreas de gestión de TIC ni tampoco indicar exactamente los pasos a seguir o metodologías ni herramientas en particular a usar. En lugar de eso se pretende que sea una guía útil para establecer directrices en la formulación de planes de eliminación o mitigación de riesgos del tipo indicado y planes de respuesta en caso de que lleguen a presentarse. Por otro lado, es necesario establecer que el tipo de entidades para las propone son aquellas que tienen un área dedicada exclusivamente a la gestión de TIC. Las bases principales sobre las que se sustenta y que le dan su valor son el enfoque preventivo, en lugar de reactivo, a situaciones de crisis en áreas de gestión de TIC; y el abordar riesgos de carácter socio-técnico existentes en esas áreas, en vez de sólo atender cuestiones puramente técnicas.

INTRODUCCIÓN

Las Tecnologías de la Información y Comunicación (TIC) se refieren a hardware, software, conocimientos, procedimientos o métodos que permiten la creación, almacenaje, manipulación, procesamiento, recuperación y comunicación de información digital. Mediante ellas se busca una eficiente organización, análisis y uso de dicha información para potencializar la mejora de las condiciones de quienes las ocupan en contextos económicos, sociales, salubres, de innovación y culturales, por mencionar algunos.

En la actualidad es difícil imaginar la vida cotidiana sin la intervención de las TIC. Prácticamente todos los servicios que utilizamos y los productos que ocupamos de alguna manera han dependido de ellas, ya sea en su producción, transporte, mecanismos o instrumentos de compra, por mencionar algunas ideas. A nivel mundial su importancia es reconocida por sectores privados, gubernamentales y organizaciones internacionales (International Telecommunication Union, 2014) (Tawfik, 2000) (Observatorio para la Sociedad de la Información en Latinoamérica y el Caribe, 2004). En el sector privado y en el gubernamental la presencia de las TIC es indiscutible, una gran parte de sus actividades dependen de ellas, particularmente de las TIC que están involucradas en sus procesos internos. Éstas, en organizaciones que han alcanzado cierto grado de madurez son gestionadas por un departamento especializado.

Como en otras áreas en las instituciones, en el campo de la tecnología es posible que se presenten situaciones que comprometen o deterioran su desempeño. En el peor de los casos pueden evolucionar a un nivel de crisis y llegar a mermar o deteriorar el desempeño de las funciones esenciales de la organización e incluso afectar a otros sectores de la sociedad (Bozeman, 2011; I. Mitroff & Alpaslan, 2003; Tarn et al., 2008). Las causas de este tipo de situaciones en las áreas de gestión de TIC son variadas. Pueden ser del tipo de cuestiones técnicas como fallas o desempeño inadecuado de los sistemas técnicos de las organizaciones; cuestiones operacionales como errores en la forma de realizar las actividades asignadas, uso inadecuado de las herramientas, infringir reglamentos o medidas de seguridad o normas de calidad; situaciones organizacionales como inconsistencias en reglamentos internos, en la documentación sobre los procedimientos a realizar, en la desobediencia de normas o

políticas internas, definición ambigua de objetivos o actividades y desorganización en la toma de decisiones; y también se encuentran las causas que incluyen aspectos sociales como consideraciones personales, la forma en que se relaciona el personal, opiniones diversas sobre la forma de trabajo, el reconocimiento que esperan las personas por su trabajo, etcétera.

Los departamentos de gestión de TIC siguen normas de calidad para evitar crisis en tecnologías u ocupan metodologías o planes para el restablecimiento de operaciones cuando ya han sucedido. Sin embargo estas acciones por lo general están orientadas a atender factores técnicos o procedimientos administrativos, y causas sociales u organizacionales pasan desapercibidas; por ejemplo la forma en que se relacionan las personas que trabajan allí, la sensación de valor que tienen de sí mismos por las actividades que realizan, el trabajo en equipo, y el nivel de interés por las actividades que realizan. En este documento se atiende este tipo de factores que pueden causar una crisis en TIC desde enfoque de prevención principalmente. Para esto se desarrolla un *Sistema de Planeación para la prevención de crisis socio-técnicas en áreas de gestión de TIC* y se valida con expertos en el ramo con el fin de saber su nivel de utilidad, conveniencia y factibilidad de aplicación. Las organizaciones para las que está pensado esta forma de planeación son aquellas que en su estructura contienen un departamento dedicado a la gestión de las tecnologías de la información y comunicación que ocupan en sus procesos internos.

Este documento se integra por cuatro capítulos en los que se explica el proceso que se siguió para el desarrollo del *Sistema de Planeación* y su validación, un apartado de conclusiones y un apartado de anexos.

En el primer capítulo se revisan varias concepciones respecto al concepto de Tecnologías de la Información y Comunicación con el fin de formular una definición propia que incluya las áreas de interés de este trabajo. A manera de justificación de la importancia actual de las TIC se presenta información sobre su uso y potencialidad a nivel mundial que tiene como fuente a organizaciones como la International Telecommunication Union (ITU) que es la agencia especializada de las Naciones Unidas para las TIC, y como el World Economic Forum (WEF). Con dicha información se delinea la situación de México a nivel internacional con respecto al uso de las TIC y las formas en las que puede beneficiarse con su desarrollo y difusión. De forma similar se describe un panorama interno del país con respecto al uso de las TIC en el sector gubernamental y privado a partir de datos del Instituto Nacional de Estadística y Geografía (INEGI). Por otro lado, se expone la forma en que las organizaciones han hecho frente a las crisis en TIC y los principales factores que toman en cuenta. Al final del primer capítulo se describe la problemática, y se especifican el problema y el objetivo de este trabajo.

El segundo capítulo presentan los fundamentos teóricos en los que se basa la tesis. Se detallan las características, causas y cuestiones sobre la gestión de crisis en las organizaciones, y también se hace una revisión de cómo se han abordado aquellas que tienen un origen social. A partir de la revisión de dicha información se genera una definición de las crisis socio-técnicas, que es esencial para el desarrollo del producto principal. Para el desarrollo del modelo de planeación fue necesario estudiar enfoques y

modelos formales desarrollados por quienes se han interesado en el tema. Una breve descripción de los principales trabajos revisados con esa investigación se presenta también en este segundo capítulo y se destaca la idea de las crisis como un proceso y no como un evento aislado, razón por la que generar planes de prevención se hace factible. De forma similar se presentan las bases del desarrollo organizacional, del enfoque socio-técnico, y un sistema de planeación visto como apoyo en el proceso de conducción, que representan las directrices con las que se elabora el *Sistema de Planeación*.

Con el capítulo tres se explica este *Sistema de Planeación*. Lo primero que se describe es la forma en cómo se diseñó y se presentan, retoman o formulan definiciones esenciales para este trabajo: riesgos socio-técnicos, sistema, gestión de TIC, sistema de gestión de TIC y *Sistema de Planeación para la prevención de crisis socio-técnicas en áreas de TIC*. Enseguida se detallan los objetivos y actividades de las fases que considera el *Sistema de Planeación*, se explican las relaciones entre ellas y los flujos de información y acción que son necesarios. Para esto se ocupa un esquema gráfico que representa cada una de las fases del modelo, sus componentes y relaciones.

El cuarto capítulo se refiere a la búsqueda de la validación del *Sistema de Planeación*. En la primera parte se habla de cómo fue elaborado el instrumento para este fin, de cómo se aplicó y a quienes. En su segunda mitad se presenta un análisis de la información recabada y se concluye con respecto a 4 aspectos de gran importancia en la evaluación del *Sistema de Planeación*: la utilidad de su aplicación, la compatibilidad con las áreas de gestión de TIC, la factibilidad para poder aplicarlo y las mejoras que se le pueden hacer.

La penúltima sección contiene conclusiones generales respecto al objetivo particular de la tesis, sobre los productos elaborados para conseguirlo y además se incluyen comentarios importantes, resultado de su desarrollo. El apartado de anexos, incluye la lista de los expertos en gestión de TIC que evaluaron el sistema y el cuestionario que se diseñó para tal fin.

Capítulo 1. Tecnologías de la Información y Comunicación y la prevención de crisis

1.1 Tecnologías de la Información y Comunicación

El concepto de las Tecnologías de la Información y Comunicación (TIC) cada vez es usado de una manera más familiar en diversos ámbitos debido a que tecnologías como las computadoras y el Internet están involucradas, al menos de forma indirecta en la gran mayoría de las actividades cotidianas. Por lo general se tiene un conocimiento aproximado de a qué se refiere este término ya que como por sí mismo lo indica, se enfoca en herramientas para manejar información y permitir la comunicación. Debido al uso de las TIC en varios contextos es común que no exista una definición única ni tampoco una definición correcta única.

En Zuppo (2012) se indica que las definiciones de TIC giran en torno a la idea de "dispositivos e infraestructura que facilitan la transmisión de la información por medios digitales". Dicha autora señala que existe dificultad para encontrar un consenso en las definiciones de TIC, sin embargo identifica cuatro principales contextos en donde se definen: TIC y el Desarrollo Socioeconómico, TIC como un sector económico, TIC y la educación, TIC y negocios. Así, para el ámbito educacional señala que se relacionan mucho con el desarrollo continuo de destrezas y habilidades, mientras que para el ámbito de los negocios refiere a la definición en Information Technology Infrastructure Library (2011):

> *Es el uso de la tecnología para el almacenamiento, la comunicación o el procesamiento de la información. Típicamente, la tecnología incluye computadores(as), telecomunicaciones, aplicaciones y otro software. La información puede incluir datos del negocio, voz, imágenes, video, etc. A menudo, la tecnología de la información se utiliza para apoyar los procesos de negocio a través de servicios de TI.*

En Zuppo (2012) se concluye que para el estudio de las TIC se debe tener una definición acorde al contexto que considere las aplicaciones relevantes del concepto.

En Bravo et al. (2008) se presenta la siguiente definición del sector de las TIC acorde a lo planteado por la Organización para la Cooperación y el Desarrollo Económico (OCDE) y la Unión Europea: *"Las TIC se definen como sistemas tecnológicos mediante los que se recibe, manipula y procesa información, y que facilitan la comunicación entre dos o más interlocutores".*

En dicho trabajo se concluye que es necesario buscar alternativas más eficientes para el impulso de las TIC en el país y para su registro, debido a una marcada diferencia regional en su uso y su desarrollo así como una fuerte inconsistencia entre los datos registrados por organismos nacionales como la Asociación Nacional de Universidades e Instituciones de Educación Superior en México (ANUIES), la Secretaría de Educación Pública (SEP), la ahora disuelta Comisión Federal de Telecomunicaciones (COFETEL), la Secretaría de Comunicaciones y Transportes (SCT), el Consejo Nacional De Ciencia Y Tecnología (CONACYT), y la Asociación Mexicana de la Industria de Tecnologías de la Información A.C. (AMITI); y por organismos internacionales como la OCDE; la Comisión Económica para América Latina y el Caribe (CEPAL), la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), y la International Telecommunication Union (ITU).

La ITU es la agencia especializada de las Naciones Unidas para las TIC y se encarga de asignar el espectro radioeléctrico y órbitas satelitales, de elaborar normas técnicas de interconexión de tecnologías y redes, y de mejorar el acceso a las TIC de comunidades en todo el mundo. Se integra por 193 países miembro, organismos reguladores de TIC, instituciones académicas reconocidas y alrededor de 700 empresas privadas (International Telecommunication Union, 2013a). Debido a estas actividades, a la infraestructura y al compendio de información que reúne la ITU, es de destacar que no proporciona una definición propia y específica de las TIC en todo su sitio Web, sin embargo sí reúne una gran cantidad de valiosos documentos sobre su importancia, su desarrollo, y un registro a nivel mundial de la adopción de TIC a lo largo de los años, por mencionar algunos tipos de información. Esto refuerza la idea de que la definición de las Tecnologías de la Información y Comunicación depende del contexto en que se ocupe, y que aun así ésta no se aleja de la idea esencial.

En International Telecommunication Union (2015) se presenta un estudio de la CEPAL, a través del Observatorio para la Sociedad de la Información en América Latina y el Caribe (OSILAC), donde se reconocen distintas definiciones de TIC para los distintos países (Observatorio para la Sociedad de la Información en Latinoamérica y el Caribe, 2004). Para el caso de México refiere la proporcionada por la Conferencia de Autoridades Iberoamericanas de Informática en 2001:

> Las Tecnologías de la Información y la Comunicación se pueden concebir como resultado de una convergencia tecnológica, que se ha producido a lo largo de ya casi medio siglo, entre las telecomunicaciones, las ciencias de la computación, la microelectrónica y ciertas ideas de administración y manejo de información. Se consideran como sus componentes el hardware, el software, los servicios y las telecomunicaciones.

Otro punto de vista es el que ve a las TIC como una herramienta indispensable para habilitar las estrategias de negocio y facilitar la evaluación del desempeño de las empresas. Tal es el caso de la definición que se considera en Instituto Mexicano de Ejecutivos de Finanzas (2007). Allí se considera que las TIC incluyen a las tecnologías que permiten recopilar, almacenar y transmitir información, además de las técnicas administrativas y de operaciones para llevar a cabo su procesamiento y que también posibilitan el desarrollo de sistemas de apoyo en la toma de decisiones.

Una definición más concreta de las TIC es la que proporciona el Banco Mundial a través de su sitio Web (The World Bank, 2015):

> Consisten del hardware, software, redes y medios para la colección, almacenaje, procesamiento, transmisión y presentación de la información (voz, datos, texto, imágenes) también como los servicios relacionados. Las TIC pueden ser separadas en *Infraestructura de la Información y Comunicación* y *Tecnología de la Información*.

Ante esta diversidad de definiciones se observa que en la actualidad lo importante al referirse a las TIC, más que las palabras que se utilicen es la idea esencial a lo que refieren y los beneficios que pueden generar en el ámbito donde se ocupen. A manera de resumen se desarrolla un enunciado que considera las ideas expresadas hasta el momento sobre el significado de las TIC.

> *El concepto de Tecnologías de la Información y Comunicación engloba soluciones de hardware, software, conocimientos, procedimientos o métodos que permiten la creación, almacenaje, manipulación, procesamiento, recuperación y comunicación de información digital, con lo cual*

se busca una eficiente organización, análisis y uso para potencializar la mejora de las condiciones de quienes las ocupan en contextos económicos, sociales, salubres, de innovación y culturales, por mencionar algunos.

1.2 Impacto global y nacional de las TIC

1.2.1 Panorama global

La incorporación de TIC en las organizaciones privadas o públicas se debe a los beneficios que traen consigo. Desde la mecanización de operaciones y con ello el ahorro de inversiones de tiempo, de personal y de dinero; la rapidez, precisión y exactitud en la realización de tareas especializadas en campos científicos, administrativos y de salud; la ayuda para desarrollar o mejorar las habilidades en las personas; la facilidad y eficacia para permitir la comunicación; la contribución para el cuidado del medio ambiente; y la organización y control de servicios de emergencia, por ejemplo.

Las empresas del sector privado son los primeros usuarios de las TIC e impulsan la economía de la información en todo el mundo proporcionando servicios y contenidos en línea y participando en el comercio electrónico; además transforman sectores empresariales enteros y crean nuevas cadenas de valor con el uso de las TIC. La difusión de las TIC en la economía ha facilitado el desempeño macroeconómico y el crecimiento empresarial mediante el aumento de la productividad del trabajo, ha ampliado el alcance del mercado de las empresas e impulsado la innovación (International Telecommunication Union, 2014).

Organismos internacionales refieren la gran importancia hoy en día de las TIC por sus efectos y potencialidades en la aplicación en un sinnúmero de áreas de la sociedad. Para el Programa de las Naciones Unidas para el Desarrollo (UNDP), uno de los propósitos de las TIC es favorecer una amplia distribución de recursos y oportunidades, de acuerdo con los derechos humanos, democracia, creación de la sustentabilidad en salud y del medio ambiente. De forma similar la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) reconoce la importancia económica de las TIC desde el punto de vista de desarrollo humano e indican que “proporcionan instrumentos importantes para mejorar la salud y la educación, ofrecen nuevos canales para la difusión del conocimiento y crean espacios físicos y virtuales para la comunicación social” (Tawfik, 2000).

Una de las TIC de mayor uso en el mundo es la Internet, la cual involucra muchos otros elementos de tecnología; desde los dispositivos para acceder al contenido disponible en línea, la infraestructura que permite la comunicación de la información y aquella que permite su modificación y almacenamiento. De acuerdo con International Telecommunication Union (2014) a finales del 2014 aproximadamente 3000 millones de personas estaban utilizando Internet como medio de comunicación y como fuente de información, lo que equivale al 40.4% de individuos en el mundo (un porcentaje de individuos de 78.3% países desarrollados, 32.4% en países en vías de desarrollo y 8% en los países menos conectados). Este

uso de la Internet ha sido principalmente impulsado por los medios móviles de comunicación ya que existen alrededor de 6900 millones de suscripciones a telefonía celular a nivel mundial (International Telecommunication Union, 2014). En la figura 1.1 se muestran gráficas de suscripciones a telefonía móvil por cada 100 habitantes a nivel mundial (World), en países en desarrollo (Developing), en países desarrollados (Developed), de países menos desarrollados (Least Developed Countries, LDCs) y por regiones a nivel mundial, entre los años 2005 y 2013; para el año 2014 se muestra un estimado. En dichas gráficas también se incluyen datos de la Comunidad de estados independientes (Commonwealth of Independent States, CIS).

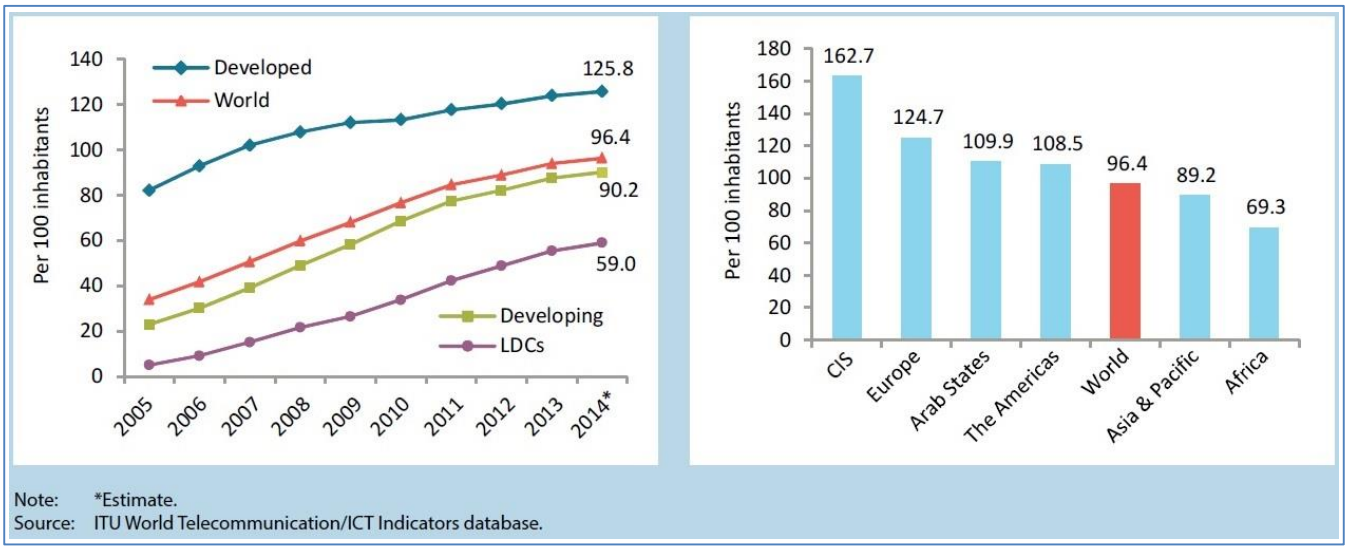


Figura 1.1. Suscripciones a telefonía móvil por cada 100 habitantes según el nivel de desarrollo de los países y por regiones. World = A nivel mundial, Developing = Países en desarrollo, Developed= Países desarrollados, LDCs (Least Developed Countries) = Países menos desarrollados, CIS (Commonwealth of Independent States) = Comunidad de Estados independientes. Tomado de International Telecommunication Union (2014).

También en International Telecommunication Union (2014) se proporcionan datos muy interesantes respecto a la situación de las TIC a nivel mundial como por ejemplo el crecimiento que ha experimentado el ancho de banda internacional que ha pasado de 1,600 Gbit/s en 2001 a más de 140,000 Gbit/s en 2013 con un crecimiento anual promedio de 45% que implica una fuerte inversión en la infraestructura de red troncal en todas las partes del mundo. De igual forma proporciona datos de cómo ha crecido el porcentaje de hogares con acceso a Internet del 2005 al 2013 y se hace una estimación respecto al 2014 (figura 1.2), haciendo evidente un incremento notable de su uso en la sociedad de este tipo de TIC.

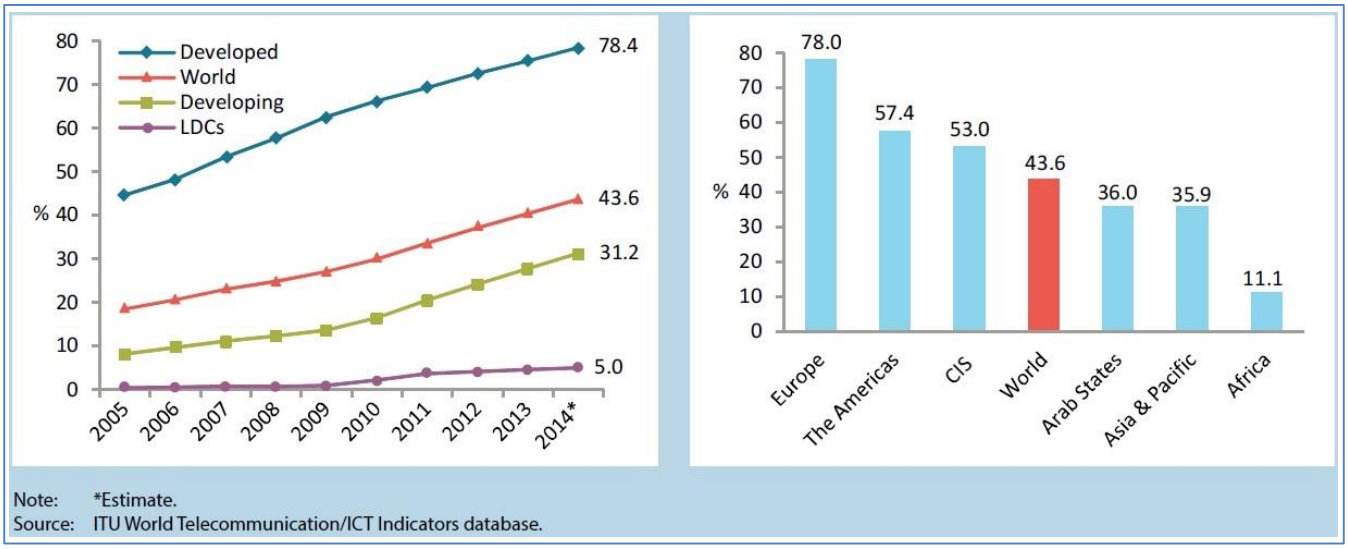


Figura 1.2. Porcentaje de hogares con acceso a Internet según el nivel de desarrollo de los países y por regiones. World = A nivel mundial, Developing = Países en desarrollo, Developed= Países desarrollados, LDCs (Least Developed Countries) = Países menos desarrollados, CIS (Commonwealth of Independent States) = Comunidad de Estados independientes. Tomado de International Telecommunication Union (2014). Tomado de International Telecommunication Union (2014).

El uso de las TIC no es homogéneo, siendo los países en vías de desarrollo los más atrasados en su adopción, sin embargo esto no implica que su uso sea pequeño en lo más mínimo. Aunque del 2011 al 2012 se observa un decremento en los ingresos generados por las TIC en los países desarrollos también se habla de la creciente importancia del sector de las telecomunicaciones en el crecimiento económico de los países en desarrollo ya que el total de ingresos las telecomunicaciones aumentó del 26% en 2007 al 32% en 2012, lo que implica un amplio crecimiento en infraestructura y en la adopción de las TIC, de forma individual y por las organizaciones. Esta idea se ve reforzada por el incremento en la inversión en telecomunicaciones en un 4% en todo el mundo hasta alcanzar 307,000 millones USD (figura 1.3).

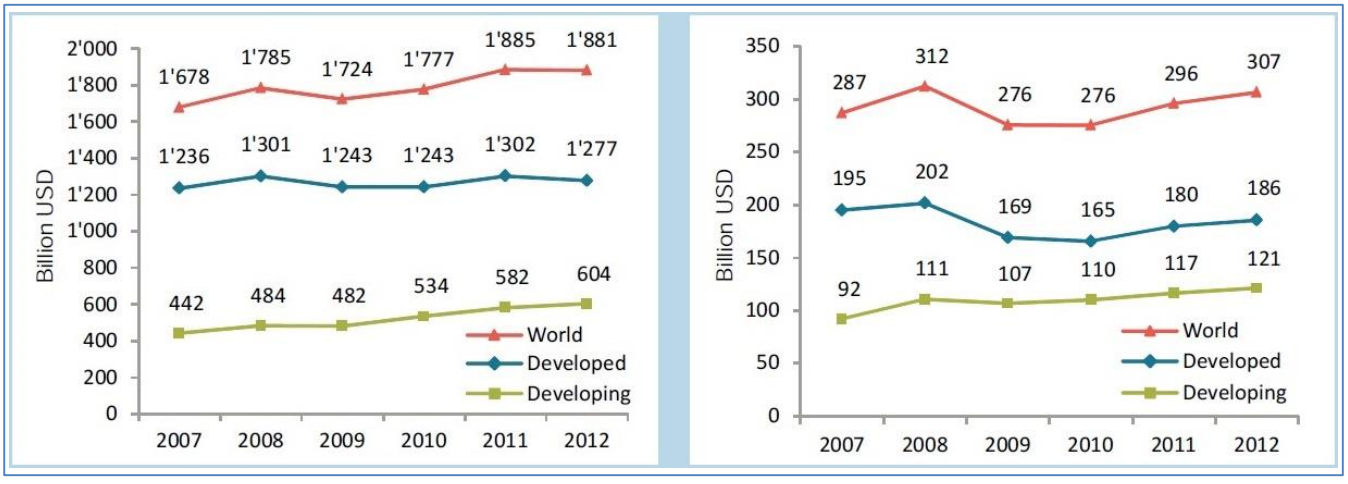


Figura 1.3. Ingresos generados por las TIC (izquierda) e inversión de los operadores de telecomunicaciones (derecha) en países según su nivel de desarrollo. 1 Billion USD = 1,000,000,000 USD. World = A nivel mundial, Developed = Países desarrollados, Developing = Países en desarrollo. Tomado de International Telecommunication Union (2014).

En los países en vías de desarrollo los datos sobre las TIC en las empresas son escasos; la proporción de empresas con acceso a Internet varía mucho entre países, además de que no todos tienen acceso de banda ancha, lo cual es un factor muy importante para aprovechar el máximo potencial del comercio electrónico. Las micro y pequeñas empresas tienen mucho menos acceso a Internet que las grandes empresas y lo mismo sucede con las empresas rurales en comparación con las empresas urbanas. El acceso a banda ancha de calidad a alta velocidad es importante para el sector empresarial al igual que otras TIC que son la base de infraestructuras y servicios necesarios para ejecutar un negocio exitosamente (International Telecommunication Union, 2014).

A nivel mundial, el e-government (gobierno electrónico) contribuye a incrementar la eficiencia y transparencia de los gobiernos en los países además de reducir sus costos y mejorar sus servicios. De acuerdo con un estudio que la ONU realiza cada 2 años, los gobiernos de todos los países han creado páginas web centrales y más del 50% de ellos proporciona enlaces a los sitios web de los organismos gubernamentales locales y/o regionales; además se tiene registro de que en la última década los servicios y la información de sitios web gubernamentales se ha triplicado (International Telecommunication Union, 2014). En la figura 1.4 se presenta cómo ha ido creciendo el Índice de Desarrollo de Gobierno Electrónico registrado por la ITU en los 5 continentes.

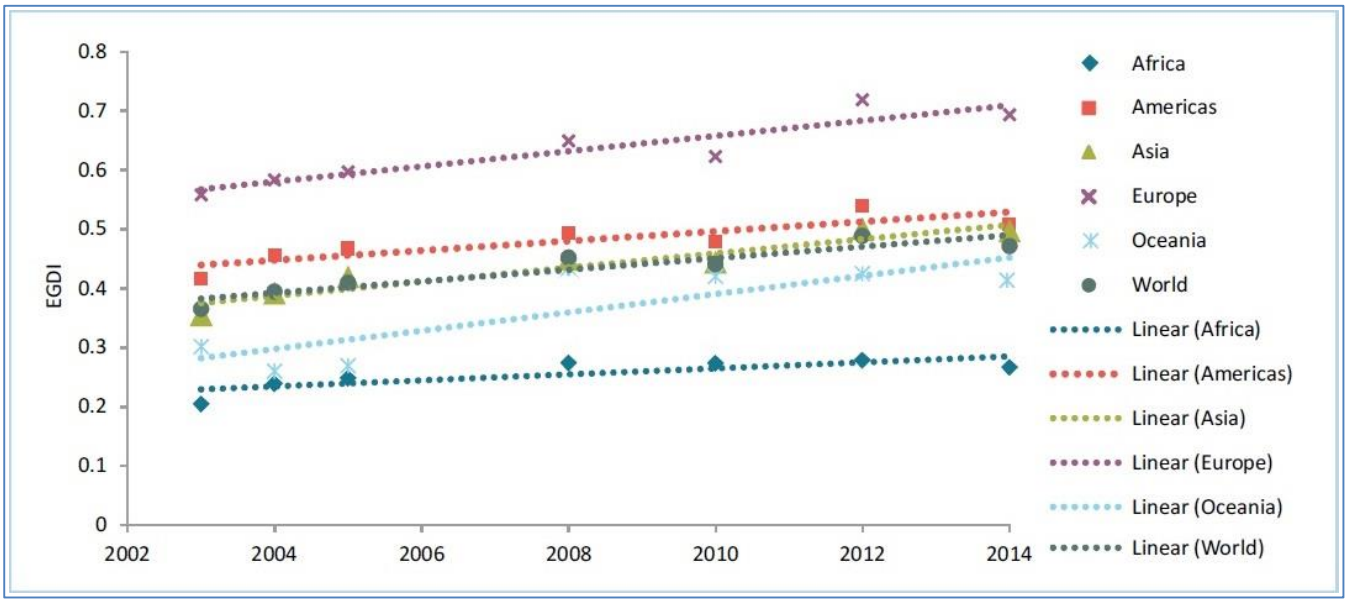


Figura 1.4. Índice de Desarrollo de Gobierno Electrónico (EGDI). Tomado de International Telecommunication Union (2014).

A nivel internacional se reconocen principalmente 2 indicadores con los cuales se puede comparar el uso y desarrollo de las TIC entre los países. El primero de ellos, el ICT Development Index (IDI) de la ITU no pretende indicar qué país tiene el mayor avance en TIC, sino más bien medir cómo ha sido su cambio en el nivel y la evolución cronológica del desarrollo de las TIC con respecto a sí mismo y con respecto a otros países de forma anual. Otros de sus objetivos son medir la brecha digital, es decir, las diferencias entre los países según sus niveles de desarrollo de las TIC; y medir las posibilidades de desarrollo de las

TIC. Se compone de 3 subíndices que a su vez se integran con valores de diferentes parámetros. El Subíndice de Acceso, que tiene un peso del 40% en el IDI, registra la cantidad de suscripciones a la telefonía fija por cada 100 habitantes, la cantidad de suscripciones a la telefonía móvil celular por cada 100 habitantes, el ancho de banda internacional de Internet por cada usuario de Internet en bits/s, el porcentaje de hogares con computadora y el porcentaje de hogares con acceso a Internet. El Subíndice de Uso tiene un peso del 40% en el IDI y se conforma por valores del porcentaje de personas que utilizan Internet, la cantidad de suscritos a la banda ancha (alámbrica) fija por cada 100 habitantes, y la cantidad de registrados a la banda ancha inalámbrica por cada 100 habitantes. Por su parte, el Subíndice de Habilidades conforma el 20% del IDI y se conforma por la tasa de alfabetización de los adultos, el porcentaje bruto de inscripción en enseñanza secundaria y el porcentaje bruto de inscripción en enseñanza terciaria. En el año 2012 la posición de México fue la 93 con un valor IDI de 4.29 y en el año 2012 fue la 94 con un valor IDI de 4.07 (International Telecommunication Union, 2014). En la tabla 1.1 se muestran las primeras posiciones de este conteo, la posición de algunos países de América y las últimas posiciones. En la figura 1.5 se muestra un resumen de los valores promedio, valores máximos y mínimos, el rango, la desviación estándar y el coeficiente de variación del IDI y de sus subíndices.

Economía	Posición en 2013	IDI 2013	Posición en 2012	IDI 2012		Economía	Posición en 2013	IDI 2013	Posición en 2012	IDI 2012
Dinamarca	1	8.86	2	8.78		Argentina	59	5.8	56	5.58
República de Korea	2	8.85	1	8.81		Brasil	65	5.5	67	5.16
Suiza	3	8.67	3	8.68		Trinidad y Tobago	67	5.29	63	5.36
Islandia	4	8.64	4	8.58		Colombia	77	4.95	80	4.61
Reino Unido	5	8.5	7	8.28		Venezuela	80	4.81	78	4.68
Japón	11	8.22	6	8.35		Panamá	82	4.75	77	4.69
Estados Unidos	14	8.02	14	7.9		Ecuador	88	4.56	88	4.2
Canadá	23	7.62	25	7.37		**México**	**95**	**4.29**	**94**	**4.07**
España	28	7.38	29	7.14		El Salvador	110	3.61	110	3.47
Uruguay	48	6.32	51	5.92		India	129	2.53	129	2.42
Costa Rica	55	5.92	55	5.64		Mozambique	159	1.52	159	1.4
Chile	56	5.92	54	5.68		República Centroafricana	166	0.96	166	0.93

Tabla 1.1. Algunas posiciones de los países según el valor del IDI obtenido en 2012 y 2013. Elaborado con datos de (International Telecommunication Union, 2014).

	IDI 2013						IDI 2012						Cambio en el valor promedio 2012 - 2013
	Valor promedio	Mínimo	Máximo	Rango	Desv. estándar	Coef. de variación	Valor promedio	Mínimo	Máximo	Rango	Desv. estándar	Coef. de variación	
IDI	4.77	0.96	8.86	7.90	2.22	46.44	4.60	0.93	8.81	7.87	2.19	47.61	0.20
Subíndice de acceso	5.41	1.27	9.46	8.18	2.24	41.39	5.27	1.22	9.40	8.18	2.26	42.93	0.18
Subíndice de uso	3.19	0.03	8.71	8.68	2.44	76.45	2.90	0.03	8.47	8.44	2.36	81.33	0.32
Subíndice de habilidad	6.66	1.10	9.90	8.80	2.15	32.28	6.66	1.10	9.90	8.80	2.15	32.30	0.01

Figura 1.5. Valores del IDI y sus subíndices en el año 2013 y 2012. Desv. estandar = Desviación estándar. Coef. de variación = Coeficiente de Variación. Adaptado de International Telecommunication Union (2014).

En lo que respecta a los subíndices que conforman en IDI, en el acceso a TIC México ocupaba en el año 2013 el puesto 93 con un valor de 4.80 y en 2012 ocupaba el lugar 97 con valor de 4.54; para el subíndice que mide el uso de TIC en el año 2013 México estaba en el lugar 95 con 2.45 y en el año 2012 en la posición 90 con valor de 2.17; y para el índice de habilidades estaba en la posición 88 con valor alcanzado de 6.96 para los años 2012 y 2013.

El otro indicador internacional destacable es el Networked Readiness Index (NRI) del foro económico mundial. El NRI mide el rendimiento de 143 economías en el aprovechamiento de las TIC para impulsar la competitividad y el bienestar. Su escala va del 1 (peor rendimiento) al 7 (mejor rendimiento). Se compone por 53 indicadores individuales distribuidos en 10 categorías o pilares que conforman 4 subíndices generales. El *Subíndice del Ambiente* contiene los pilares de ambiente de políticas y regulaciones de TIC y el ambiente de innovación y negocios; el *Subíndice de Preparación* considera la infraestructura, la asequibilidad y las habilidades; el *Subíndice de Uso* contempla los pilares de uso de TIC por individuos, uso de TIC por las empresas y el uso de TIC por el gobierno; y el *Subíndice de Impacto* se conforma por los pilares de impacto económico e impacto social. En World Economic Forum & INSEAD (2015) se indica que México alcanza un valor de 4.0 en este índice y con ello ocupa el lugar número 69 al año 2015. En la figura 1.6 se muestran las calificaciones que alcanza México en cada subíndice y pilar; además de una gráfica de radar donde se muestra su comportamiento con respecto al promedio de las economías donde el Banco Mundial lo clasifica por su nivel de ingresos (grupo de economías de ingresos medios-altos). En la figura 1.7 se presenta la ubicación de las economías a nivel mundial de acuerdo con el valor de NRI.

	Posición (total de 143)	Valor (1-7)
Networked Readiness Index 2015	**69**	**4.0**
Networked Readiness Index 2014 (total de 148)	79	3.9
Networked Readiness Index 2013 (total de 144)	63	3.9
A. Subíndice del Ambiente	**81**	**3.9**
Pilar 1. Ambiente de políticas y regulaciones de TIC	70	3.7
Pilar 2. Ambiente de innovación y negocios	87	4.1
B. Subíndice de Preparación	**58**	**5.0**
Pilar 3. Infraestructura	81	3.7
Pilar 4. Asequibilidad	4	6.7
Pilar 5. Habilidades	92	4.5
C. Subíndice de Uso	**79**	**3.7**
Pilar 6. Uso de TIC por individuos	87	3.3
Pilar 7. Uso de TIC por empresas	72	3.6
Pilar 8. Uso de TIC por el gobierno	56	4.2
D.Subíndice de impacto	**72**	**3.6**
Pilar 9. Impactos económicos	72	3.2
Pilar 10. Impactos sociales	76	4.0

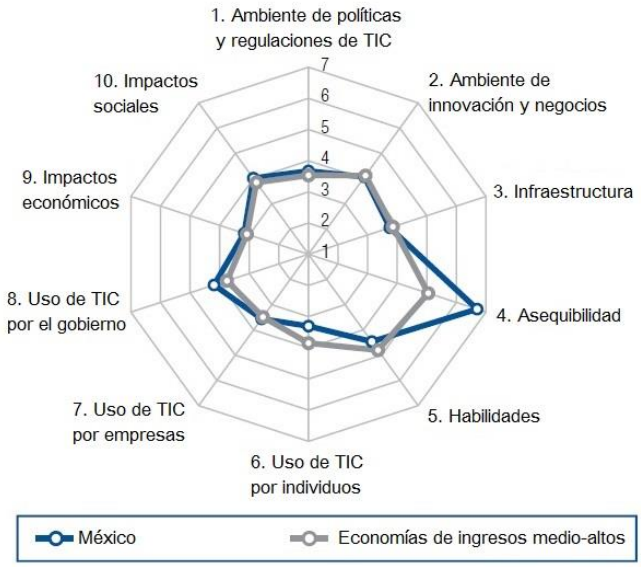


Figura 1.6. Valores para México del NRI, sus subíndices y subcategorías y gráfica de radar donde se ubica el desempeño de México con respecto al promedio de las economías con ingresos medios-altos de acuerdo con la clasificación del banco mundial. Adaptado de World Economic Forum & INSEAD (2015).

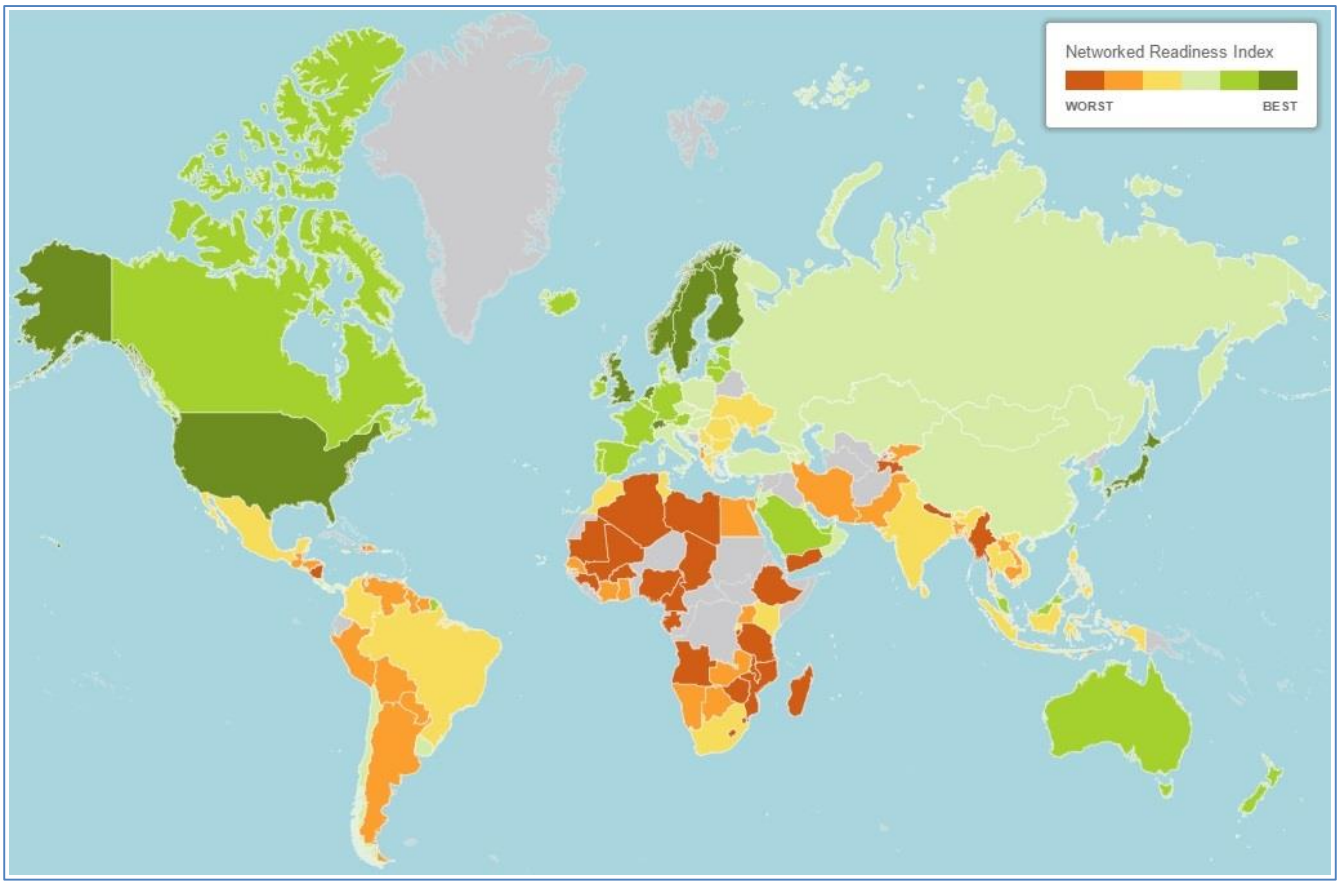


Figura 1.7. Ubicación de las economías a nivel mundial de acuerdo con el valor de NRI. Los colores verdes indican un mejor desempeño. México se encuentra en la posición 69 de un total de 143. (World Economic Forum, 2015).

En World Economic Forum & INSEAD (2015) se indica que existen muchos aspectos en qué mejorar para México, empezando en la innovación y el uso de las TIC en los negocios, en el nivel de los impuestos a pagar y las deficiencias del proceso legislativo y poder judicial con respecto a TIC. Se destaca que la implantación de las TIC entre las empresas y la población en general sigue siendo muy baja nivel global e incluso en la región de Latinoamérica.

1.2.2 TIC en México

Desde finales del 2013, los gobiernos de 146 países miembros de la ITU han adoptado políticas nacionales para potenciar el mercado de TIC y la conexión a banda ancha, entre ellos México con la actual *Estrategia Digital Nacional* que se refiere a una mejora de la experiencia del ciudadano como usuario de servicios públicos mediante la adopción de tecnologías por parte de gobierno, al incremento de servicios digitales en la economía para estimular la productividad y desarrollo de empresas, a actividades en busca de mejorar la enseñanza y la salud, así como a una mayor utilización de TIC para promover la seguridad de la sociedad y prevenir y mitigar riesgos por fenómenos naturales (Presidencia de la República de México, 2013). Estos esfuerzos se encaminan a la creación de una infraestructura nacional de conexión mediante banda ancha y a la estimulación de la demanda mediante la adopción de servicios y aplicaciones en línea tales como cibercomercio y otros (International Telecommunication Union, 2013b).

Según datos citados en Asociación Mexicana de la Industria de Tecnologías de Información A.C., Instituto Mexicano para la Competitividad A.C., & Select Estrategia A.C. (2013), 54% de la población y 76% de las empresas usan algún servicio de e-gobierno superando el 42% y 82% respectivo que alcanza el promedio de los países de la OCDE.

El Instituto Nacional de Estadística y Geografía (INEGI) presenta un conteo de los principales usos del Internet por usuarios en México desde 2010 a 2014. A este respecto, las personas que lo ocupan para interactuar con el gobierno fueron 384,953 en el mes de mayo de 2010, 479,111, 457,826, 581,928 en los meses de abril de 2011, 2012 y 2013 respectivamente, y como cifra preliminar para el mes de abril de 2014 se estimó una cantidad de 594,580. Es decir, de 2010 a 2014 se incrementó en poco más de 20,000 la cantidad de usuarios que el e-gobierno debe de ser capaz de atender mensualmente (Instituto Nacional de Estadística y Geografía, 2015).

Por otro lado, el interés de las empresas por el uso de las TIC se debe a las ventajas competitivas que les permiten mediante el *posicionamiento estratégico* (proveer un valor único a los clientes u operar de manera distinta a la de los competidores) y *eficiencia operativa* (hacer mejor lo que hacen los competidores); sin embargo es importante hacer notar que las TIC por sí solas no proporcionan dichos beneficios ya que éstos dependen de la forma en que se hace uso de ellas, lo cual depende a su vez de que las organizaciones tengan sus objetivos claros y definir las actividades adecuadas que les permitan actuar en esa dirección (Instituto Mexicano de Ejecutivos de Finanzas, 2007).

En Asociación Mexicana de la Industria de Tecnologías de Información A.C. et al. (2013) se presenta información de la OCDE y otra aportada por Select Estrategia A.C. generada en parte por una encuesta que se realizó a 938 empresas mexicanas en 2012, y en parte construida con datos del Foro Económico Mundial (WEF). De dicho informe se extrae la gráfica de la figura 1.8, en donde se ve una clara asociación entre competitividad y aprovechamiento de las TIC con un coeficiente de correlación de 0.94.

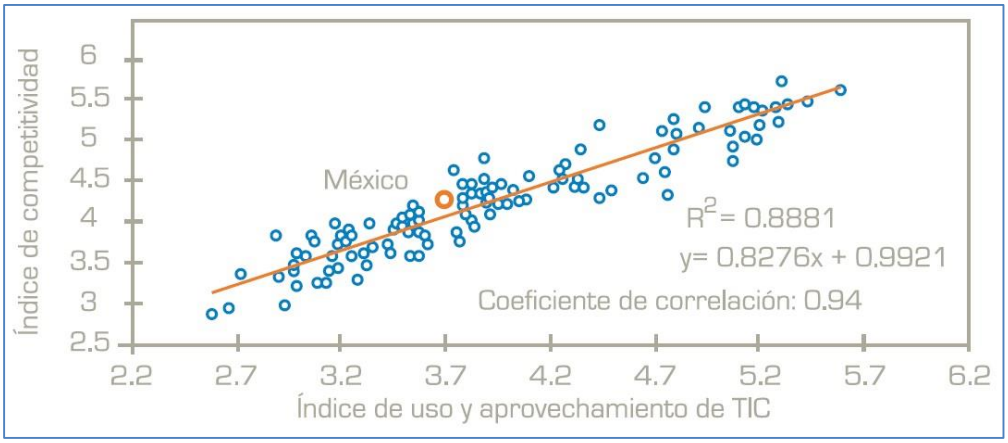


Figura 1.8. Correlación entre competitividad en las empresas y el uso de TIC. Tomado de Asociación Mexicana de la Industria de Tecnologías de Información A.C. et al. (2013).

En lo que respecta a industria en México enfocada específicamente en desarrollo de TIC su presupuesto creció 67% al año 2011 con respecto al año 2003, llegando a 42,623 millones de dólares. En el año 2003 el porcentaje de personal relacionado con las TIC representaba 5.9% del empleo total, pero para el año 2011 este valor aumentó a 7.5%, sumando aproximadamente 1.6 millones de empleados en total. Un estimado del crecimiento es del 8.4% anual hasta el 2025, siendo los sectores de servicios en la nube, servicios de TIC y de desarrollo de software los que impulsarán este crecimiento. El mercado total de la industria TIC se conforma por uno que se refiere al sector organizacional y otro al sector residencial. En la figura 1.9 se presenta el crecimiento estimado de la industria TIC dedicada al sector organizacional, de ésta se observa un crecimiento de los servicios de TIC y de desarrollo de software, lo que implica un incremento en proyectos específicos para su desarrollo y para su administración una vez implantadas.

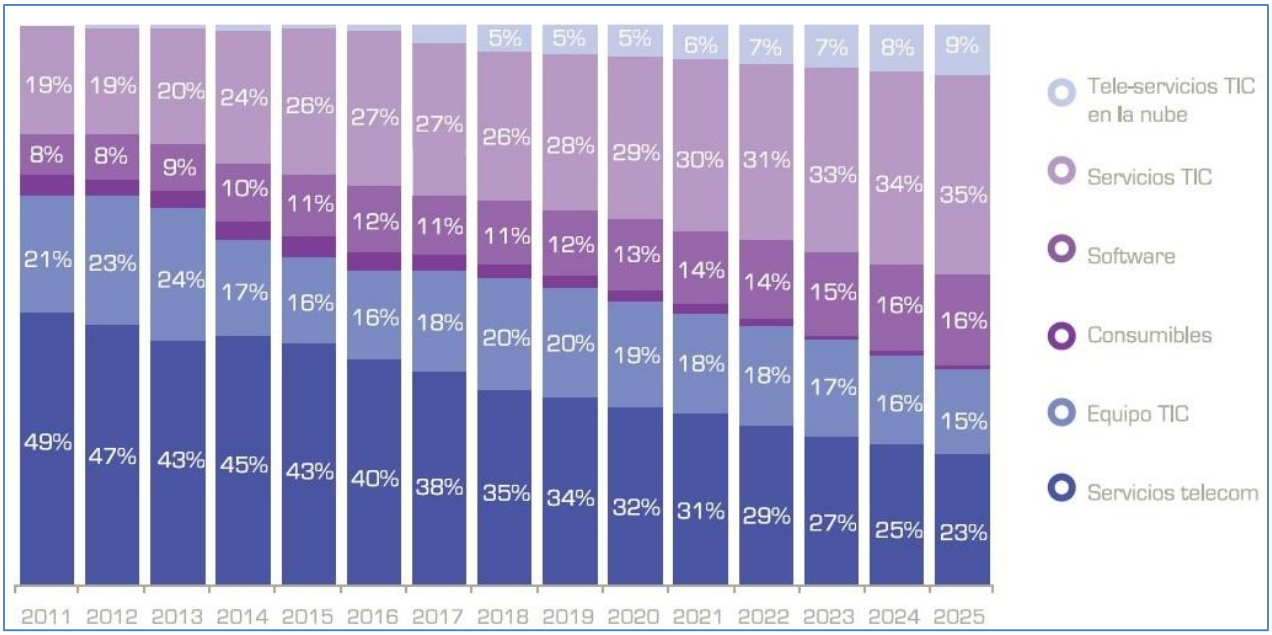


Figura 1.9. Estimación crecimiento de la industria TIC dedicada al sector organizacional en México del año 2011 al año 2025. Tomado de Asociación Mexicana de la Industria de Tecnologías de Información A.C. et al. (2013).

Otros datos importantes se presentan en la figura 1.10 se muestra una comparativa del año 2003 al año 2011 de la cantidad de empleados que hacen uso de las TIC en México, de forma total y por tamaño de empresa. De acuerdo con un estudio de Select Estrategia A.C. a 938 empresas, la principal utilización de las TIC es en actividades de administración y finanzas, en segundo rubro se encuentran funciones de abasto y logística, desatendiéndose áreas más sustantivas para generar valor, como investigación, desarrollo y análisis de información. Entre los países miembros de la OCDE el promedio al año 2008 del porcentaje del valor agregado de las TIC en el sector empresarial es del 8.25%, y en México se alcanza el 4.99% por la capacidad limitada del uso de las tecnologías (Asociación Mexicana de la Industria de Tecnologías de Información A.C. et al., 2013).

Los datos del pronóstico que realiza por Select Estrategia A.C., también presentado en Asociación Mexicana de la Industria de Tecnologías de Información A.C. et al. (2013) , apuntan a que en el año 2025 cada trabajador contará con un promedio de cuatro computadoras personales en las grandes empresas y con alrededor de una en las micro y pequeñas. Select Estrategia A.C prevé que para ese mismo año la tendencia que más beneficiará a las empresas será el incremento en la eficiencia de la transmisión y análisis de datos como herramienta para analizar el comportamiento de los clientes o consumidores de servicios.

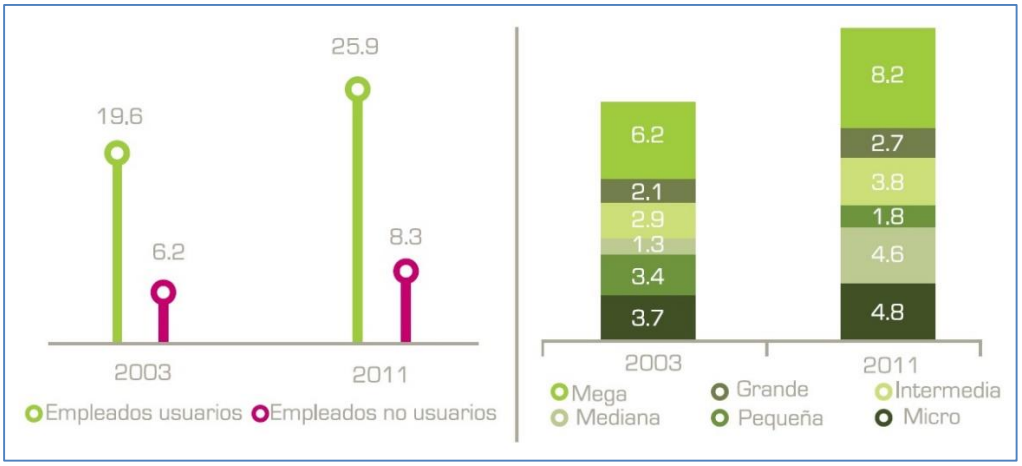


Figura 1.10. Uso de tecnología en empleados (izquierda) y empleados usuarios de tecnologías por tamaño de empresas (derecha). Cifras indicada en millones. Tomado de Asociación Mexicana de la Industria de Tecnologías de Información A.C. et al. (2013).

En Asociación Mexicana de la Industria de Tecnologías de Información A.C. et al. (2013) también se indica que de acuerdo con datos del INEGI el porcentaje del PIB atribuible al sector TIC en México pasó de 3.2% en el 2000 al 5.6% en el 2010, contribuyendo en mayor medida que el total de las actividades primarias que contribuyen con el 3.8%. En este aspecto México se encuentra rezagados con respecto a otros países como U.S.A., Japón, o Costa Rica, donde las TIC representan el 7.4%, 6.8% y 6.5 respectivamente.

El INEGI, como parte de sus censos económicos, incorpora desde el año 2004 un apartado sobre investigación e innovación tecnológica para el sector privado que por sus características está en posibilidad de emprender proyectos de este tipo, innovar en procesos o productos o incorporar tecnología como parte integral de sus procesos. De la gran cantidad de información que el INEGI pública a través de sitio web, la que se agrupa en la categoría de Sociedad de la Información brinda datos muy importantes sobre el uso de las TIC en las organizaciones. Los datos que se presentan en la tabla 1.2 refieren a distintos sectores productivos e indica de cada uno de ellos la cantidad de empresas en ese rubro que fueron estudiadas (población objetivo), la cantidad total de personas que trabajan en esa población objetivo de empresas, y lo más importante para este trabajo, datos sobre el uso de TIC en ese sector productivo. De esta información que engloba la tabla 1.2 es importante destacar la que se refiere a la cantidad de empresas que cuentan con una intranet, una red de área local (Local Area Network, LAN) y extranet, pues esto implica que como parte de sus actividades productivas utilizan TIC que necesitan ser gestionadas técnica y administrativamente, aspecto que es clave para el tema que se trata con esta tesis. De un total de 151,024 empresas consideradas en este censo, 45,459 (30.1%) empresas cuentan con una intranet, 99,731 (66.04%) cuentan con una red LAN, y 10,710 (7.09%) cuentan con extranet; cifras que indican una cantidad importante de negocios en los que es necesario atender temas de crisis en TIC que puedan afectar su desempeño. Con los datos de dicha tabla es importante destacar una relación directa entre las magnitudes 4 rubros: Empresas con red LAN,

Empresas con intranet y Empresas con Internet de banda ancha fija; en estos casos existe coincidencia entre los valores grandes, valores medianos y valores pequeños en esos campos. Los valores de la columna de Empresas con extranet tienen un comportamiento similar.

En la tabla 1.3 también se presenta información del uso de las TIC en las empresas, pero haciendo una clasificación con respecto al número de empleados que las conforman; las categorías son de empresas con 10 a 49 empleados, con 50 a 249 empleados y empresas de más de 250 empleados. Para cada grupo se indican datos en 2 formatos, el primero en valor absoluto y el segundo en el porcentaje de la población total que representa dicho valor absoluto. Así, por ejemplo se señala que de 132398 empresas que tienen entre 10 y 49 empleados, son 114916 las que usan Internet, lo que representa un 86.8% del total; y que de un total de 6714850 personas que laboran en las empresas con más de 250 empleados, el 29% (1944789 empleados) usan computadoras. Estos ejemplos se resaltan con negritas en la tabla.

De los datos de la tabla 1.3 se puede concluir en consideración a la complejidad de las empresas según la cantidad de personal que tienen y a la necesidad de la utilización de las TIC para su operación. En este sentido se observa que a mayor complejidad de la empresa, indicada por la cantidad de empleados, más son las que utilizan TIC como parte de sus labores. La mayoría de las organizaciones privadas que tienen cantidad de empleados grande se ven obligadas a tener un mayor nivel de organización en sus procesos y en consecuencia tienen una mayor dependencia del uso eficiente de las TIC para desempeñar sus funciones de manera satisfactoria. Esto lo podemos ver en la cantidad de empresas que cuentan con red LAN ya que el 61.5% de las empresas que tienen entre 10 y 49 empleados tienen una red LAN, y este porcentaje se incrementa a 88.1% y a 95.2% en las que tienen de 50 a 249 empleados y en las que tienen más de 250 empleados, respectivamente. Un comportamiento parecido sucede con casi todos los demás rubros, a excepción de los que se refieren a las empresas que reciben y hacen pedidos por Internet, en donde se tiene ligeramente un porcentaje mayor en las empresas que tienen entre 50 y 249 empleados. Se destacan con colores distintos en dichas tablas los datos para empresas que cuentan intranet, extranet, banda ancha fija y red LAN.

Los datos presentados hasta el momento sirven como referencia para conocer el nivel de importancia de las TIC en México en sectores productivos. Por dicho valor de las TIC es necesario procurar su adecuado funcionamiento a fin de que coadyuven a alcanzar los objetivos de cada entidad donde se usan. Sin embargo, es común que se presenten desperfectos técnicos o en su operación, lo cual puede afectar en distintos grados su eficiencia e incluso ocasionar alteraciones de carácter importante para las organizaciones donde se usan y generar una crisis. En el apartado siguiente, se introducen conceptos sobre estas situaciones de emergencia. Primero desde el enfoque de los fenómenos naturales, que es un área donde se han desarrollado trabajos con algunos aspectos comunes al de esta tesis: el desarrollo de planes de prevención de crisis. Posteriormente se tratan las crisis con respecto a las organizaciones productivas.

Sector	Total de Empresas población objetivo	Personas empleadas en empr. en la población objetivo	Empr. que usan comp.	Empleados que usan comp.	Empr. que usan Internet	Empleados que usan Internet	Empr. con página web	Empr. con intranet	Empr. reciben pedidos Internet	Empr. hacen pedidos Internet	Empr. con Internet de banda angosta	Empr. con Internet de banda ancha fija	Empr. con Internet banda ancha móvil	Empr. con red LAN	Empr. con extranet
Manufacturas	31866	3522722	28573	857632	28244	712165	13646	8693	3238	4697	4572	27123	8130	20671	2443
Comercio al por menor	26004	1734394	23464	549642	22997	419723	8448	7895	2399	4912	2983	21645	3802	17534	2157
Servicios de alojamiento temporal y de preparación de alimentos y bebidas	19967	712213	15004	120893	12239	102159	7035	5516	1377	1309	2921	11034	1191	10484	1399
Comercio al por mayor	12431	654575	12410	276907	11814	227184	6936	4660	2041	2772	2147	11529	4105	10019	763
Servicios educativos	13091	529721	13091	213973	13091	210024	8057	4586	69	1365	2027	11486	1506	8938	113
Servicios profesionales, científicos y técnicos	8828	375471	8403	225712	8403	214681	4606	4292	444	2318	295	8402	2878	7172	759
Transporte, correos y almacenamiento	7510	767565	6457	196079	5980	181756	2205	2448	304	808	459	5762	1723	4881	808
Otros servicios (personales, reparación y mantenimiento)	7200	148787	6156	39616	5512	35456	2159	1143	7	315	921	4966	1067	4381	363
Serv. de apoyo a los negocios y manejo de desechos y servicios de remediación	5306	1105852	5111	229026	5012	159405	2417	1616	393	830	1141	4390	1360	4359	589
Serv. de salud y de asistencia social	9557	274758	7102	85174	6824	61995	2814	1602	205	856	2085	6294	1000	4295	396
Serv. inmobiliarios y de alquiler de bienes muebles e intangibles	3758	104977	3217	39857	2692	37624	1015	965	159	421	444	2388	816	2348	91
Construcción	2027	133267	2027	34771	2004	31680	621	554	301	393	330	1822	711	1773	197
Información en medios masivos	1657	246756	1593	156270	1593	88597	1363	645	162	290	101	1586	489	1448	286
Serv. financieros y de seguros	971	372926	970	223962	963	150743	719	554	44	189	112	961	342	892	217
Minería	751	155044	669	48364	640	44119	346	222	5	134	90	603	144	445	97
Corporativos	63	46918	57	30557	58	29421	47	39	5	10	8	58	40	57	27
GTDEE,SAGDCF	37	132877	36	24898	36	23080	25	29	1	10	4	36	15	34	5
Totales	**151024**	**11018823**	**134340**	**3353333**	**128102**	**2729812**	**62459**	**45459**	**11154**	**21629**	**20640**	**120085**	**29319**	**99731**	**10710**

Tabla 1.2. Uso de TIC en empresas en México de acuerdo con su sector productivo. Abreviaturas: Empr. = Empresas; Serv.= Servicios; Comp = Computadoras; GTDEE, SAGDCF="Generación, transmisión y distribución de energía eléctrica, suministro de agua y de gas por ductos al consumidor final". Adaptado de Instituto Nacional de Estadística y Geografía (2015).

Indicador	Total		10 a 49		50 a 249		Más de 250	
	Cantidad	%	Cantidad	%	Cantidad	%	Cantidad	%
Total de Empresas en la población objetivo	156620	100	132398	100	18921	100	5301	100
Número total de personas empleadas de las empresas en la población objetivo	11216872	100	2413290	100	2088732	100	6714850	100
Empresas que usan computadora	138881	88.7	**114916**	**86.8**	18675	98.7	5290	99.8
Empleados que usan computadora	3421427	30.5	846904	35.1	629734	30.1	**1944789**	**29.0**
Empresas que usan Internet	132573	84.6	108819	82.2	18477	97.7	5277	99.5
Empleados que usan Internet	2793463	24.9	783634	32.5	563910	27.0	1445919	21.5
Empresas con página web	64920	41.5	47545	35.9	13207	69.8	4168	78.6
Empresas con intranet	46135	29.5	33864	25.6	8547	45.2	3724	70.3
Empresas que reciben pedidos por Internet	11407	7.3	9005	6.8	1899	10.0	503	9.5
Empresas que hacen pedidos por Internet	22224	14.2	17676	13.4	3747	19.8	801	15.1
Empresas con Internet de banda angosta	21159	13.5	17209	13.0	2971	15.7	979	18.5
Empresas con Internet de banda ancha fija	124272	79.3	101444	76.6	17712	93.6	5116	96.5
Empresas con Internet de banda ancha móvil	29758	19.0	21967	16.6	5425	28.7	2366	44.6
Empresas con red LAN	103126	65.8	81410	61.5	16667	88.1	5049	95.2
Empresas con extranet	10781	6.9	6927	5.2	2282	12.1	1572	29.7

Tabla 1.3. Uso de TIC en empresas de acuerdo a la cantidad de empleados con los que cuentan. Adaptado de Instituto Nacional de Estadística y Geografía (2015).

1.3 Conceptos generales de crisis

1.3.1 Crisis causadas por fenómenos naturales

Gran parte de la literatura que trata sobre prevención de crisis enfoca su atención en los fenómenos naturales. El conocimiento generado sobre esta perspectiva está muy desarrollado y expone distintas formas de pensar sobre las etapas de prevención, mitigación y recuperación de desastres. En Gelman & Macías (1983) se señala la falta de planes de acción en aquel entonces y la falta o ineficacia de los planes de procedimientos de coordinación de los organismos de rescate en emergencias. Se cita también la importancia de que los planes de acción los deben realizar quienes participan en la atención de emergencias con base en lineamientos y una metodología que considere la realización del rescate y

la coordinación con las entidades involucradas, como parte de un contexto mayor de protección y restablecimiento. Dichos autores definen varios conceptos. Por un lado consideran a un *Sistema Afectable*, que es aquel que está expuesto a sufrir eventos que pueden modificar sus condiciones y pasar desde un *estado Normal* o un *estado Deficiente* a un *estado de Desastre*, en el cual se presentan daños graves. Por otro lado definen a un *Sistema Perturbador* como aquel en donde se genera un *acontecimiento perturbador* que puede impactar a un *Sistema afectable* y modificar sus condiciones a un *estado de Desastre*. En específico, a dicho *evento perturbador* lo denominan *Calamidad*.

En su *Plan General de Protección y Restablecimiento* proponen un organismo coordinador para unificar y controlar a las demás entidades involucradas. Se indica que las actividades para esta entidad de gestión deben considerar 3 fases generales que corresponden a tres planes principales: 1) Plan general de prevención de calamidades y mitigación de sus impactos, 2) Plan general de atención a emergencias para salvar vidas y rehabilitar servicios de soporte de vida y 3) Plan general de recuperación y mejoramiento de las condiciones previas. Los objetivos de los dos primeros planes están enfocados a la reducción de riesgos o protección en el *Sistema Afectable*; y el objetivo del tercer plan se orienta al restablecimiento de sus condiciones de funcionamiento. Aspectos cruciales en la elaboración del plan de emergencia que remarcan son la continua actualización de los planes, la participación de expertos en el tema, la consideración de encadenamientos de calamidades y suma de sus impactos definiendo límites mínimos y máximos de su gravedad (Gelman & Macías, 1983). La ejecución de estos planes y sus objetivos se ubican con respecto a la aparición de la *Calamidad* y el *Desastre* en la figura 1.11.

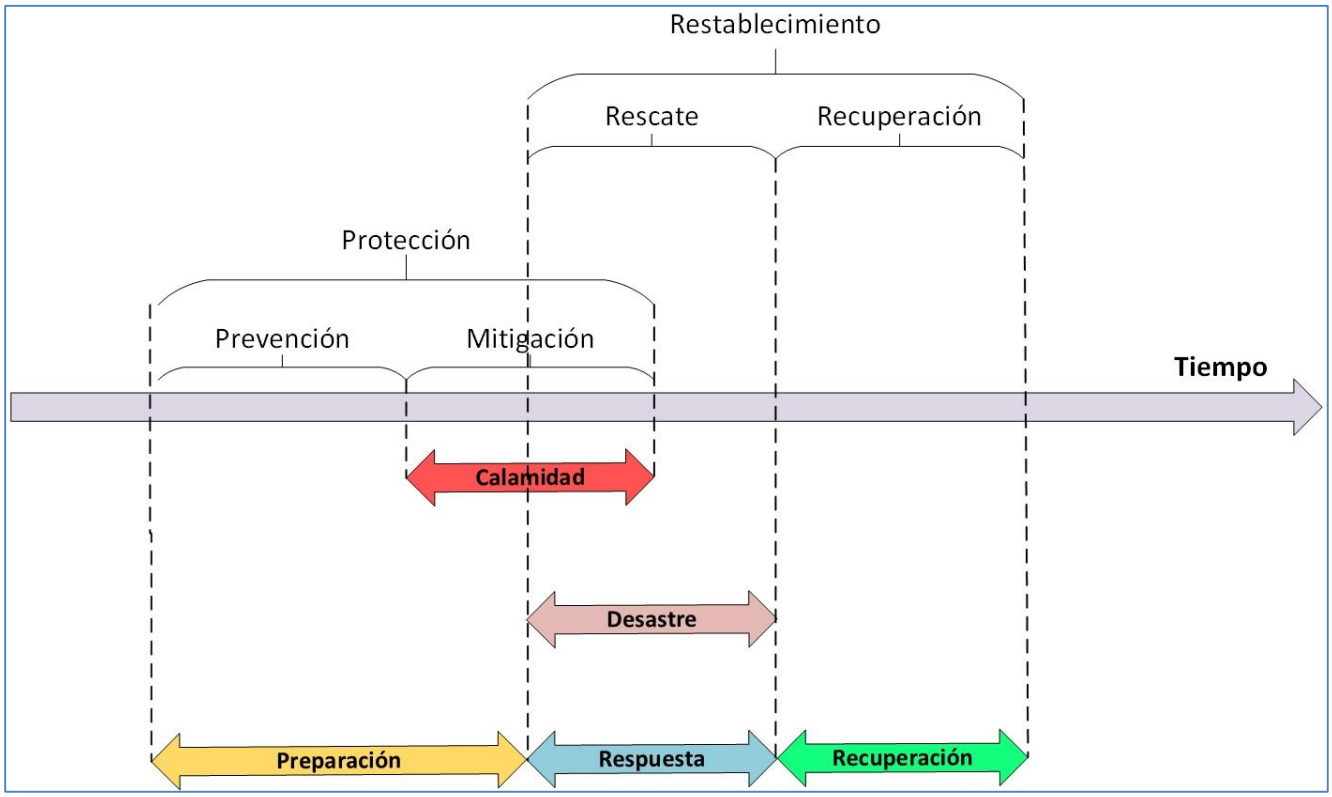


Figura 1.11. Ubicación temporal de los planes de protección y restablecimiento ante una calamidad y desastre. Adaptada de Gelman & Macías (1983).

1.3.2 Crisis en las organizaciones

En la literatura existente, es común usar el término *Crisis* para referirse de forma general a las situaciones de emergencia y desastre en las organizaciones, incluidas aquellas que se refieren a los desastres con respecto a las tecnologías. Muchos autores se han dado a la tarea de extrapolar estas ideas de planeación para la prevención, respuesta y recuperación en las organizaciones sobre una base sólida de conceptos.

En Pollard & Hotho (2006) se hace referencia a la importancia de la administración de las crisis y la integración de un plan de crisis en los procesos estratégicos de la organización. Presentan la definición de crisis citada en Pearson & Clair (1998):

> Un evento de baja probabilidad, de alto impacto que amenaza la viabilidad de la organización y que se caracteriza por una ambigüedad de la causa, el efecto y los medios de resolución, así como por la creencia de que las decisiones deben tomarse rápidamente.

En dicho artículo se cita también la clasificación de crisis en las organizaciones propuesta en I. I. Mitroff (2004) en donde se remarca que los tipos de éstas no son mutuamente excluyentes:

- Relacionadas a la economía (problemas laborales, crisis económicas, caídas en rentabilidad)
- Informacionales (manipulación o pérdida de datos)
- Físicas (pérdida o degradación de la planta o instalaciones clave, fallas en productos, explosiones), Recursos humanos (muerte de personal clave, corrupción, vandalismo interno)
- Relacionada a la reputación (rumores, manipulación de logotipos corporativos, sitios web)
- Actos psicópatas (terrorismo, secuestro, actos criminales)
- Desastres naturales (incendios, inundaciones)

En Simola (2005) se habla del papel de la ética en la prevención primaria de las crisis organizacionales, la cual define como un conjunto de actividades destinadas a prevenir situaciones de crisis en conjunto. En dicho documento se cita a Ian Mitroff al asegurar que no todas las crisis se pueden prevenir, pero que sin embargo la mayoría de las crisis son precedidas por señales de advertencia, a través de las cuales pueden ser prevenidas. Siguiendo con la idea expuesta en I. I. Mitroff & Anagnos (2000), Simola (2005) refiere que la detección de esas señales sólo será eficaz en la medida en que la información sea identificada por alguien facultado para actuar.

En Kovoor-Misra, Zammuto, & Mitroff (2000), se repasan concepciones comunes a varios enfoques para enfrentar las crisis y se afirma que hay una marcada discrepancia entre la literatura existente sobre preparación ante crisis y lo que realmente se practica en las organizaciones. Estas afirmaciones se sustentan en resultados de un estudio inductivo de los preparativos ante crisis mayores de nueve organizaciones cuya columna vertebral son las tecnologías y cuyas precauciones deben ser en extremo

amplias por la catástrofe que una crisis en ellas puede generar. En este sentido, dichos autores afirman la idea de que las crisis son causadas por una combinación de fallas humanas, tecnológicas y de organización dentro de las entidades, y por el efecto de sistemas externos; definen a la *preparación para una crisis* como las actividades tomadas y los procesos desarrollados por una organización para *prevenir*, *contener* y *recuperarse* de las crisis. Con respecto a la primera de ellas son comunes 3 prescripciones para las organizaciones: a) Abordar proactivamente las causas sistémicas subyacentes de crisis potenciales, b) Institucionalizar mecanismos de detección de señales, y c) Aprender y *desaprender* mientras se enfrentan a las crisis, lo que implica que la alta dirección debe hacer caso a las opiniones disidentes. En Kovoor-Misra, Zammuto, & Mitroff (2000) también se defienden la idea de que es necesario generar equipos interdisciplinarios que hagan frente a las crisis y que reciban entrenamiento frecuentemente con técnicas como juegos de rol y creación de escenarios con el fin de reducir la ansiedad y discapacidad de actuar al momento en que realmente se presente una crisis; pero también añaden que se deben diseñar planes que atiendan las crisis de los distintos tipos que se establecen en I.I. Mitroff (2004), y que ya se mencionaron anteriormente. Con respecto a las prescripciones para recuperarse de una crisis mencionan la importancia fundamental de aliviar los traumas psicológicos generados, ansiedad y depresión por ejemplo, ya que las entidades que lo hacen se suelen recuperar más rápidamente. Los resultados presentados de dicho trabajo revelan que todas las empresas del estudio prestaban especial atención a precauciones técnicas pero que a otros subsistemas los dejaban de lado. De forma similar, estas organizaciones habían realizado investigaciones después de que se presentaron crisis técnicas, pero no contaban con mecanismos formales para sistematizar el aprendizaje de otros tipos de crisis. Algo común en estas organizaciones con un enfoque tecnológico fue la limitada comunicación entre los niveles organizacionales con respecto a los planes de gestión de crisis; en los niveles corporativos sólo se sabía que existía preparación para crisis técnicas pero no en qué consistía. Con respecto a los planes de recuperación sólo una de las organizaciones contaba con un programa de atención psicológica para los afectados.

En Pollard & Hotho (2006) se afirma que las precauciones que deben tener las organizaciones a estos tipos de crisis dependen del campo de actividad en el que se desempeñen. Se considera que al igual que en la administración de crisis se requiere de la atención de un grupo de administradores, más que sólo la participación de un solo individuo o del departamento directamente relacionado con la emergencia, y que los planes de emergencia deben cubrir un amplio espectro de eventualidades. Se asegura que en una administración de riesgo eficiente, las personas se deben involucrar en el diseño de los planes de crisis y en los procesos para mitigar el impacto y consecuencias de una situación de emergencia, y que se deberá ser cuidados en la definición de roles, la determinación de los canales de comunicación y estructuras de mando y responsabilidades. Además, se hace notar que un plan de administración de crisis es necesario, pero no es una medida suficiente para prevenir la emergencia o mitigar sus efectos. De forma similar, se afirma que en ocasiones las organizaciones no toman en cuenta las señales de aquello que causa o advierte una crisis por seguir estrictamente lo establecido en los planes que han diseñado, y que la confianza excesiva en planes apegados a las tipologías de las crisis puede generar un falso sentido de seguridad (Pollard & Hotho, 2006).

También en Pollard & Hotho (2006) se menciona que una técnica para la administración de crisis es la planeación de escenarios, que básicamente consiste en plantear la pregunta "¿qué pasa si..?" y con ello pensar futuros probables a las condiciones planteadas y describirlos en narrativas rigurosas y posteriormente diseñar medidas estratégicas para solventarlas. En dicho documento se señala que desde esta perspectiva el proceso de administración de crisis tiene características similares con el proceso de planeación estratégica, tales como la valoración de las condiciones del contexto, los stakeholders y la alta dirección; en ambos procesos se distingue el diseño de la implantación; y en ambos casos se evalúa el impacto de las estrategias seleccionadas. Del mismo modo los autores son conscientes del efecto que pueden tener la cultura organizacional, la autoconfianza de los directivos en los planes generados o condiciones existentes y la falta de incidentes anteriores referentes a la organización de todos sirven para influir en las actitudes en relación con la necesidad de la gestión de crisis; y en consecuencia los planes generados serán diferentes entre organizaciones.

En Jaques (2007) se exponen algunas de las limitaciones de ciertos enfoques para la administración de crisis y presenta un modelo que intenta solventar dichas deficiencias. En dicho trabajo se citan 2 definiciones para el termino *crisis*, una de ellas es la citada anteriormente en Pollard & Hotho (2006), sin embargo el autor hace hincapié en que no existe en la literatura especializada consenso en la definición de ese concepto, ni del término problemas, ni mucho menos de lo que es la administración de crisis, y de esta última destaca que lo importante es que sea vista como una disciplina proactiva que engloba procesos interrelacionados de la preparación para una crisis, dé respuesta táctica cuando esta se presente y de procesos de recuperación. Con respecto a modelos de ciclo de vida para la administración de crisis explica que la mayoría de ellos tienen como punto débil el ser lineales en la ejecución de sus fases y en manejar las situaciones problemáticas una a la vez por considerar que se presentan de forma secuencial.

Menciona que durante los recientes 20 años no ha habido una evolución importante en la administración de crisis y como prueba menciona el modelo de crisis de seis pasos de Littlejohn (diseño de la estructura, selección de equipo de crisis, entrenamiento del equipo, auditoría de la situación de crisis, plan de contingencias, gestión de la crisis), el modelo de 4 fases de Fink (prodrómica, aguda y crónica, la resolución) y el enfoque de Burnett de la matriz de clasificación de 16 celdas (Jaques, 2007).

Lee, Woeste, & Heath (2007) presentan los resultados de un estudio que se realizó a 122 organizaciones estadounidenses de distintos ramos en el artículo. Los resultados cuantitativos indican que el 79% de las compañías reportó que tenían un plan de administración de crisis y que el 71% de ellas tenían conformado un equipo de gestión de crisis. Por otro lado sólo una de las empresas indicó que no tenían asignada alguna persona para cumplir con las funciones de vocero del equipo anticrisis. En cuanto al entrenamiento que recibían poco más del 50% de las organizaciones indicó que éste sólo era la revisión del plan y sólo 29.5% de ellas realizaba ejercicios de simulación. Se encontró también que el 26% realizaba prácticas anualmente, que 16.4% nunca practicaban, y que el 10.7% lo practicaban cada 3 meses. Los autores destacan que las organizaciones con mejores resultados prácticos anticrisis

participan más en actividades de planeación y capacitación, pero que una deficiencia amplia en el resto de las empresas sobre las que se realizó el estudio es la poca capacitación del personal de forma individual y de forma grupal. Por otro lado, afirman que no hay un patrón claro en la forma en cómo las empresas con excelentes prácticas promueven la formación en su personal.

Por otra parte, en Kovoor-Misra et al. (2000) se señala que la brecha entre lo indicado en la literatura para la preparación ante desastres y lo que sucede en la realidad se debe a factores contextuales, en particular cinco. Dos de ellos son la *tecnología base* y el *background* educativo de los administradores principales, ya que mientras más diversa sea la formación educativa de los miembros de la alta dirección o administración se tendrá un mejor panorama de la situación por los distintos enfoques en la toma de decisiones estratégica y se podrán identificar en mayor grado los problemas y proponer soluciones diversas. Otro elemento que afecta la preparación para crisis son las influencias de poder, ya que los puestos con funciones de mayor poder determinan el enfoque de los planes a realizar. Los otros 2 factores son la experiencia con crisis pasadas y la estructura de la organización.

Estos cinco factores se explican en las siguientes proposiciones que plantean en Kovoor-Misra et al. (2000):

1. Las organizaciones son propensas a prepararse para crisis que la alta administración percibe como amenazantes a la tecnología estructural de la empresa. Las áreas que no afectan las operaciones principales de la empresa reciben menor atención.
2. Mientras más homogénea sea la preparación educativa de la alta administración será menos probable que se desarrollen planes de gestión en un rango más amplio de tipos de crisis.
3. Los tipos de crisis para las que se prepare la organización reflejan el interés de las más poderosas funciones organizacionales.
4. Es más probable que las organizaciones se preparen para el tipo de crisis que han experimentado anteriormente.
5. Mientras más grande sea el grado en el cual la toma de decisiones sea descentralizada, se involucrará menos la alta dirección en la preparación para las crisis.
6. Una organización estructurará sus actividades de preparación de crisis de acuerdo con la estructura de su organización.
7. Mientras más grande sea el desarrollo de la estructura funcional, es más probable que las actividades para la preparación para crisis sean funcionalmente segmentadas.
8. Cuanto mayor sea el grado en que la estructura existente se organiza a lo largo del flujo de trabajo o líneas de proceso, es más probable que no haya integración entre los planes de crisis a través de diferentes tipos de crisis.

Otro aspecto que se destaca a lo largo del artículo recién citado es que de acuerdo con la complejidad de una organización se incrementa el potencial de crisis, además de señalar que las prescripciones sobre la preparación para las crisis no se pueden tomar como *un traje que a todos les queda*, sino que debe *ajustarse* a las realidades contextuales de cada organización.

1.3.3 Crisis relacionadas a las TIC

A lo largo del tiempo se ha presentado una gran cantidad de desastres en los que la parte técnica y social se han visto involucradas directamente o indirectamente, teniendo incluso consecuencias catastróficas: quebrantos millonarios, daños al medio ambiente y pérdida de vidas humanas, por ejemplo. Algunos eventos que ejemplifican esto son el derrame de petróleo en el golfo de México en el año 2010 que se describe en Bozeman (2011), la desintegración del transbordador espacial Columbia y la muerte de toda su tripulación, así como la explosión del reactor nuclear de Chernobyl en 1986 (Tarn et al., 2008) o la crisis por fallas en neumáticos Firestone en el año 2000 (Alpaslan, Green, & Mitroff, 2009). En la figura 1.12 se presenta una línea de tiempo con algunos desastres ocurridos desde finales de la década de 1970 en los que las causas han se conforman por una parte técnica y una parte social.

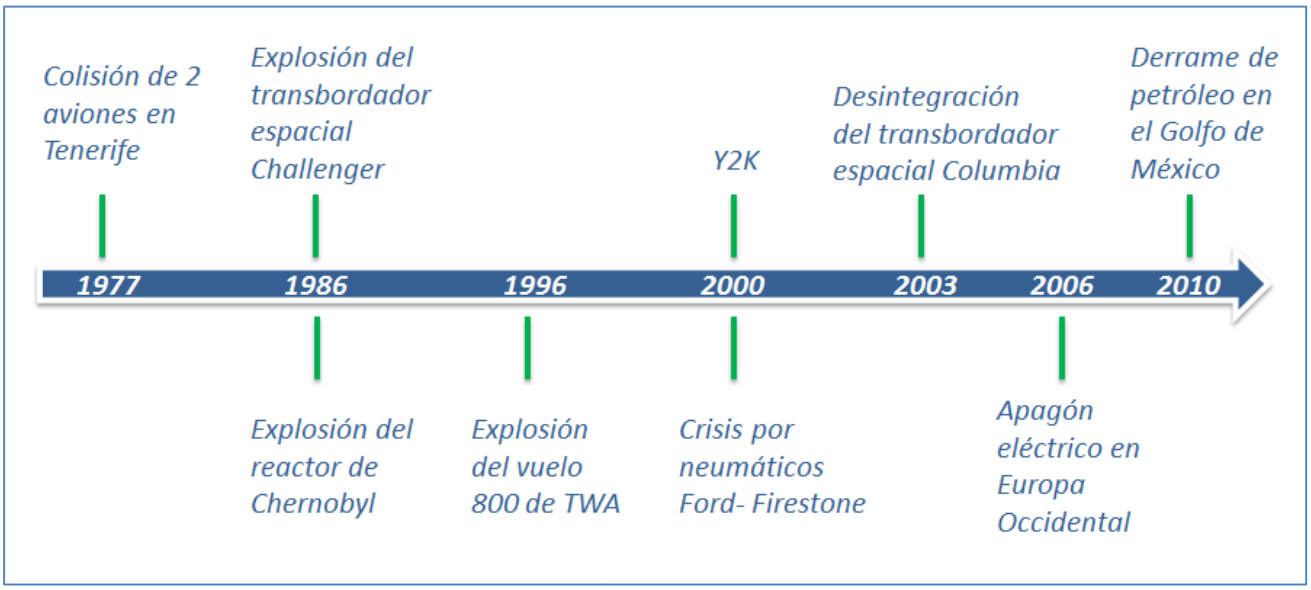


Figura 1.12. Línea de tiempo con algunos desastres socio-técnicos. Información de Bozeman (2011), Tarn, Wen, & Shih (2008), Alpaslan, Green, & Mitroff (2009), Manion & Evan (2002) y I. Mitroff & Alpaslan (2003).

En varios sectores de la industria se reconoce el impacto de las TIC en cuestiones de seguridad y riesgos. Por ejemplo, en Panteli & Kirschen (2011) se indica que la fuerte dependencia de los sistemas de potencia y seguridad hacia las TIC hace que la infraestructura entera sea más vulnerable a fallas de la información y ataques maliciosos. En dicho documento se desarrolla un estudio del impacto y probabilidad de apagones catastróficos a causa de una falla en las tecnologías relacionadas. Y en Panteli (2013) se refuerza la idea de que los errores humanos así como una inadecuada infraestructura de TIC y sus fallas tienen un peso significativo en este tipo de incidentes. Por otra parte, en el resultado del estudio que se presenta en Gardner & GRID Consortium (2007) se concluye que áreas en sistemas de generación de energía son vistas como críticas y/o vulnerables debido a su relación con las TIC. De acuerdo con Khidzir, Mohamed, & Arshad (2010), en los casos de outsourcing para los servicios de TIC

en las organizaciones también se presentan incidentes en la seguridad de la información que pueden ser difíciles de manejar y de mitigar. Se concluye en dicho estudio que las vulnerabilidades más críticas son la insuficiente atención a los factores humanos en el diseño e implementación del sistema y que las amenazas más críticas son los errores de los sistemas de TIC.

Otro aspecto importante de las TIC es el software que usan ciertos dispositivos para realizar alguna actividad o el que usan las computadoras para realizar algún tipo de procesamiento. A este respecto se cuenta con metodologías para desarrollo de software que tienen como objetivo generar un producto de calidad, tal es el caso de las especificaciones del *Ciclo de vida del software* (ISO/IEC-IEEE, 2008) o la *Ingeniería de Software* que en Pressman (2010) se define como "La aplicación de un enfoque sistemático, disciplinado y cuantificable al desarrollo, operación y mantenimiento de software" y que debe basarse en un compromiso organizacional de calidad. En Medikonda & Ramaiah (2014) se indica que el software puede tener un impacto severo en la seguridad de los sistemas debido a que un proceso general de ingeniería de software no es insuficiente para generar por sí mismo aplicaciones seguras y confiables, sobre todo en *sistemas de seguridad* crítica que define como *aquellos que tienen el potencial para causar accidentes*. A este respecto se señala en dicho artículo que el software es peligroso si puede causar un peligro, ya sea que provoque que otros componentes lleguen a ser peligrosos o si es usado para controlar un peligro, y que la gravedad de los eventos que puede producir son catástrofes como pérdidas de propiedades físicas, daño físico, y pérdida de vidas. Ejemplos de esto son el caso sucedido a mediados de la década de 1980 en que una máquina de radio terapia controlada por computadora suministraba sobredosis masivas provocando daños a varias personas e incluso la muerte, también la explosión durante el despegue en 1996 de un cohete de la Agencia Espacial Europea, o el caso reportado en 2008 por la Oficina de Seguridad de Transporte de Australia en el que se dijo que a causa de información incorrecta de una computadora defectuosa se dispararon una serie de alarmas y posteriormente ocasionó que las computadoras del vuelo Airbus A330 pusieran al jet en picada por 197 metros. De esta forma se afirma que además de las metodologías de desarrollo, los ingenieros de software en sistemas de seguridad crítica requieren de una clara comprensión del rol del software en el sistema Medikonda & Ramaiah (2014), con lo que se identifica que el papel humano es de gran importancia en la prevención de posibles catástrofes.

1.4 Definición del problema y del objetivo

En las secciones anteriores se ha abordado la presencia e importancia que tienen las Tecnologías de la Información y Comunicación en el mundo. De acuerdo con la opinión de organismos internacionales las TIC tienen el potencial para mejorar las condiciones de vida de la humanidad, para ello es indispensable garantizar el acceso a ellas en primer lugar y después hacerlo de forma dirigida, eficaz y eficiente. Independientemente del sector en el que desarrollan sus actividades y sin distinción de sus fines, las organizaciones se han visto beneficiadas por el uso y desarrollo de las tecnologías en general.

México, a pesar del rezago en la difusión, adopción, uso y desarrollo de las TIC con respecto a otros países tiene una gran oportunidad para mejorar en sus condiciones de seguridad, comerciales, de salud, educativas y de desarrollo, por mencionar algunos ámbitos. Con la estrategia nacional digital, el gobierno mexicano reconoce la importancia del uso de las TIC en diversos ámbitos, incluyendo la salud, educación, economía, como enlace con la ciudadanía para trámites públicos y como medio de información, entre otros. De esta forma es de esperar que cada vez más servicios públicos se realicen a través de plataformas tecnológicas, o se apoyen en éstas para hacerse más eficientes o ser más accesibles.

En el caso del sector privado la situación es parecida. Conforme a la información que se ha presentado, en México no más del 15% de las empresas en general ocupa Internet en sus relaciones con clientes y con proveedores. Sin embargo, es importante hacer notar que estos bajos valores se deben a la gran cantidad de micro y pequeñas empresas que se tomaron en cuenta en el estudio y cuyo alcance en cuanto a actividades comerciales es limitado, al igual que su tiempo de operación por los niveles de eficiencia y complejidad en los procesos que comúnmente opera en su organización. Si se observa nuevamente la tabla 1.2 se verá que en las empresas más grandes respecto a la cantidad de empleados, y cuyo funcionamiento supone una organización mayor, el uso de computadoras y el Internet llega a porcentajes mayores, y en consecuencia es necesario que el funcionamiento de éstos sea efectivo y eficiente. Así, una falla en las TIC de las que dependen ocasionaría en el mejor de los casos al menos un retraso en el desarrollo de sus actividades, y en el peor de los casos podría generar consecuencias de trascendencia no deseadas para la organización en cuestión; es decir, se podría generar una crisis a partir del área donde se lleve a cabo la gestión de TIC.

En este trabajo el significado de este último término se desarrolla con base en la idea de conducción que se propone en Gelman & Macías (1983) y que se refiere a aspectos de regulación, gobernación, manejo, administración, control y guía de un determinado objeto. De esta forma se propone la siguiente definición para la *Gestión de TIC*:

> *Actividades de administración, de operación, de mantenimiento, de monitoreo y de control de sistemas técnicos y de procedimientos administrativos y organizacionales relacionados con actividades al interior del área de TIC que le permiten conseguir los fines para los que fue concebida*.

Se puede considerar que en México cada vez será más grande la cantidad de empresas que consigan un nivel de madurez mayor y en consecuencia cada vez serán más las que utilicen TIC en mayor grado, no sólo en la fabricación de productos o en la prestación de servicios, sino también en el valor agregado. Así, el impacto de las TIC en el sector privado y en el gubernamental será mayor por ser un factor de potencialización para sus resultados, y al mismo tiempo por ser un factor de riesgo debido a la fuerte dependencia que se tenga de ellas.

Con base en esta última consideración las organizaciones deben dedicar suficiente atención a las actividades de prevención, contención y recuperación por situaciones de crisis en las áreas de gestión de TIC. En primer lugar, deben estar concientes que las causas de las situaciones de emergencia son variadas. Un clasificación de dichos factores es la siguiente:

- Aspectos sociales. Consideraciones personales y opiniones diversas sobre la forma de trabajo, la manera en como se relaciona el personal, la falta de reconocimiento y la desmotivación del personal, por mencionar algunos.
- Aspectos organizacionales. Como ejemplos se puede citar a las fallas o inconsistencias en reglamentos o procedimientos, a la ambigüedad en objetivos o actividades de las áreas, y a la desorganización en la toma de decisiones.
- Situaciones técnicas. Fallas o desempeño deficiciente de los sistemas técnicos.
- Errores operacionales. Fallas en la forma de hacer las actividades asignadas, usos inadecuados de herramientas para el desempeño de las tareas, no seguir los reglamentos ni medidas de seguridad o normas de calidad.

Identificar las causas de las situaciones de emergencia en una organización sólo es uno de las actividades generales, pues la problemática respecto a la gestión de crisis en las organizaciones se integra por muchos otros factores, algunos de los cuales son:

- El diseño de actividades de gestión de crisis por una sola persona, por un grupo reducido o por personas con una formación homogénea, lo cual limita los puntos de vista para generar acciones y el llevarlos a cabo.
- La poca atención para la gestión de emergencias en áreas que no afectan las operaciones principales de la empresa de forma directa, pero que sin embargo contribuyen a realizar tareas de soporte que solas o en combinación con otras contribuyen de forma importante para el adecuado funcionamiento de la organización.
- El poco interés de la alta dirección en la revisión o supervisión de actividades de gestión de crisis.
- Actividades de gestión que sólo contemplan una solución de problemas de manera superflua o que sólo de los efectos y no las causas.
- Planes de atención a crisis que se enfocan en sólo dar una respuesta y no consideran acciones de prevención.
- El desarrollo de planes de gestión sólo para aquellas emergencias que se han presentado anteriormente en la organización.
- La elaboración de planes de gestión de crisis sin integración entre las distintas áreas de las instituciones.
- Una inexistente o ineficiente cultura de aprendizaje de experiencias anteriores.
- Mecanismos inexistentes o ineficaces para la detección de señales de lo que causa o vaticina una emergencia.

- Una escasa capacitación y/o entrenamiento en actividades de gestión de crisis, lo que conlleva a una insuficiente generación de propuestas.
- Planes de atención de emergencias con actividades genéricas y no las apropiadas a la situación de la organización.

De forma particular a las crisis asociadas a TIC en las organizaciones, se destacan los siguientes elementos que también integran la problemática.

- Preparación deficiente en actividades de gestión de TIC.
- Desarrollo de actividades de gestión de TIC sin planeación y de manera urgente.
- Desinterés en áreas esenciales en la organización para apoyar planes de prevención de crisis asociadas a tecnologías.
- Desarrollo de planes de atención a crisis desarrolladas sólo bajo un enfoque técnico y sin considerar aspectos organizacionales ni sociales.
- Desarrollo de planes de gestión de crisis para cuando ésta se presenta, sin considerar acciones de prevención.

Estos 2 últimos problemas son a los que se enfoca la propuesta de esta tesis, debido a que se considera que no se les ha dado la suficiente importancia en la práctica.

La interacción entre los elementos sociales y técnicos de las áreas laborales que integran una organización determina su desempeño y de la misma forma puede generar ciertos riesgos en ella. En las áreas de gestión de TIC dicho factor por lo general pasa desapercibido ante la presencia de otros elementos más visibles, a pesar de tener gran importancia no sólo para la misma área y sus actividades internas, sino también para toda la empresa a causa de las dependencias hacia la tecnología.

Por otro lado, es importante destacar que la mayoría de las actividades de gestión se enfocan en dar una respuesta a la crisis una vez que se ha presentado, en la mitigación de los efectos adversos causados, en el restablecimiento de operaciones y en la recuperación de un estado anterior a la crisis, pero con este trabajo se abordarán las crisis en una fase distinta y poco tratada en comparación con lo recién mencionado: *La prevención*. Bajo esta perspectiva las organizaciones no se verán en la necesidad de interrumpir sus actividades y destinar recursos y tiempo a causa de un evento adverso e inesperado ya que se estará en posibilidad de actuar para evitarlo.

Algunos de los puntos esenciales para la prevención de crisis son la detección de señales que anuncian que están próximas a presentarse, así como la identificación de riesgos en la organización, su eliminación o su control. Dichos aspectos son la base que toma la propuesta de este trabajo.

Por tratarse de un área donde las actividades primarias se refieren a la administración de la tecnología la gran mayoría de los mecanismos de control existentes se enfocan sólo en aspectos técnicos; y sobre esto existe una gran cantidad de herramientas, técnicas, recomendaciones y estándares, pero no se consideran aspectos sociales ni organizaciones. Sin embargo, este trabajo la atención a crisis se

abordará desde un punto de vista diferente y poco tratado en lo que respecta a las TIC: el enfoque socio-técnico.

A partir de lo anterior se establece el objetivo general de esta tesis:

> *Desarrollar un Sistema de Planeación para la prevención de crisis con origen socio-técnico en áreas que se dedican a la gestión de las Tecnologías de la Información y Comunicación, con base en los principios del enfoque socio-técnico y de la estructura organizacional.*

Esto servirá a las organizaciones para evitar crisis en áreas de administración de TIC a partir del enfoque socio-técnico y la estructura organizacional, sin importar si su negocio principal gira en torno a la eficiencia en las tecnologías que ocupa o si utilizan las TIC como mera herramienta en sus procesos cotidianos. Por último, es importante mencionar que el tipo de entidades para las que se pretende sea útil este *Sistema de Planeación* son aquellas que tienen un área que se dedique exclusivamente a la gestión de TIC.

Capítulo 2. Crisis socio-técnicas en áreas de gestión de TIC y enfoques de análisis

En el primer subtema de este capítulo se profundiza en la descripción formal de las crisis con origen socio-técnico y de otros conceptos relacionados con el fin de establecer de una manera más precisa las causas, consecuencias e impacto que tienen en las organizaciones. A partir de esta base, en el segundo subtema se revisan enfoques que distintos autores han propuesto al respecto y se seleccionan total o parcialmente las propuestas afines y útiles para el desarrollo de una estrategia para la consecución de los objetivos de estas tesis. En el tercer subtema se hace una breve descripción de las características de los enfoques a partir de los que se plantea el desarrollo de los planes de prevención de crisis. Finalmente se presenta la estrategia de investigación.

2.1 Crisis socio-técnicas

2.1.1 Conceptos base sobre la gestión de crisis socio-técnicas

En distintos sistemas de los que se tiene conocimiento, ya sean sociales, naturales, científicos, organizacionales, laborales, etcétera, se presentan eventos que tienen un impacto importante en su comportamiento habitual, que los pueden sacar de equilibrio, cambiar su rumbo de forma

trascendental e incluso determinar su existencia o desaparición. En la literatura estos sucesos se identifican con distintos nombres debido a la formación de los autores y por supuesto al ambiente donde se presentan y desde el que se abordan. Así, para los desastres naturales se utiliza el concepto de *Calamidad* para referirse al evento perturbador que ocasiona *Desastres*, es decir, daños en los asentamientos humanos (Gelman & Macías, 1983). En las organizaciones humanas otro término que se utiliza para referirse a sucesos que tienen características similares es el de *Crisis*, del cual se acepta ampliamente la definición de Pearson y Clair que se presenta en Pollard & Hotho (2006):

> Un evento de baja probabilidad, de alto impacto que amenaza la viabilidad de la organización y que se caracteriza por una ambigüedad de la causa, el efecto y los medios de resolución, así como por la creencia de que las decisiones deben tomarse rápidamente.

En otros trabajos, para establecer una clara diferencia en las organizaciones humanas de los eventos perturbadores que se consideran naturales se ocupa el concepto de *Desastres de origen humano* (*Man-made disasters*) para referirse a los *desastres socio-técnicos que implican un pérdida del control sobre procesos percibidos como controlables* (Aini & Fakhrul-Razi, 2010). En Ibrahim M. Shaluf et al. (2002) se presenta la definición de Shirivasta sobre los *Desastres de origen humano*: "Evento que ocasiona un daño extenso y ruptura social que involucra múltiples stakeholders y que se desarrolla a través de la complejidad tecnológica, organizacional y procesos sociales."

Por otra parte, en Hovden, Albrechtsen, & Herrera (2010) se considera el término de *Accidente* como el equivalente a eventos que dependiendo de la magnitud de sus consecuencias pueden considerarse como las crisis o desastres de origen humano. Lo definen como un peligro que se puede materializar de forma repentina, es decir, como un evento probabilístico o cadena de eventos con consecuencias adversas, y los clasifican en 4 categorías:

- Daño/pérdida. Lesiones y fatalidades, pérdidas materiales económicas y/o daños a la reputación.
- Incidente. Caídas, deslizamientos, explosiones, etc.
- Condición peligrosa. Herramientas defectuosas, diseños inseguros, labores domésticas con riesgo, etc.
- Actos inseguros. Errores u omisiones.

Jaques (2010) señala que existen varias concepciones acerca de las crisis como la impulsada por Perrow o Coombs, en la que se argumentae que éstas son accidentes normales debido a que son inevitables, impredecibles pero sí esperadas. De forma similar apunta que existen los enfoques contrarios que se refieren a la administración de crisis como actividades continuas con potencial de prevenir y evitar las crisis, y en caso de que se presenten, como actividades posteriores de gestión a largo plazo. En esta línea de investigación, algunos otros autores consideran que los cambios radicales en los

procedimientos y en la organización debidos a la actualización tecnológica pueden desencadenar situaciones de crisis (Carmeli & Schaubroeck, 2008).

En Carmeli & Schaubroeck (2008) se afirma que entre los potenciales riesgos que una crisis conlleva se encuentran:

- Interferencia en la realización de los asuntos habituales y el daño en la productividad.
- Interrupción de las actividades de forma escalada, es decir, en áreas diferentes de donde se presentó inicialmente la crisis.
- Deterioro técnico y de la imagen de la organización, de sus gerentes y propietarios por los seguimientos de los medios de comunicación y/o las autoridades.

De acuerdo con esta idea, las crisis se consideran como un factor determinante en las condiciones de la organización y se les da una connotación contraria al bienestar; sin embargo otros puntos de vista, aunque reconocen su importancia por sus efectos y consecuencias, los llegan a considerar como un suceso favorable debido a la oportunidad que originan para cambiar los componentes, comportamiento, y relaciones de los sistemas que afectan (Carmeli & Schaubroeck, 2008) y con ello reinventarse.

En Aini & Fakhrul-Razi (2010) se citan investigaciones que indican una relación directa entre el nivel de desarrollo de las organizaciones y sus vulnerabilidades, y concluyen que es probable que se incremente en el futuro el impacto de los desastres, ya que se desarrollan comportamientos sociales y tecnologías que pueden ocasionar daños a gran escala a un ritmo mucho mayor que con el que se generan técnicas de control de daño y de respuesta a tales situaciones. Dichos autores concuerdan con la postura de Barry A. Turner (Turner, 1976) en la que los desastres socio-técnicos emergen como propiedades en los sistemas por fallas en la combinación de arreglos técnicos, sociales, institucionales y administrativos.

En Manion & Evan (2002) se indica que para explicar los desastres tecnológicos se tienen que considerar 4 factores: el rol del operador humano, el rol del diseño técnico, el rol de los sistemas organizacionales, y el rol de los factores socioculturales; sin tomar en cuenta los actos de terrorismo tecnológico que son difíciles de categorizar en una de estas 4 causas. En un desastre tecnológico es frecuente que se presenten múltiples causas por separado e incluso combinadas.

En Ibrahim M. Shaluf et al. (2002) se describen 4 casos de estudio de crisis con causas socio-técnicas que tuvieron lugar en Malasia y a partir de ellos se identifican 4 tipos de errores: aspectos sociales como la moral, personalidad, conciencia y experiencia, así como las decisiones de la administración; situaciones técnicas, como cuando no se considera en el diseño el peor de los casos posibles a causa de las presiones administrativas o no se toman en cuenta los análisis de estrés o las especificaciones estándar o no se contempla el diseño de alarmas para advertir de desviaciones del funcionamiento normal; aspectos organizacionales que son el enlace entre los operadores y la administración, deficiencias en aspectos organizacionales que son el enlace entre los operadores y la administración por ejemplo falta de seguridad, políticas de salud, contradicciones de las instrucciones y mala

administración del cambio; y errores operacionales (manejo de las instalaciones, pruebas y almacenaje de materiales peligrosos, reparación incorrecta, etc.).

También destacan que si las causas se presentan durante largos periodos y no se les atiende de inicio pueden ocasionar que las señales de advertencia no sean visibles por su *cotidianeidad* en el desarrollo de las actividades; y por otra parte, que es frecuente que haya deficiencias en la última línea de defensa a crisis.

Otras investigaciones afirman que los desastres tecnológicos se pueden predecir, sólo hace falta un conocimiento más profundo de los sistemas socio-técnicos (Chapman, 2005). Consideran que existen factores de muchos tipos que los ocasionan: humanos, mecánicos, ambigüedades, cambios por evolución de la tecnología, innovación, comunicación pobre, por mencionar algunos. Chapman también refiere que si las evaluaciones de los riesgos no son actualizadas continuamente o si las suposiciones acerca de ellos no son revisadas, cualquier instalación puede ser cada vez más peligrosa independientemente de la tecnología que ocupe. Afirma que los peligros también se dan por elementos psicosociales y la interface con elementos técnicos, que las acciones de las personas son orientadas por modelos mentales que son susceptibles de tener varias fallas: retención de conocimiento caducado, uso de fuentes de información no fidedignas y fallas en los procesos comunicación.

En Tarn et al. (2008) parten de que existen vacíos en las interfaces de los sistemas de control de desastres a gran escala causados por el hombre y proponen medidas para solventar estas deficiencias. Las recomendaciones se sustentan en que las catástrofes o desastres causados por el hombre tienen un patrón común de desarrollo. Consideran que las tecnologías han avanzado mucho pero que a su vez pueden ser causa de grandes desastres y no sólo a consecuencia del descuido de las personas, sino a que el grado de desarrollo de los sistemas automatizados y la combinación de todos los escenarios se encuentra fuera del conocimiento de los diseñadores del sistema, de los sistemas de control existentes y de los expertos en situaciones particulares. Los sistemas socio-técnicos evolucionan a través del tiempo y como consecuencia los peligros también; de forma similar sucede con los peligros generados en el entorno de las organizaciones (Chapman, 2005).

En el Instituto Tavistock desde la década de 1980 se empezaron a plantear enfoques socio-técnicos influenciados por modelos de accidentes debido a su amplia tradición en el estudio de ambientes de trabajo. Anteriormente a los enfoques propuestos se les llegó a criticar que no eran los suficientemente prácticos o científicos, que ninguno de ellos era lo suficientemente específico ni holístico para servir a su propósito. Este interés surgió también en algunas empresas como DuPont, que se enfocó en la responsabilidad de la administración, comportamiento de los trabajadores e indicadores de desempeño seguro basados en el reporte de incidentes. Con el transcurrir del tiempo y la incorporación y actualización de tecnologías en el ambiente laboral ha cambiado la naturaleza de los accidentes y nuevos tipos de peligros han obligado a la modificación de las regulaciones de seguridad y el punto de vista público de seguridad, además de que la prevención de accidentes también ha sido afectada por los cambios organizacionales, afirman Hovden et al. (2010). Dichos autores conciben que la prevención

de accidentes puede llevarse a cabo observando las causas directas y eventos desencadenantes; y que un error común es la identificación de una causa cercana al accidente como la *causa raíz*, lo que puede provocar un falso sentido de seguridad por la eliminación de síntomas en caso de que se solvente dicha deficiencia únicamente pero que no implica un impacto profundo en la reducción de futuros accidentes al no atender las *causas raíces* verdaderas.

Existen 2 escuelas reconocidas que se han enfocado en aspectos de seguridad. Una de ellas, la Normal Accident Theory (NAT) considera que los accidentes son inevitables y normales, y que tal sistema involucra la interacción no anticipada de múltiples fallas. Realiza una tipología de accidentes con base en 2 grados de interacción y unión entre sus elementos; así, si existe un sistema socio-técnico complejo en sus interacciones y muy ajustado con respecto a la unión de sus elementos, éste debe ser abandonado debido a las múltiples e impredecibles formas de accidentes con consecuencias desastrosas. La teoría High Reliability Organization (HRO) está basada en estudios de organizaciones que manejan tecnología compleja de una forma satisfactoria a través de entrenamiento continuo, uso de redundancia, y numerosas fuentes directas de información. HRO sostiene que una organización consciente puede operar con base en la habilidad para estar al tanto de eventos inesperados sensibilizándose en sus operaciones, se siente comprometida con la resiliencia, y considera la pericia de expertos. Considera a los accidentes como una ruptura en el flujo e interpretación de la información así que pone especial énfasis en cómo los individuos y la organización la perciben y la usan. Un modelo basado en HRO considera como factores importantes en los accidentes a la interpretación errónea de la información, ambigüedades en la información, despreocupación por reglas e instrucciones y exceso de confianza y arrogancia en las organizaciones. Bajo la idea de HRO se han desarrollado modelos sistémicos, dos de ellos son el Functional Resonance Accident Model (FRAM) y el Systems-Theoretic Accident Model and Procceses (STAMP) (Hovden et al., 2010).

Chapman (2005) describe que son necesarios mejores modelos y marcos conceptuales que revelen la complejidad y hagan a los sistemas más transparentes, y un más satisfactorio enfoque a la administración del riesgo. Retoma la idea de Smallman (1995) en la que se recomienda un enfoque holístico que considere un continuo proceso de monitoreo de los peligros identificados, la predicción de escenarios de riesgo utilizando diversas técnicas, y una mejora en el aprendizaje organizacional. También afirma que modelos y marcos conceptuales son esenciales para el proceso de análisis de riesgos para revelar las fuentes de complejidad en sistemas socio-técnicos, y para reconocer las fases de desarrollo de un desastre.

En Manion & Evan (2002) se consideran como estrategias de prevención de desastres tecnológicos las siguientes:

- Conseguir con una mayor atención al potencial de desastres tecnológicos por parte de científicos e ingenieros, ya que varias restricciones organizacionales los desensibilizan: jerarquías organizativas rígidas, la prevalencia de la información clasificada y de propiedad, el

conflicto entre la necesidad de mejorar a corto plazo la rentabilidad de la empresa y el riesgo de pasar por alto un peligro de seguridad significativo.

- Lograr que ejecutivos de la empresa y especialistas en la administración de investigación se preocupen más respecto a la atención a la posibilidad de peligros y desastres. Para ello deberán de desarrollar códigos de conducta bien articulados y los mecanismos para asegurar que se lleven a cabo; por ejemplo auditorias sociales a la empresa para identificar los impactos de las acciones organizacionales antes de que se conviertan en desastres. Administradores de la agencia de gobierno deben de estar al día del creciente número de fallas tecnológicas, por no hablar de los desastres, que se producen anualmente.
- Contar un área más capacitada en cuestiones de tecnología en el gobierno que no esté limitada en cuanto a presupuesto y otras restricciones para hacer su labor.
- Fomentar una proactividad mayor de legisladores y oficiales del gobierno respecto a los riesgos y peligros de la tecnología moderna.
- La enseñanza de temas relacionados con las crisis tecnológicas, no sólo a científicos e ingenieros sino también a otros profesionales de diversas áreas.
- Contar con la participación de la ciudadanía para presionar a los tomadores de decisiones a actuar de forma más responsable y para encontrar a los responsables de catástrofes tecnológicas.

En Khodarahmi (2009) se apunta que la gestión de las crisis puede variar entre organizaciones o entre países por razones de cultura o normas en las que se encuentre inmerso; así las crisis generalmente derivan de objetivos fallidos y en tales casos necesitan ser redefinidos con el fin de recuperar la garantía y la confianza pública. Señala que el proceso para manejar la crisis debe ser planeado y estructurado, y que el rol esencial de quienes las gestionen es identificar y analizar las situaciones vulnerables a posibles crisis. Concuerda con la idea de que éstas inician por asuntos y problemas que crecen en el interior de las organizaciones y fuera de ellas, y refiere la idea en Wells (1978) de que una comunicación suficiente y una administración efectiva de la información es crucial (Ashcroft, 1997), pues el flujo esencial de información debe ser comunicado a los *stakeholders* relevantes en las situaciones de crisis. Independientemente del modelo que se use para la atención de crisis las principales acciones van enfocadas a encontrar una solución de la forma más eficaz y rápida. Otras ideas comunes sobre la administración de crisis que se reúnen en Khodarahmi (2009) son que la flexibilidad de la administración en la organización y la confiabilidad de la información son factores importantes, que tener planes efectivos de administración de crisis es esencial para facilitar la toma de decisiones, que relaciones con los medios y con la comunidad serán soporte para la organización en las situaciones de turbulencia, y que el entrenamiento o instrucción son indispensables para las estrategias.

En los párrafos anteriores se han expuesto distintas ideas acerca de las situaciones que pueden comprometer el desarrollo de las actividades esenciales de las organizaciones, sin embargo, no existe un consenso entre los distintos autores sobre la forma de denominarlas. Algunos ocupan el término de *Crisis* tal cual, otros ocupan el de *Desastre socio-técnico*, otros son más específicos y utilizan *Desastre*

de origen humano. De la misma forma son recurrentes los términos *Desastres tecnológicos* o simplemente *Accidentes en las organizaciones*. En lo que respecta a las causas de estas situaciones el panorama es un poco diferente ya que si bien no se tiene una opinión unánime en los documentos que hablan sobre esto, una gran cantidad de autores consideran que no hay una causa de un solo tipo y citan tanto fallas técnicas como deficiencias en cuestiones procedurales, de revisión o administrativas, así como el desempeño de las personas.

En este trabajo se ocupa el término compuesto *Crisis socio-técnica*. Se parte de la definición antes expuesta de Pearson y Clair en Pollard & Hotho (2006) de lo que es una crisis ya que indica claramente la importancia y las características esenciales que tienen los eventos de este tipo en las organizaciones y que establece de forma precisa que el evento desestabilizador se hace presente. Con el término socio-técnico pretendo incluir las ideas que afirman que el origen de estas situaciones implica un factor técnico pero también uno social debido a la interacción de componentes de tecnología con el comportamiento humano. A partir de se propone la siguiente definición de crisis socio-técnica en áreas de TIC:

> *"Aquellas crisis que tienen origen en la combinación de factores sociales y técnicos propios de las áreas de administración de TIC y que afectan de manera considerable su desempeño, así como el de los otros sistemas de la organización con las que están relacionadas, ya sean humanos, técnicos, administrativos, productivos o la combinación de éstos".*

2.2 Enfoques para la gestión y prevención de crisis

Turner (1976) fue el primero que utilizó el término de *incubación* en 1976 para referirse a la acumulación de una serie de eventos desapercibidos con la creencia aceptada de su peligro y las normas de su evasión. Esta característica es parte esencial de la *fase precursora* de las crisis en los modelos elaborados al respecto. En 1986 se presentó el modelo de 4 fases de Fink y se introdujo el concepto de *Pródromo* para identificar a las señales de advertencia de las fase pre-crisis con lo que se apuntó la importancia de que actuar en respuesta al pródromo determina la supervivencia de la organización a una crisis (Jaques, 2010). Las otras 3 fases del modelo de Fink son: *Agudeza de la crisis*, *Crisis crónica* y *Resolución*.

2.2.1 Modelo relacional de administración de crisis

En Jaques (2007) se presenta una concepción de gestión de desastres en donde los diferentes elementos que lo componen pueden ser trabajados simultáneamente en cierto grado para atender las situaciones que se presentan y que no son una serie de eventos que inician y paran con cada ocurrencia de un desastre como se muestra en la figura 2.1. Sin embargo hace la aclaración que no es propiamente

una propuesta para la gestión de crisis pues involucra la participación del gobierno o autoridades territoriales para la atención de desastres comunitarios o nacionales, pero que sin embargo es un buen marco de referencia por vislumbrar sus elementos como procesos vinculados y no como disciplinas independientes.

Figura 2.1. Ciclo de gestión de desastres. Adaptada de Jaques (2007).

Dicho autor denomina a su propuesta *Modelo relacional de gestión de crisis*, y toma como base una disciplina continua basada en grupos o *clusters* y en elementos no lineales para tratar la crisis de una manera holística. Precisa que los elementos del modelo deberán ser vistos como *clusters* de disciplinas relacionadas y no como pasos a ser tomados de forma secuencial; así los elementos individuales pueden ocurrir en cualquier momento e incluso simultáneamente. Con la figura 2.2, que representa este modelo, explica que los elementos adyacentes se pueden superponer cuando se ejecutan las acciones del modelo pero que también actividades de clusters no adyacentes pueden ejecutarse de manera simultánea y no dependiente, como por ejemplo la *detección temprana* y el *reconocimiento de una crisis*. Y que también, los aprendizajes posteriores a la crisis de una organización pueden proporcionar una alerta temprana y una mejor preparación ante las crisis para otras organizaciones.

Figura 2.2. Modelo relacional de gestión de crisis. Adaptada de Jaques (2007).

2.2.2 Gestión de problemas para la prevención de crisis

Jaques (2010) resalta la importancia de la idea de crisis como un proceso y no como un evento, y se enfoca en la descripción del periodo de incubación de crisis. Propone un modelo integrado de preparación y prevención de crisis que se compone de una etapa de advertencia temprana, una de administración de riesgos y de situaciones problemáticas, y otra respuesta de emergencia. Las 2 primeras se enfocan en la gestión de problemas, entendida como los intentos para minimizar las sorpresas que acompañan a los cambios sociales y políticos. Afirma que la atención de problemas desde el enfoque de prevención de crisis no ha evolucionado tanto como en la emergencia ante crisis o la gestión post-crisis pero concuerda con la idea de que quienes estén a cargo deberían tomar medidas preventivas al inicio del ciclo de crisis, y afirma que el concepto de gestión de problemas para la prevención de crisis puede ser muy útil al desarrollar cuatro áreas en particular:

a) Direccionamiento proactivo a causas sistémicas subyacentes de crisis potenciales. Las causas sistémicas de las crisis pueden ir más allá de riesgos específicos de la industria: comportamiento

incompetente, discriminación sexual, racial, deshonestidad, tecnología, e incluso áreas tabú de discusión; y por lo tanto es necesario ir más allá de los riesgos sistémicos obvios en cada industria. Otros retos en esta área son eliminar la interrupción del flujo de información importante hacia los altos ejecutivos de las organizaciones por administradores intermedios que no permiten críticas, y facilitar la traducción de información en acciones mediante una perspectiva amplia de la situación.

b) Establecimiento de mecanismos efectivos de detección de señales. En muchas ocasiones las señales de advertencia de problemas son ignoradas porque se da poca importancia a actividades periféricas al negocio de la organización, sin embargo, esta detección debe ser en sí un proceso principal por su relación con muchos sistemas de información, procedimientos de planificación y técnicas de toma de decisiones.
c) Identificación adecuada de *stakeholders* y sus perspectivas. Considera que un inadecuado entendimiento del potencial de los stakeholders es una seria falla, particularmente en relación al rol y respuesta de los oponentes incluyendo organizaciones no gubernamentales y activistas sociales y políticos.
d) Aprendizaje y *desaprendizaje* de forma continua. Es necesario una honesta evaluación de lo que ha sucedido en el pasado, y aprender de los disidentes y críticos de la forma de administración de la organización. La gestión de problemas implica el aprendizaje de las crisis que experimentan los otros y de las simulaciones de crisis que evidencia resultados desfavorecedores.

Con este enfoque de gestión de problemas Jaques presenta un marco para un efectivo proceso de prevención que requiere la capacidad de registrar lo que sucede en el ambiente, de reunir información, medirla y evaluarla, así como del diseño de una interfaz para transformarla en acciones pertinentes. De esta forma apoya la idea de que la prevención es inherentemente un proceso político y no esencialmente técnica (Tombs & Smith, 1995).

2.2.3 Resiliencia en las fases de prevención de crisis

En Hernantes, Rich, Laugé, Labaka, & Sarriegi (2013) se maneja el concepto de Infraestructura Crítica, *IC*, que es aquella de cuyo funcionamiento depende el bienestar de la sociedad (sistemas de energía, agua, transporte y telecomunicaciones, por ejemplo). Cuando algún elemento de la IC es afectada por una crisis se buscan estrategias proactivas y reactivas para mejorar la resiliencia cuando la planeación es inadecuada. Estos autores refieren que la administración de crisis requiere la cooperación de un conjunto diverso de stakeholders que inicialmente tienen diferentes perspectivas, de la ejecución de una serie de actividades de forma simultánea en una manera coherente, además de la necesidad de aprender de las crisis propias y de las de otros. En este sentido, afirman que el éxito o falla de una respuesta está basado en el desarrollo de las relaciones, recursos, información y procedimientos durante la fase de preparación.

Tanto el concepto de Infraestructura Crítica y las actividades de preparación para enfrentar una crisis se pueden trasladar al dominio de crisis socio-técnicas al interior de las organizaciones, y en consecuencia se hace necesario identificar las áreas esenciales de negocio y generar mecanismos para prevenirlas o posibilitar la resiliencia en caso de no poder evitarlas.

Durante las crisis en las IC se presentan 4 tipos de problemas (Hernantes et al., 2013) :

a) Heterogeneidad. Los sistemas que necesitan apoyarse tienen fallas en sus relaciones o medios de interacción ya que los planes ante crisis se elaboran por lo general con una perspectiva interna, y no contemplan la importancia de las relaciones y sinergias entre otros subsistemas o los sistemas de su ambiente. De esta forma se presentan problemas particulares de lenguaje, entendimiento y efectos colaterales.
b) Límites múltiples e inconsistentes. La interrelación a través de los límites entre infraestructuras críticas posibilita un efecto de cascada cuando se presenta una crisis en alguna de ellas; estos límites pueden ser geográficos, físicos, políticos, culturales o legales, por mencionar algunos tipos. Otro límite de importancia es el tiempo, ya que retrasos o adelantos en alguna actividad estructural pueden alterar alguna IC relacionada. Cuando se toman decisiones con base en tiempos ajustados se pueden generar efectos no deseados en el ambiente del sistema; esto va de la mano con la toma de decisiones considerando sólo consecuencias inmediatas, siendo que lo recomendable es que los administradores de crisis deben adoptar y actuar conforme a una perspectiva estratégica y enfocarse en consecuencias a largo plazo. De manera relacionada, quienes se orientan por la dinámica de sistemas buscan identificar acciones y reacciones dentro de los límites del sistema e incluso fuera mediante elementos probabilísticos y análisis de sensibilidad.
c) Diversidad de actividades para construcción de resiliencia. Hacen notar que es difícil realizar actividades de planeación para alcanzar la resiliencia del sistema afectado y definir métricas claras de éxito ya que esta sólo se puede evaluar cuando una crisis es evitada. Proponen llevar el concepto de resiliencia más allá de su significado y presentan la idea de Bruneau de que ésta puede incluir actividades proactivas que apoyen a la prevención de fallas y con ellos la crisis. Cuando los límites del sistema se extienden la resiliencia es más compleja; sin embargo es necesario plantear actividades que permitan incrementar la resiliencia del sistema, por ejemplo: Infraestructura adecuada y redundancia, entrenamiento interno y externo, definición clara de regulaciones y documentación de lecciones aprendidas.
d) Compartir y transferir el conocimiento. Es necesario el desarrollo de una cultura para compartir el conocimiento que sea capaz de atravesar los límites organizacionales, sustentada por intereses comunes y confianza inter-organizacional. Es necesario generar bases de datos de conocimiento ganado a través de crisis, emergencias o eventos simples, teniendo en cuenta que no sólo se trata de reunir datos técnicos o identificar responsabilidades, sino también analizar situaciones humanas y organizacionales que los precedieron.

Para estas tareas se propone el uso de 2 técnicas complementarias que buscan atender los puntos de importancia ya mencionados. La primera de ellas es el *Group Model Building* (GMB), una metodología colaborativa en la que expertos con distintas formaciones reflexionan sobre algún tema para definir causas endógenas de un problema y generar una percepción compartida. Los talleres donde se generan el conocimiento se llevan a cabo siguiendo scripts preparados previamente pero con la flexibilidad necesaria para adaptarse según se desarrollen las sesiones. La otra técnica se refiere a modelos de simulación (Dinámica de Sistemas) para identificar áreas de interés para mejorar decisiones estratégicas, cuyas entradas provienen de haber consolidado el conocimiento que inicialmente estaba fragmentado a través de actividades del GMB (Hernantes et al., 2013).

2.2.4 Aprendizaje organizacional en el proceso de prevención y preparación para crisis socio-técnicas

En Carmeli & Schaubroeck (2008) se apoya la idea de que no hay un modelo exhaustivo que indique cómo deben prepararse las organizaciones para las crisis y se sostiene que lo que hace a una organización estar preparada para una crisis es concientizarse y vigilar su fuerza de trabajo de tal forma que se puedan identificar eventos desencadenates y se les pueda informar a los tomadores de decisiones. Como parte de la preparación a crisis es necesario que los líderes, administradores o tomadores de decisiones tengan conciencia del riesgo de futuras crisis para institucionalizar practicas y regulaciones industriales que resulten en actividades de preparación. Dichos autores indican que la administración de crisis debe cubrir actividades que partan de la estructura organizacional, cultura y políticas; en ese mismo sentido, Ian Mitroff afirma en varias de sus publicaciones (Alpaslan et al., 2009; I. I. Mitroff & Anagnos, 2000; I. I. Mitroff, 2004; Pearson, Misra, Clair, & Mitroff, 1997) que la cultura organizacional es uno de los principales factores que determinan cómo se responderá a una situación de crisis. También citan a Watkins & Bazerman (2003), quienes consideran tres tipos vulnerabilidades relacionadas con las situaciones de crisis:

- Psicosociales. Defectos cognitivos que imposibilitan reconocer amenazas próximas.
- Organizacionales. Barreras al interior de las entidades que impiden la comunicación y/o diluyen la responsabilidad.
- Políticas. Deficiencias en los mecanismos de toma de decisiones.

Indican que el proceso de prevención y preparación para crisis sociotécnicas puede requerir acciones más profundas que el monitoreo del desempeño, como por ejemplo mejorar o adquirir nuevos comportamientos en la organización e incluso olvidar (*desaprender*) algunos modos de pensamiento en favor de nuevos. Así, precisan que el aprendizaje en la organización es parte esencial en la preparación para crisis, y para definirlo citan a Edmonson & Moingeon (1999): *"Grado en el cual los miembros de un particular negocio usan activamente datos para guiar el comportamiento a fin de aumentar la adaptabilidad"*. Observan las dos formas de aprendizaje propuestas en Argyris & Schön

(1978): aprendizaje de un solo bucle (*single-loop*) y de dos bucles (double-loop). El primero se presenta cuando el sistema reconoce errores y sólo los corrige, asegurando la continuidad de operaciones, pero no busca ni atiende las causas que originaron esa falla para evitar que se vuelvan a presentar, como se haría con el aprendizaje de doble bucle. Esta *solución de problemas de segundo orden*, correspondiente al aprendizaje de doble bucle es la que señalan se debe llevar a cabo en el proceso de preparación para crisis.

También en Carmeli & Schaubroeck (2008) se describe un interesante estudio que involucró información útil de 106 compañías de sectores de agricultura, química, comida, papel, impresiones, electrónicos, software, textiles y farmaceúticos, de las cuales el 25% son industrias de alta tecnología, y el 40% son de mediana tecnología. Como variable dependiente se definió la preparación para crisis en dos sentidos: una preparación presente para crisis, que se explica como la habilidad para manejar crisis inmediatas, y una preparación prospectiva para crisis, que se refiere a la capacidad para enfrentar crisis en un futuro distante. La variable independiente que se observó fue el comportamiento de aprendizaje de fallas desde una perspectiva de solución de problemas de segundo orden (doble loop); y la variable de control fue el desempeño que se percibió de la organización, debido a que se tiene la creencia común de que las entidades con alto desempeño son menos vulnerables a las situaciones de crisis. Se concluyó que existe una positiva asociación entre el aprendizaje de las fallas y la preparación presente y prospectiva de las organizaciones para situaciones de crisis, con lo que se indica que las organizaciones que adoptan una solución de problemas de segundo orden son más proactivas en los preparativos para situaciones de crisis.

Algo más a tener en cuenta es que si en las situaciones de crisis no se tiene una adecuada preparación para hacerles frente, es posible que las respuestas que se den las empeoren. Otro inconveniente común que se presenta en las organizaciones es el aprendizaje sobre aspectos particulares de las fallas, ya que al intentar aplicar las lecciones aprendidas en nuevos escenarios de crisis se pueden generar resultados contraproducentes porque las condiciones no son exactamente las mismas a las que se presentaron en la ocasión anterior. En este sentido es necesario aprender lecciones generales, es decir, los principios más amplios de las circunstancias y no aspectos específicos de la crisis. El proceso de preparación para crisis es complejo debido a que depende de muchos factores, la preparación de los administradores o gerentes es importante, pero también es necesaria una capacitación colectiva de quienes se verán afectados por las situaciones de crisis, con un ánimo de responsabilidad común (Carmeli & Schaubroeck, 2008).

2.2.5 Modelos de reacción en cadena y de sistemas de control (Tarn et al., 2008)

En Tarn et al. (2008) se propone un modelo que se enfoca en 3 principales fases del ciclo del desastre: *Quiesciente*, *Pródromo* y *Desastre*. Para las 2 primeras propone auxiliarse de sistemas de información para predecir calamidades potenciales, advertir a una autoridad de administración de control de lo que se está desarrollando e incluso responder a las circunstancias que superan las capacidades de reacción del ser humano. Las otras 2 etapas de este ciclo que consideran los autores también son *Rescate* y *Recuperación*.

Sustentados en la revisión de distintos tipos de desastres socio-técnicos identifican factores comunes, que caracterizan en los dominios humano y técnico. Los factores humanos que citan son:

- Económicos. Cambios en la operación debidos a ajustes económicos
- Entrenamiento. Deficiencias en la instrucción o falta total de entrenamiento para personal de operaciones.
- Procesales. Cambios en procedimientos operacionales que ahorran tiempo y dinero pero que comprometen pasos críticos en la detección o información de emergencias.
- Complacencia operativa. Falta de atención debido al aburrimiento o pérdida de interés.
- Deficiencia en la construcción. Violación de diseños o estándares con el fin de ahorrar dinero o tiempo.

Con respecto al dominio técnico los factores que identifican son:

- Fallas en el diseño del sistema.
- Fallas en la operación del equipo. Operación del equipo de forma diferente a las especificaciones.

Dichos factores ocasionan una ruta de desastre común en estas situaciones. Este modelo de reacción en cadena (figura 2.3), puede utilizarse para el diseño de sistemas de control de crisis sociotécnicas. En este modelo, los puntos en la fase quiesciente representan los eventos que pueden permitir la falla de los componentes de los sistemas; si éstos superan los mecanismos humano-máquina de prevención, protección o supervisión alcanzan la fase pródromal donde se acumulan en *clusters* y empiezan a interactuar generando reacciones en cadena. Cuando un evento crítico es lanzado por uno o más *clusters* puede desencadenar una serie de fallas críticas que ocasionan el desastre.

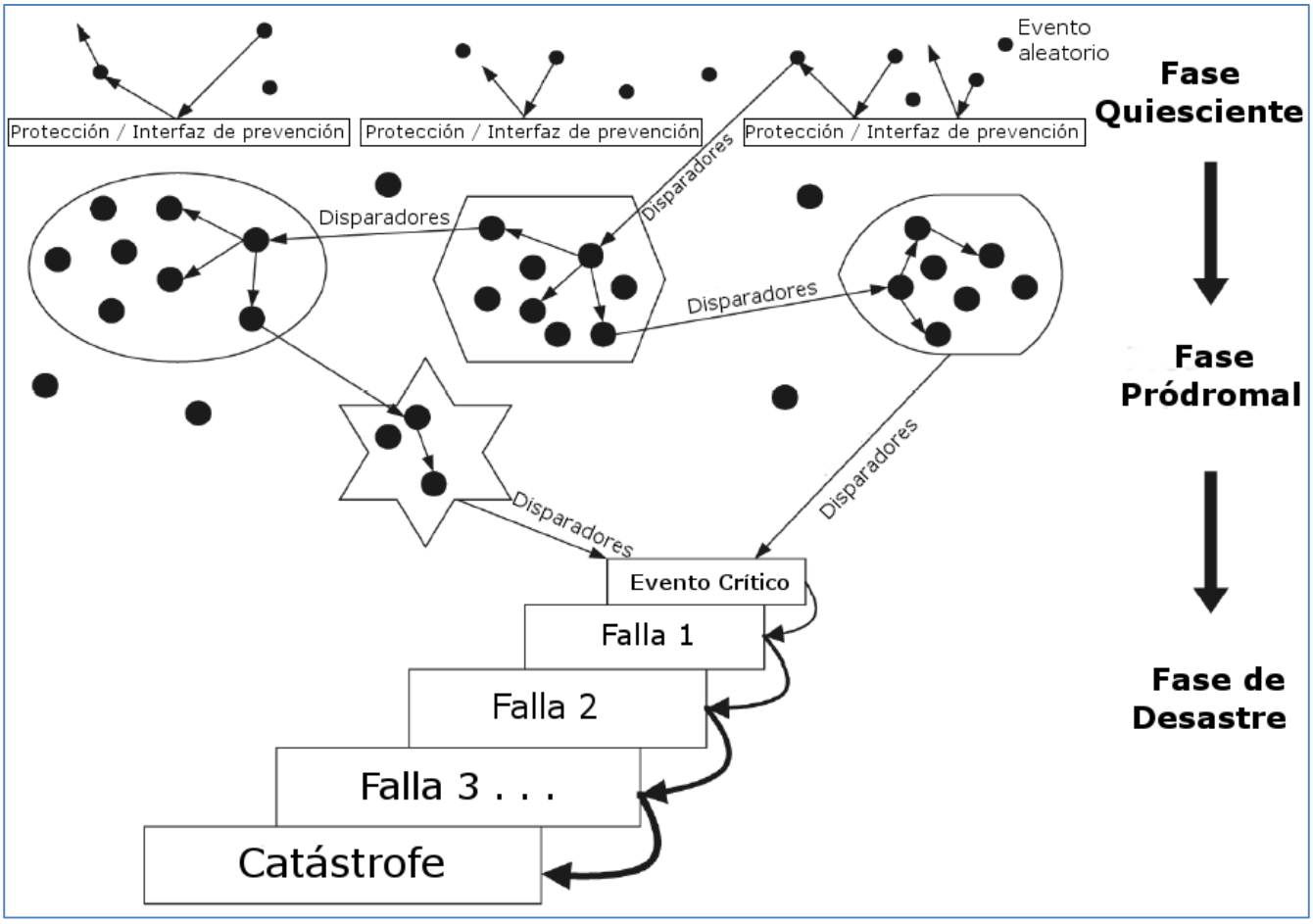


Figura 2.3. Modelo de reacción en cadena. Adaptada de Tarn et al. (2008).

Otra de las principales propuestas de los autores mencionados es que existen vacíos en los sistemas de control, uno extrínseco entre el humano y las capacidades de las máquinas, respuestas e interfaces debido a que idealmente debe ser familiar con todo el sistema y sus operaciones; y un vacío intrínseco entre los procesos de control y la construcción del sistema. Para llenar tales huecos, proponen el uso de tecnología que englobe el conocimiento colectivo de los diseñadores del sistema, de los ingenieros de seguridad, de los ingenieros de mantenimiento y los operadores. Con el mismo objetivo presentan un modelo para el diseño que pretende mejorar los sistemas de control de contingencias convencionales. Se plantea que los sistemas deben ser capaces de analizar los escenarios que se presentan mientras se procesa el flujo de datos e información en tiempo real, y que debe considerar interfaces de control internas y externas, además de monitorear a través de un loop de control y proporcionar soluciones a los problemas exteriores. Los componentes de este modelo son:

a) Un subsistema de administración y de operación, que lleva a cabo toma de decisiones por medio de un *loop* cibernético humano-maquina.
b) Un subsistema de monitoreo que realice funciones de detección de advertencias. Debe contemplar un mecanismo de registro para obtener datos duros desde puntos de control del

sistema mientras que componentes inteligentes de monitoreo obtienen datos suaves desde dentro o fuera de la organización. Debe ser capaz de detectar fluctuaciones en las operaciones normales y reportar esta actividad a un colector de información de un *Sistema de procesamiento de conocimiento* que determine el estado de todo el sistema. Este sistema de procesamiento de información puede ser humano, combinación humano-máquina o puramente máquina, y la información que genere puede dirigirse a un *modelo de bases catastróficas* que indique acciones con correcciones sugeridas y las instrucciones necesarias con base en estructuras de escenario predefinidas, o que en caso de no poder asignar a un caso predeterminado pase el control a un *Sistema de control de decisión inteligente*. Éste puede englobar como elementos de control a personas y a tecnología, y puede sugerir transitar el estado del sistema de una orientación pasiva a activa en 4 niveles:

1. Indicar alertas o advertencias iniciales para llamar la atención del operador a problemas potenciales.
2. Proporcionar sugerencias y advertencias que deben ser tomadas para evitar problemas.
3. Tomar un control parcial de la operación mediante el establecimiento y la vigilancia de los requisitos de control que se deben cumplir para el funcionamiento continuo del sistema o mediante la validación de la conclusión de una alternativa de decisión. Las acciones no se llevan a cabo hasta que el operador confirme la opción propuesta por el sistema.
4. Tomar por completo el control del sistema, excluyendo la intervención humana, de acuerdo con un procedimiento preprogramado, con el fin de evitar un camino catastrófico.

Como elementos de realimentación considera el envío de información a los sistemas de operación y administración y al sistema de control. Esta propuesta de diseño para sistemas de control se ejemplifica en la figura 2.4.

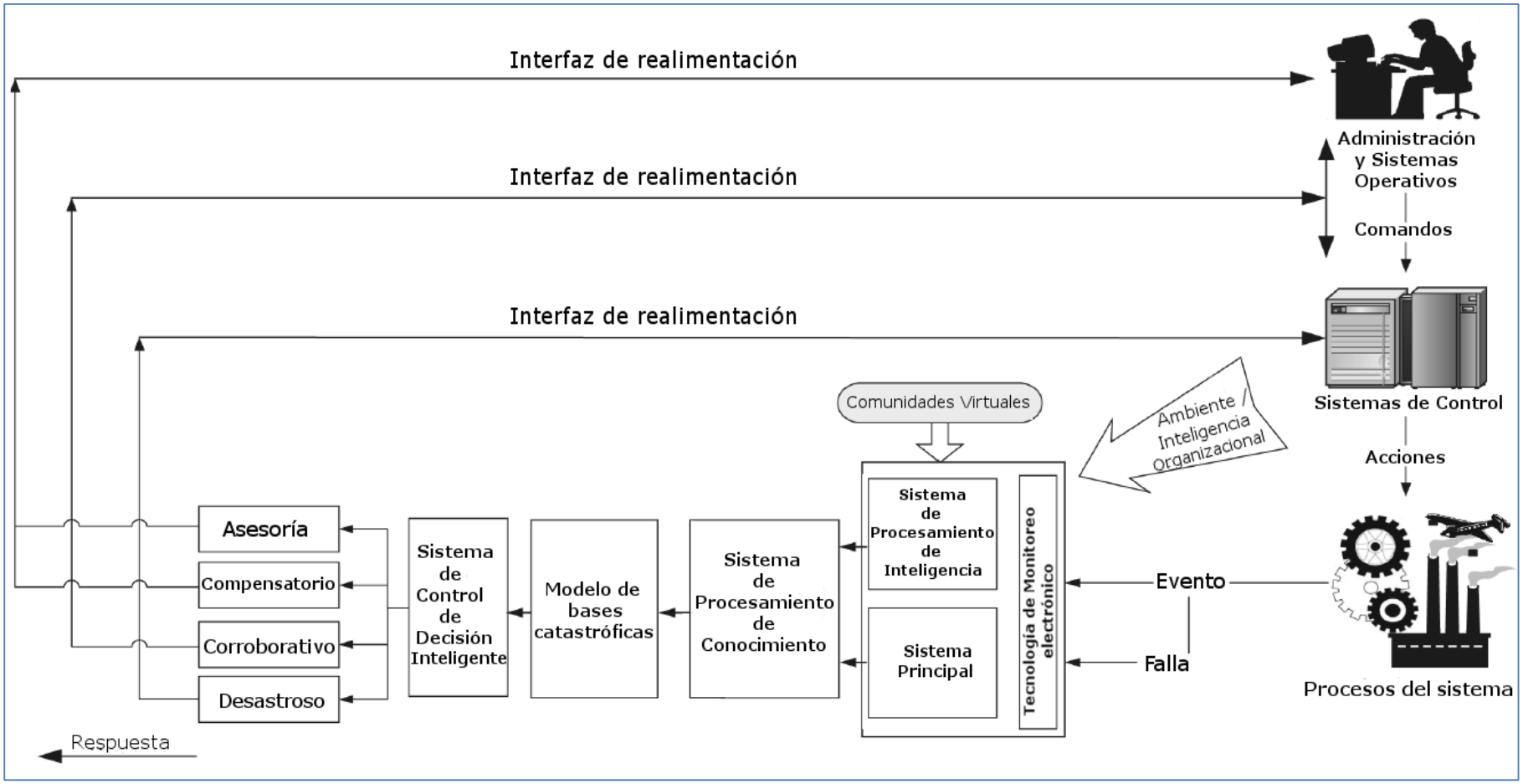


Figura 2.4. Modelo para el diseño de sistemas de control. Adaptada de Tarn et al. (2008).

2.2.6 Comparación de modelos para gestión de crisis socio-técnicas

En Ibrahim M. Shaluf et al. (2002) se presenta el modelo de Ibrahim-Razi para la fase de precondición de desastres tecnológicos causados por el hombre (Figura 2.5) que se enfoca en el origen y precondiciones. Dicha propuesta se conforma por las siguientes fases:

Fase 1. Generación de errores. Tiene lugar en la organización en etapas tempranas. En particular en el diseño de etapas procesales, políticas de operación y procedimientos ambiguos.

Fase 2. Acumulación de errores. Generación de errores operacionales y acumulación junto con errores organizacionales y técnicos. Como consecuencia se tiene la falta de continuidad del personal de la organización, falta de comunicación entre la parte operativa y la administración, así como la falta de compromiso de esta última.

Fase 3. Advertencia. Revisiones y auditorias periódicas que examinen las actividades de la organización para hacer recomendaciones que sirvan como señales de advertencia a la administración. En ciertos escenarios los errores acumulados aparecen en la organización como cuasi accidentes, incidentes y accidentes.

Fase 4. Correcciones. Si las advertencias son reconocidas y corregidas, la organización retomará los procesos de operación seguros y normales.

Fase 5. Condiciones inseguras. Cuando los errores se acumulan y las señales no son identificadas o atendidas, la organización operará bajo condiciones inseguras y entrará en una fase de desastre inminente.

Fase 6. Evento desencadenante. Cuando un acto inseguro en la forma de un error, falta y/o violación de reglas de los procedimientos suceda, se desencadenará el desastre.

Fase 7. Defensas. La organización entra en un estado de emergencia. Las condiciones de emergencia son controladas si los planes de emergencia, respuestas de emergencia y soporte externo son disponibles y efectivos.

Fase 8. Desastre. Pérdida de personal, propiedad e impactos ambientales.

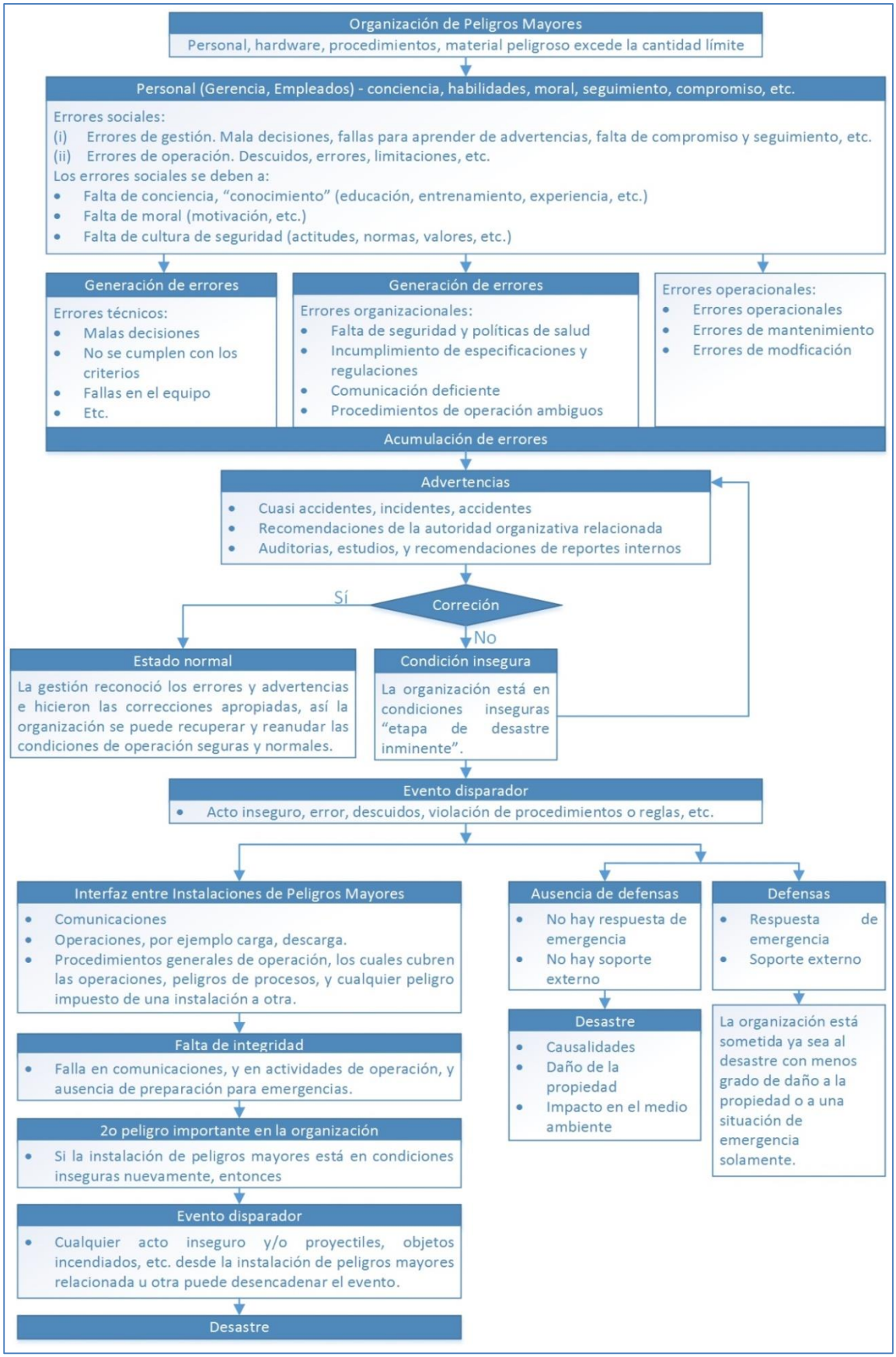


Figura 2.5. Fase de precondición de desastres tecnológicos causados por el hombre (Ibrahim M. Shaluf et al., 2002).

En Aini & Fakhrul-Razi (2010) se observa que Turner identificó en sus estudios un periodo de incubación donde existen precondiciones para las fallas y se citan resultados de estudios de desastres de origen humano en las organizaciones en los que se afirma que éstos se pueden considerar como un ciclo que puede ser dividido en 3 periodos:

I. Periodo Pre-desastre.
    a. Fase de operación. Punto inicial donde el sistema socio-técnico inicia su operación.
    b. Fase de incubación. Periodo en el que se incuban errores en el sistema hasta que desencadenan eventos que generan el desastre. Se compone una fase de preaviso donde se presentan señales de que algo no está bien o es inaceptable, y que por lo general son malinterpretadas o menospreciadas.
    c. Fase de activación. Se refiere a la causa inmediata que genera o desencadena el o los desastres.

II. Periodo de Desastre
    a. El inicio del desastre
    b. Fase de respuesta y de recuperación. Es necesaria una respuesta inmediata y contar con los recursos, materiales y condiciones adecuadas.

III. Periodo Post-Desastre. Periodo posterior a las operaciones de búsqueda y rescate.
    a. Investigación y elaboración de informes
    b. Realimentación. Considera la recepción e implantación de las recomendaciones resultado de la investigación que son importantes a la organización.
    c. Búsqueda de justicia social. La posibilidad que se da a la sociedad civil afectada de tomar acciones contra los responsables del desastre.
    d. Reformas sociales y legislativas internas y externas, basadas en los resultados de las investigaciones.

Las etapas descritas en este modelo del desarrollo de las crisis socio-técnicos coinciden con otras posturas que tienen el mismo objeto de estudio. Una tabla comparativa es la 2.1 (Aini & Fakhrul-Razi, 2010).

Periodo	Modelo de sistemas causados por el hombre de Turner	Modelo de crisis industriales de Shirivastaba	Fallo de los sistemas y el modelo de reajuste culturales de Toft y Reynolds	Modelos de fase de precondición de Ibrahim-Razi	Modelo de desastres socio-técnicos de Aini-Razi
Pre-Desastre	I. Punto de inicio de operaciones	I. Condiciones pre-crisis	1. Incubación	1. Generación de errores	I. Operación
			2. El sistema operacional socio-técnico	2. Acumulación de errores	II. Incubación
	II. Incubación	II. Evento desencadenante		3. Advertencia	
				4. Corrección	III. Advertencia
			3. Evento precipitante	5. Condiciones inseguras	IV. Activación
				6. Evento desencadenante	
Desastre	III. Inicio	III. Extensión de la crisis	4. Desastre	8. Desastre	V. Inicio
	IV. Rescate y salvamento		5. Rescate y salvamento		VI. Rescate y recuperación
Post-Desastre	VI. Ajuste cultural	IV. Resolución de crisis	6. Investigación y reportes		VII. Investigación y elaboración de reportes
					VIII. Realimentación
			7. Realimentación		IX. Justicia social
					X. Reformas sociales y legislativas

Tabla 2.1 Distintos modelos de atención a desastres socio-técnicos. Adaptada de Aini & Fakhrul-Razi (2010).

Desde los primeros trabajos realizados por Turner en la década de 1970 hasta la actualidad se reconoce que es primordial realizar actividades antes de se presenten las crisis socio-técnicas (Carmeli & Schaubroeck, 2008; Hernantes et al., 2013; Jaques, 2010; Ibrahim M. Shaluf et al., 2002; Ibrahim Mohamed Shaluf, 2007; Tarn et al., 2008; Turner, 1976). Sin embargo la mayoría de los estudios al respecto se enfocan en las fases de desarrollo y de recuperación, y quedan en segundo término las actividades de prevención según se afirma en (Jaques, 2010).

En este sentido es muy importante considerar que las crisis se desarrollan como un proceso (Jaques, 2010) y no como un evento aislado. De esta forma es posible caracterizar dicho proceso y separarlo en fases para su análisis como se ha realizado por distintos investigadores. Entre los beneficios de esto se encuentra la posibilidad de identificar de forma general las etapas de una crisis y con base en ello proponer procedimientos, técnicas y/o herramientas para atender la prioridad que se presenta en cada una, ya sea para mitigar, recuperar un estado estable e incluso prevenir.

2.3 Enfoques para la construcción y validación del Sistema de Planeación

En esta sección se describen brevemente los enfoques de planeación que se ocupan como directriz para generar el *Sistema de Planeación para la prevención de crisis socio-técnicas en áreas de TIC*, algunos de los cuales también se proponen como base para los planes que pretende se generen.

2.3.1 Proceso de Planeación como apoyo en la conducción (Gelman & Negroe, 1982)

En Gelman & Negroe (1982) se describe un Sistema de Planeación cuyo objetivo es ayudar en el proceso de conducción que llevan a cabo organismos de administración pública y privada para conseguir sus objetivos. Este proceso de conducción equivale al concepto *management* del idioma inglés, el cual se refiere a "*actividades de regulación, gobernación, manejo, administración, control, gerencia, conducción, dirección, mando, guía y los verbos timonear y regir*", y que son actividades que un objeto conducente lleva a cabo sobre un objeto conducido.

Además de valerse del *Sistema de la Planeación*, el sistema conducente se integra por un *Sistema de Toma de decisiones* cuyas actividades se llevan a cabo, por un lado, pensando en el presente y en el corto plazo, y por otro se orientan hacia la construcción de objetivos y su logro en un largo plazo como parte de una solución integral en la que precisamente ocupa el proceso de conducción. Ocupa también un sistema denominado *Información* con el que obtiene datos del objeto conducido y de otros sistemas relacionados y además genera, selecciona, transmite, procesa y presenta información. Un tercer elemento que lleva a cabo el sistema conducente es la *Ejecución* de acciones como resultado del proceso de toma de decisiones. En la figura 2.6 se representan la relación del sistema conducido con el sistema conducente y los componentes de los que se vale este último para conseguir sus objetivos.

El Sistema de Planeación es el encargado de proporcionar al tomador de decisiones conocimiento e información necesaria. Se integra por los cuatro elementos de la figura 2.7 y descritos a continuación.

1. Subsistema Planeación. Sus objetivos son producir planes (objetivos, políticas, metas, programas y proyectos).
2. Subsistema Implantación. Se divide en 2 aspectos: a) Planeación de la ejecución, cuyas actividades se llevan a cabo en el Sistema de Planeación; y b) Ejecución, que corresponde propiamente al *Sistema de Ejecución*.
3. Subsistema Evaluación. Evalúa la eficiencia de la ejecución de los planes generados por el Subsistema de Planeación.
4. Subsistema Adaptación. Con base en la información del Subsistema de Evaluación realiza ajustes, cambios y adaptaciones para mejorar el proceso de planeación y el de conducción.

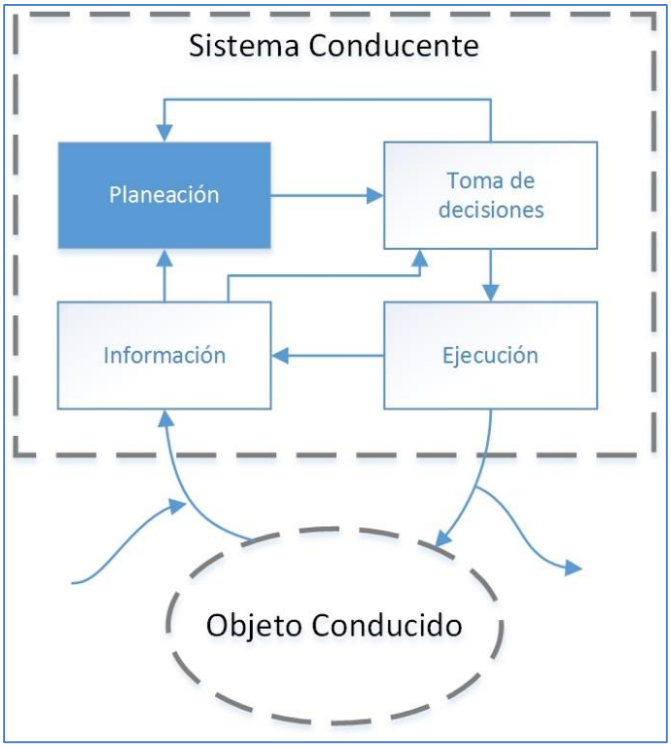


Figura 2.6. Relación entre el Sistema Conducente y el Objeto Conducido. Adaptada de Gelman & Negroe (1982).

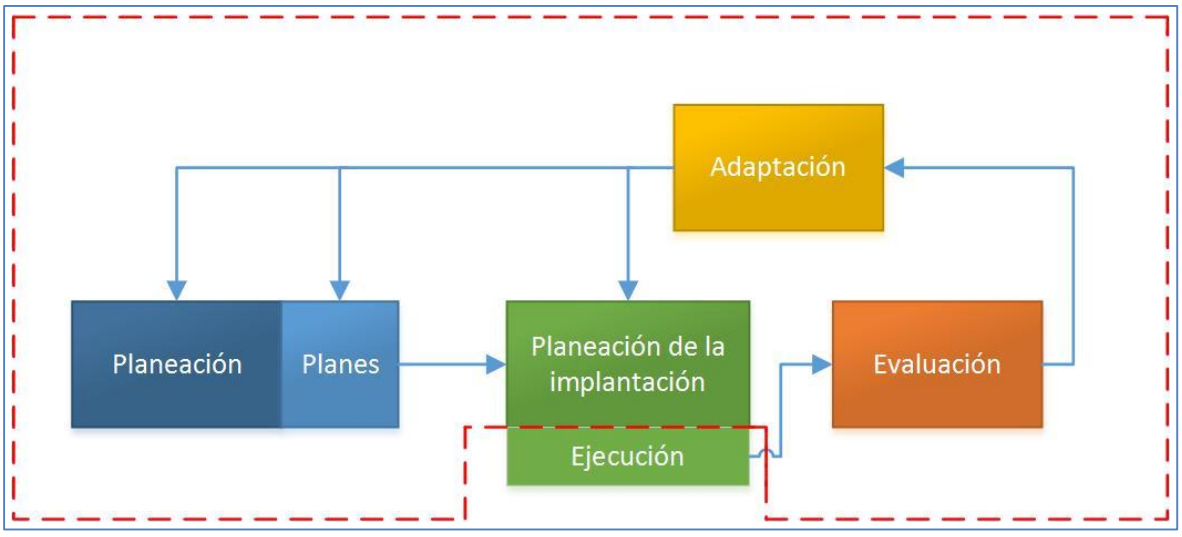


Figura 2.7. Estructura del Sistema de Planeación. Adaptada de Gelman & Negroe (1982).

Este *Subsistema Planeación* se ocupó como guía para las etapas esenciales del Proceso de Planeación para esta tesis; sus componentes se describen a continuación:

- Diagnóstico. Su objetivo es detectar, definir y plantear los problemas a resolver que se presentan por las relaciones entre el sistema conducente y el conducido, del objeto conducido

y su suprasistema, y del sistema conducente con su suprasistema. Los elementos que componen esta etapa se listan en la figura 2.8.

- Prescripción. Sus actividades están encaminadas a dar solución al problema planteado mediante la formulación de modelos, la definición de restricciones y formulación de criterios, la búsqueda de soluciones, y la evaluación de alternativas mediante técnicas de optimización y modelado. En la figura 2.9 se enuncian las acciones que integran esta etapa.
- Instrumentación de la solución. Tiene como propósito formular los objetivos a lograr, y elaborar las políticas y los programas tomando en cuenta los recursos con los que se cuenta. La figura 2.10 presenta los subcomponentes de esta etapa.

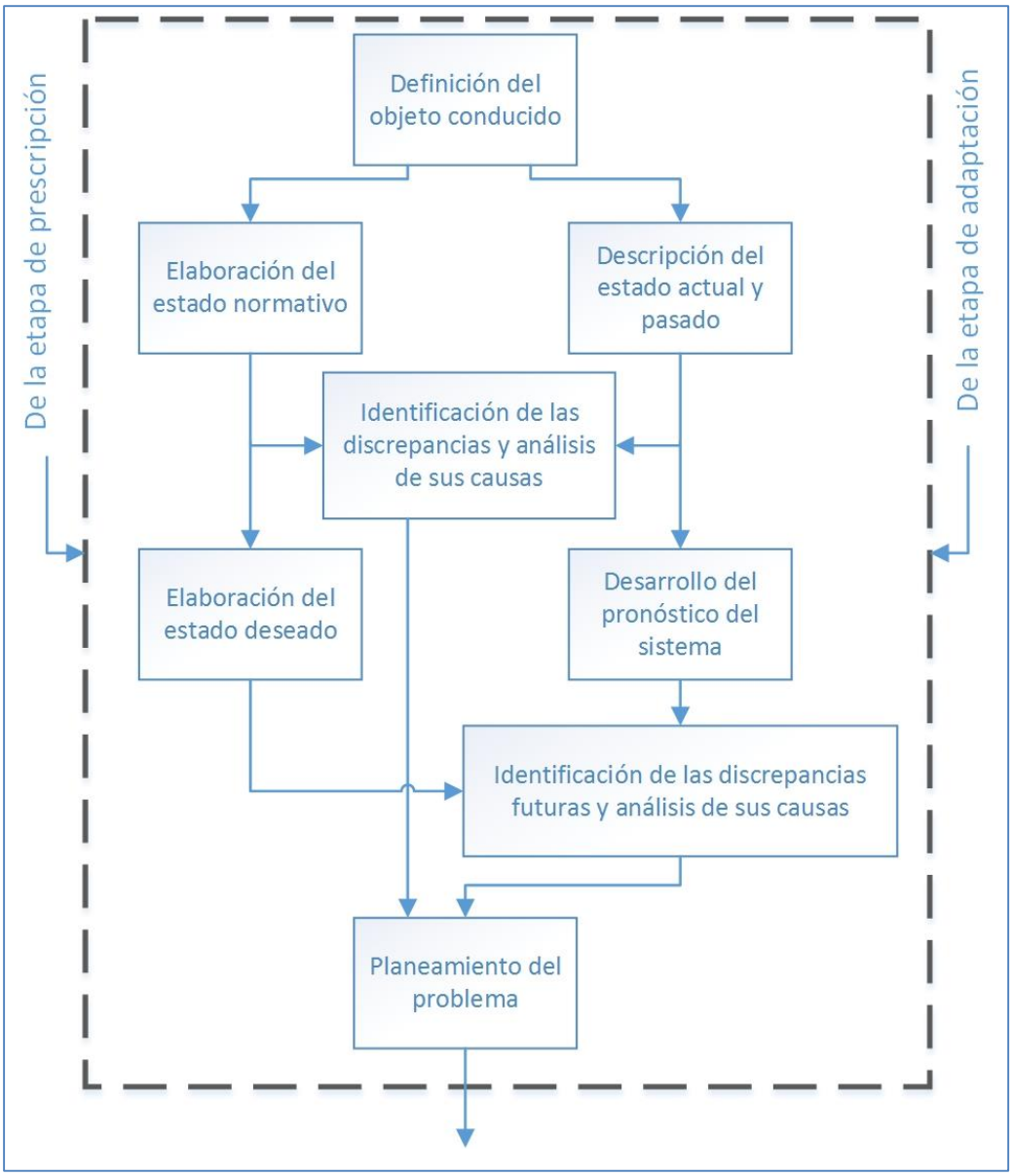


Figura 2.8. Etapa de Diagnóstico del Subsistema de Planeación. Adaptada de Gelman & Negroe (1982).

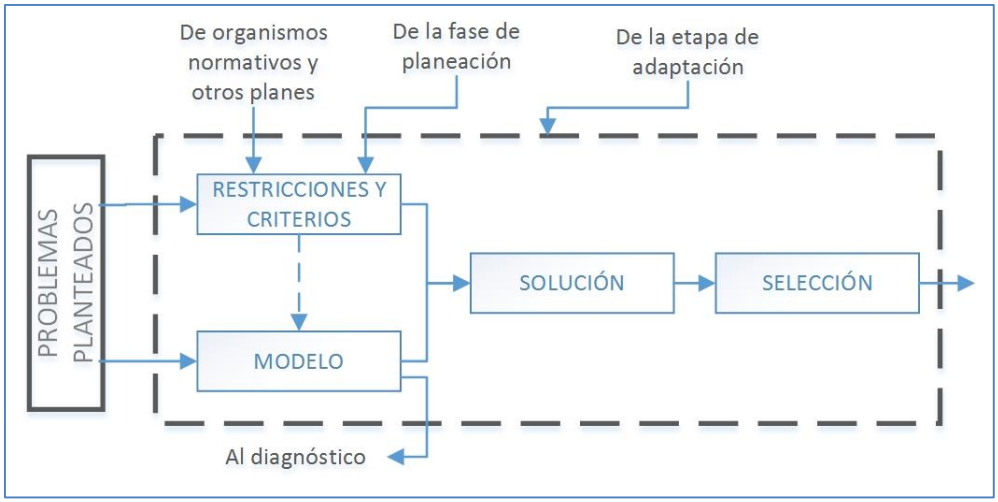


Figura 2.9. Etapa de Prescripción del Subsistema de Planeación. Adaptada de Gelman & Negroe (1982).

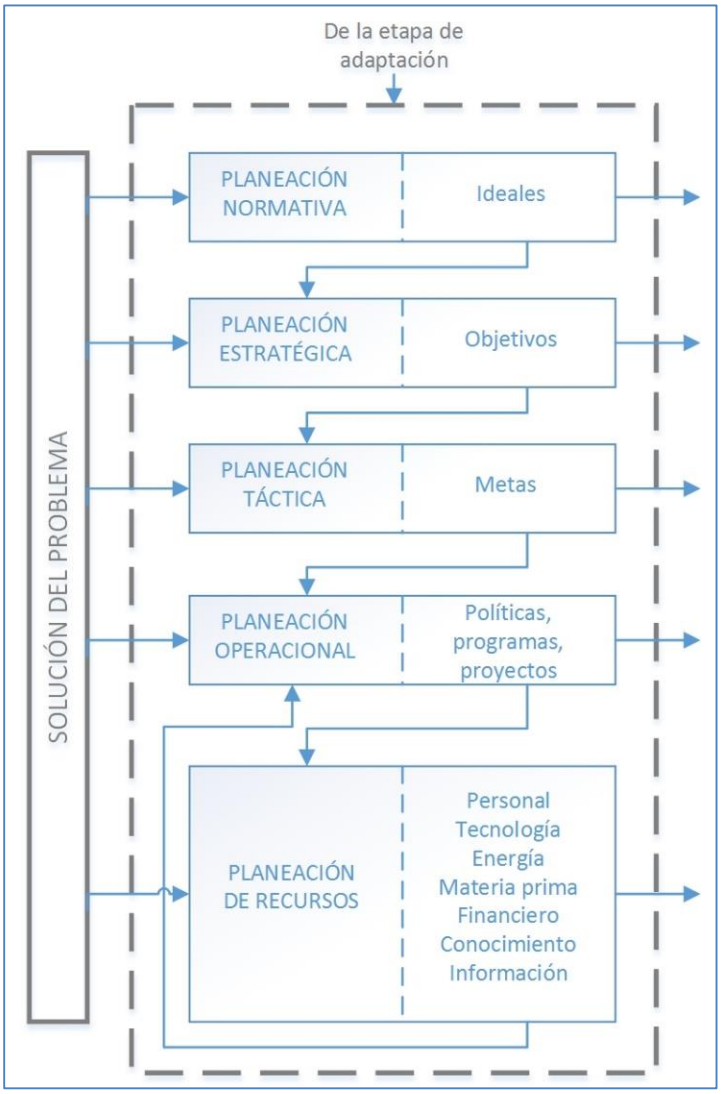


Figura 2.10. Etapa de Instrumentación de la Solución del Subsistema de Planeación.Adaptada de Gelman & Negroe (1982).

Es de destacar la importancia de este Subsistema de Planeación, pues las etapas que lo componen se toman como base principal para la planeación que permite conseguir el objetivo principal de esta tesis. Su aplicación no se llevó a cabo al pie de la letra debido a cuestiones particulares al Sistema de Planeación que se desarrolló y a los objetivos que se perseguían, sin embargo se mantuvo la estructura general de su aplicación.

2.3.2 Proceso de la Investigación de Operaciones (Sagasti & Mitroff, 1973)

En Sagasti & Mitroff (1973) se revisa el Proceso de la investigación de operaciones con una perspectiva holística y se le considera en sí como un sistema conceptual, además de que se afirma que cada uno de sus subsistemas existen sólo por su relación con otros subsistemas y que no tienen significado si se examinan de forma aislada.

La idea de la cual se parte señala que el investigador de operaciones se enfrenta a una *Situación problema* existente en la *Realidad*, en la cual se encuentran de forma desorganizada todos los conceptos que la conforman. Esta *Realidad* es diferente para cada observador, por lo cual su mera definición implica juicios de valor.

De dicha situación problema se genera una imagen mental y a partir de ella se formula un *Modelo Conceptual* que la representa, en el cual el analista pone sus percepciones pertinentes a la situación problema, identifica la estructura del problema y decide qué aspectos son relevantes y cuales son irrelevantes.

El grado de abstracción de este *Modelo Conceptual* permite generar uno o varios *Modelos Científicos*, que se definen como representaciones formalizadas de la realidad usando términos simbólicos y conteniendo variables y parámetros que se juzgan como relevantes.

Posteriormente, con la manipulación del *Modelo Científico*, el analista es capaz de evaluar su consistencia interna, establecer su grado de correspondencia con la realidad y plantear una *Solución*, que es un producto que se genera con el proceso de investigación de operaciones y constituye las bases para las recomendaciones y avisos que se dan al tomador de decisiones. Este enlace entre el *Modelo Científico* y la *Solución* se conoce como proceso de *Resolución del modelo*. Además existe un proceso de *Implementación* de la *Solución*, el cual permite determinar el grado de coherencia de la propuesta generada con la *Situación problema* inicial.

El mecanismo por el cual se da la transición entre la *Situación* problema al *Modelo Conceptual* se denomina *Proceso de conceptualización* y se lleva a cabo con base en un conjunto de ideas, conceptos, anticipaciones y expectaciones que conforman el “conocimiento”, “experiencia”, o “bases científicas”.

Además se considera un proceso de *Modelado* que establece la relación entre del *Modelo Conceptual* hacia el *Modelo Científico*, en la que se identifican las variables controlables y las no controlables definiéndolas precisamente en términos operacionales.

En todos estos procesos que enlazan las fases principales del Proceso de la investigación de operaciones interviene el conocimiento científico, que provee al tomador de decisiones de un repertorio de ideas y conceptos, metodologías, métodos y herramientas de las cuales se vale el investigador para realizar sus actividades.

Por otro lado, existen otros dos procesos destacables. El primero de ellos es el proceso de Validación cuyo objetivo es establecer el grado de correspondencia con la realidad; y el otro es el proceso de Realimentación que permite probar la coherencia y relevancia de las soluciones obtenidas mediante el contraste con la conceptualización inicial de la situación problema.

La figura 2.11 representa este Proceso de la investigación de operaciones que se ha descrito.

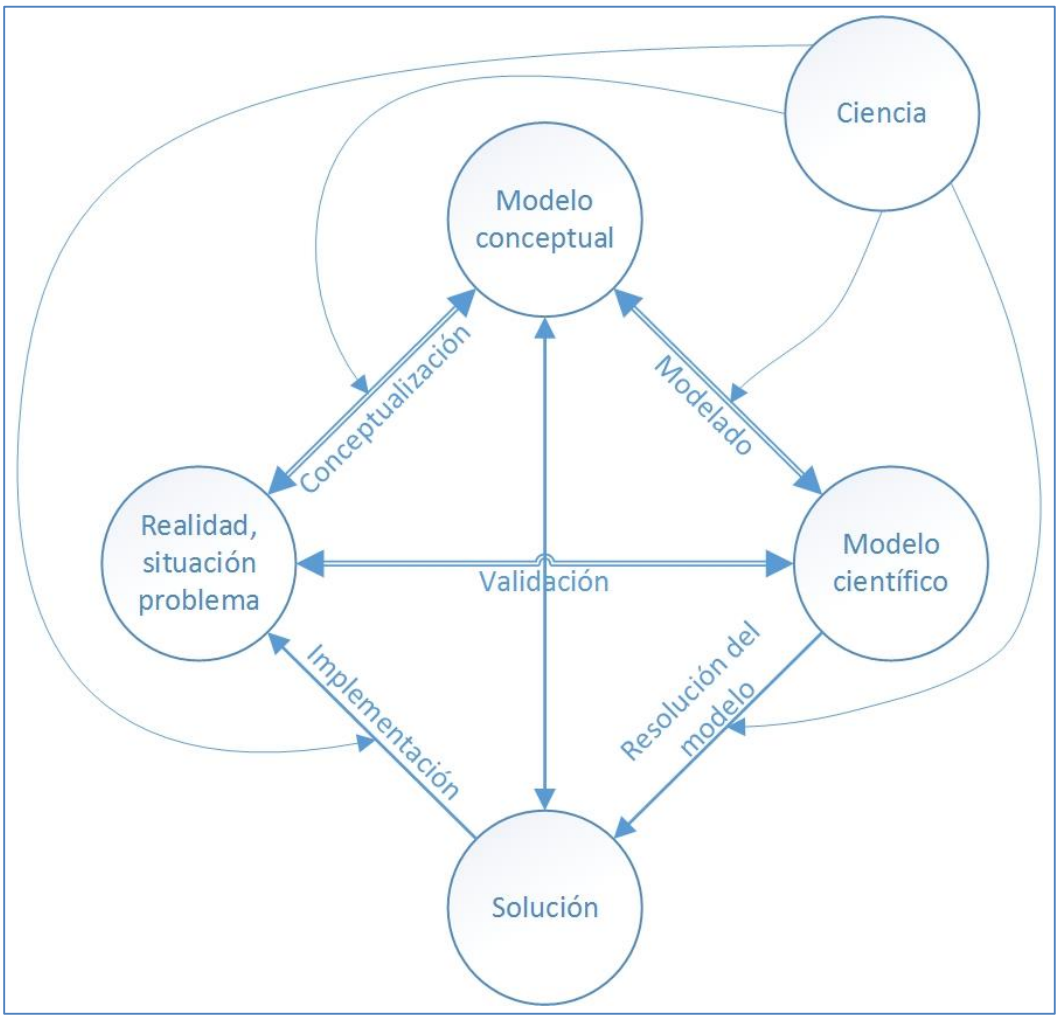


Figura 2.11. Proceso de la Investigación de Operaciones. Adaptada de Sagasti & Mitroff (1973).

2.3.3 Desarrollo organizacional

De acuerdo con Lalonde (2011) una definición del desarrollo organizacional es:

> Es una aplicación a lo largo del sistema y la transferencia de conocimientos de las ciencias del comportamiento para el desarrollo planeado, la mejora y el refuerzo de las estrategias, estructuras y procesos que conducen a la efectividad de la organización.

Sus métodos aplican según el grado en que afectan los procesos humanos (comunicación, toma de decisiones, resolución de problemas y liderazgo), a estructuras tecnológicas (tipo de diseño, la estructura de tareas, y el nivel de delegación y formalización), administración de recursos humanos (desarrollo de habilidades, modos de socialización y sistemas de promoción y recompensas), y estrategia (posicionamiento en el mercado, tipo de transacciones con el ambiente, y cultura de compañía como una herramienta para stakeholders).

El enfoque de desarrollo organizacional que presenta Lalonde (2011) se basa en la teoría de sistemas abiertos de Burke, y se clasifica en 4 tipos:

1. Intervenciones relativas a los procesos humanos con respecto a sus comportamientos y a los medios para lograr sus tareas y alcanzar sus objetivos. Por ejemplo, construcción de equipos, entrenamiento (juegos de rol, simulaciones, aprendizaje en línea), estudios de realimentación, coaching, etc. Se basa en la comunicación, resolución de problemas y participación en la toma de decisiones.
2. Intervenciones tecno-estructurales que buscan reconciliar consideraciones relativas a la estructura y tecnología. Se propone el uso de modelos como organizaciones colaterales, sistemas de aprendizaje en paralelo, sistemas socio-técnicos, equipos semi autónomos, por ejemplo.
3. Intervención en la administración de recursos humanos.
4. Intervención estratégica basada en modelos de sistemas abiertos para que las organizaciones mantengan los enlaces con su ambiente.

Lalonde (2011) se refiere a lo propuesto en Alexander (2005) e indica que el plan debe contener medidas para preparar y entrenar al personal; deben ser claramente escritos, fáciles de poner en práctica, coordinados interna y externamente y distribuidos ampliamente. También debe prever las prioridades de acción en las diferentes fases de la evolución de la crisis, es decir, antes del evento (planeación y prevención), durante el evento (detección de señales de alerta, movilización y reparación) y después del evento (informe, evaluar lo que ha sido aprendido y evaluar cómo ajustar y mejorar). Afirma que la capacidad de una organización para la preparación se incrementa como una función de 4 criterios:

a) Una evaluación de riesgos
b) Evaluación de la capacidad de la organización para enfrentar la crisis
c) El desarrollo y actualización de las capacidades de los individuos
d) El establecimiento de un diseño estructural y flexible que puede ser desplegado rápidamente en el momento de una crisis

El proceso de planeación y preparación en administración de crisis debe ser integrado en la estrategia de toda la organización. La responsabilidad para llevar a cabo tal acción debería ser encargada a una administrador que tenga acceso a un presupuesto bien establecido. Especialistas en gestión de crisis afirman que en la concepción de planes deben estar involucrados todos los stakeholders. Se recomienda usar como herramienta a la técnica de conferencia de búsqueda.

En Lalonde (2011) también se presentan los principales desafíos en la coordinación para la gestión de crisis que propone Quarantelly:

- Comunicación interna, externa y con el público (circulación de información inadecuada, sobrecarga de los canales de comunicación, dificultad para integrar la información externa a los círculos oficiales, público mal informado).
- El ejercicio de autoridad. Falta de disponibilidad de administradores por sobrecarga de trabajo, ausencia de consenso sobre las nuevas tareas derivadas de la crisis.
- El desarrollo de estructuras cooperativas (ausencia de consensos, bloqueos y disfuncionalidades).

2.3.4 Sistemas socio-técnicos

Parten de la idea de que una empresa es un conjunto de personas y medios materiales, de abstracciones de relaciones entre dichos elementos, aspectos de asignación de recursos, y de poder y responsabilidad, entre otros componentes.

A partir de 1940 en el Instituto Tavistock se realizaron algunos estudios enfocados en la minería del carbón, a través de los cuáles investigadores como Emery y Trist empezaron a trasladar conceptos científicos sobre la conducta hacia la industria. Estas fueron las primeras ideas sobre la teoría socio-técnica, donde se considera que al combinar una mejora en los factores sociales, tecnológicos y económicos de las organizaciones se pueden conseguir resultados muy satisfactorios. Este planteamiento se hace bajo la concepción de que las organizaciones son sistemas abiertos y que los elementos mencionados son esenciales en su estructura. La mejora de estos factores no significa necesariamente que estén equilibrados o que se dedique el mismo nivel de atención, sino que para una organización en particular cada uno de ellos se lleve a un estado tal de funcionamiento que sea armónico con el arreglo en general (Jackson, 2000).

El componente tecnológico desempeña un papel determinante de auto regulación de las propiedades de la organización, pues define sus límites con respecto al entorno ya que representa una pertenencia del sistema y lo restringe en su funcionamiento. El que la tecnología funja como un elemento para definir los límites de la entidad contribuye a establecer los valores en los que puede alcanzar un estado estable, ya que no sólo limita lo que se puede hacer sino que determina demandas que se deben de cubrir al interior de la organización y sus fines.

El enfoque socio-técnico enfatiza en 3 actividades generales (Tavistock Institute, 1972):

1. Revelar la forma en que el componente tecnológico y la estructura de la relación de trabajo y los roles ocupacionales, contribuyen al desempeño de la empresa y generan requerimientos para otras partes.
2. Analizar la interrelación entre las partes enfocado en los problemas de coordinación interna.
3. Análisis de los ambientes externos relevantes y la forma en cómo el sistema se relaciona con ellos.

En una empresa, los individuos son quienes llevan a cabo las actividades y es necesario que haya compatibilidad entre sus aptitudes con las tareas que les son asignadas además, claro, además de la capacidad física necesaria. Para conseguir esto es común que se lleven a cabo actividades de análisis, selección y entrenamiento de personal, así como rediseño de actividades. En este sentido se tienen dos enfoques: conseguir al individuo adecuado que se adapte a la tarea y diseñar la tarea que se adapte al individuo. Esta última concepción es un aspecto que considera el enfoque socio-técnico en el funcionamiento de las organizaciones, por lo que toma en cuenta la forma de comportarse y personalidad de los empleados y con base en ello propone modificar la estructura de la organización, incluso en mayor consideración que la que se tienen a los requerimientos tecnológicos. De forma similar se delinea por compromisos con los grupos especiales fuera de la organización (Tavistock Institute, 1972).

Como una de las propuestas clave de la teoría socio-técnica se encuentra la caracterización de la tarea primaria de la organización, es decir, aquella tarea que es imprescindible para que el sistema exista.

Algunas de las ideas que definen al enfoque socio-técnico son:

- Fomentar el trabajo en grupos semiautónomos, auto-regulados, desarrollados por sí mismos y responsables de su propia inspección.
- El trabajo en grupo es más satisfactorio para los trabajadores que el trabajo individual.
- Con el trabajo en grupo se puede realizar tareas completas y da sentido para los trabajadores de las actividades que realizan ya que conocen el resultado final.
- Desarrollo de habilidades múltiples a consecuencia de la flexibilidad en la rotación del trabajo.
- Atención lo más pronto posible de problemas y lo más cercano al área donde se presentaron para evitar que se extienda.

- Fomentar la ayuda mutua entre los integrantes del equipo cuando algunos ya terminaron sus labores asignadas y otros aún no.
- Prescindir de la intervención de un administrador externo al grupo, por lo que los esfuerzos de este elemento se pueden destinar a actividades del contexto o a la coordinación de tareas entre varios grupos.

De esta forma, la integración en los grupos de trabajo se considera un factor determinante para un logro adecuado de los objetivos de una organización. A este respecto en Tavistock Institute (1972) se citan algunos principios de la *teoría de la amistad*, que se consideran importantes para mejorar el trabajo en grupo:

a) La amistad en el trabajo posibilita un mejor ajuste individual hacia las tareas.
b) La amistad permite una mayor disposición hacia la ayuda.
c) La interacción permite un conocimiento mayor de los otros y en consecuencia una cooperación más efectiva.
d) El mejor ajuste individual hacia las tareas y la cooperación permiten una producción más alta, menor ausentismo, facilitar la supervisión y un menor gasto o daño de recursos.

Otra de las concepciones principales de los sistemas socio-técnicos es la que se refiere al ambiente en que se encuentran inmersos y a la relación que tienen con él. Se considera que cada vez es más frecuente que las organizaciones se desarrollen en entornos turbulentos; es decir, en entornos dinámicos cuyas propiedades no sólo surgen de la interacción de sus componentes sino que incluso por el mismo sistema que los genera (Emery & Trist, 1965). Por esto afirman que es necesario, en principio, que las entidades sean flexibles en sus estructuras con el fin de adaptarse a las condiciones, y posteriormente actúen en conjunto con otras para buscar soluciones a través del desarrollo de un conjunto de valores que puedan compartir entre ellas.

Desde esta perspectiva, en Tavistock Institute (1972) se considera que en las organizaciones las razones por las que un individuo realiza sus actividades son:

- El desempeño de la actividad satisface por sí mismo las necesidades psicológicas de las organizaciones.
- El desempeño de la actividad no es satisfactorio por sí mismo pero es un requisito necesario para conseguir otras satisfacciones psicológicas, o para evitar situaciones no placenteras.
- El desempeño de las actividades es inducido por las demandas que surgen de la tarea misma, es decir, de las demandas inherentes.

A partir de esto y de investigaciones en la década de 1970 del Instituto Tavistock propone seis características para garantizar la satisfacción de los trabajadores en el desempeño de sus labores (Jackson, 2000):

1. Deben ser demandantes y representar un reto para los trabajadores.
2. Deben proveer un continuo aprendizaje.
3. Los individuos deben contar con una zona, al menos pequeña, de toma de decisiones.
4. Debe proporcionar reconocimiento y apoyo social para el individuo.
5. Las tareas que realiza el trabajador y/o el producto que contribuye a generar debe estar relacionado con su vida fuera del lugar de trabajo.
6. El trabajo debe ser visto como algo que contribuye a conseguir un futuro deseado.

Uno de los métodos para el desarrollo de soluciones mediante el enfoque socio-técnico es el de Cherns, el cual se conforma por diez principios (Jackson, 2000):

a. Compatibilidad entre las técnicas del proceso de diseño con sus objetivos para el sistema.
b. Especificación crítica mínima de la forma en que el trabajo se lleva a cabo y de quién debería llevarla a cabo.
c. Las diferencias que se tengan con respecto a las especificaciones deben ser controladas lo más cerca del punto donde se originan.
d. Considerar el principio de multifunción para que cada individuo sea capaz de realizar más de una función.
e. Las actividades de un departamento deben ser responsabilidad sólo de sus miembros, mientras que el supervisor debe concentrarse en las actividades de las fronteras.
f. Se debe facilitar el flujo de información a través de sistemas de información adecuados para que la reciban en primer lugar quienes la ocupan para desempeñar sus actividades.
g. Los sistemas de apoyo social deben reforzar la estructura de la organización.
h. Diseño de empleos de alta calidad con base en las seis características que propone el Instituto Tavistock para garantizar la satisfacción de los trabajadores.
i. Diseño de la solución como un proceso iterativo.
j. Autoridad y responsabilidad de quien recibe y maneja los recursos para llevar a cabo las tareas de la solución.

Por medio del desarrollo organizacional es como se busca evitar y hacer frente a los contratiempos y problemas que se presentan en las organizaciones. Como uno de los aspectos esenciales para la mejora de la organización está la generación y transferencia de conocimientos, la intervención para la mejora de los procesos humanos, para conseguir una estructura laboral y tecnológica eficiente, y para establecer y mantener relaciones estratégicas con el ambiente. El desarrollo de planes es esencial es esencial para conseguir los objetivos del desarrollo organizacional, tal como lo plantea Lalonde (2011); planes de crecimiento, de sostenibilidad y de prevención, entre otros.

2.3.5 Modelo de Saga y Zmud sobre la aceptación tecnológica en las organizaciones (Saga & Zmud, 1994)

El modelo que se propone en Saga & Zmud (1994) citado por Quijano (2007), describe factores que intervienen en la implantación tecnológica en las organizaciones. Dicho modelo especifica 3 momento esenciales:

1. La aceptación. Recibir en forma voluntaria el uso de las TIC.
2. La rutinización. Las TIC se consideran un elemento estándar de la rutina normal de una organización.
3. La infusión. Incremento de la comprensión de la organización frente a la tecnología y con ello una afinación y perfeccionamiento de su uso en las tareas diarias.

En estas fases actúan y se interrelacionan distintos elementos que determinan si una tecnología se implanta en una organización, como se puede ver en la figura 2.12.

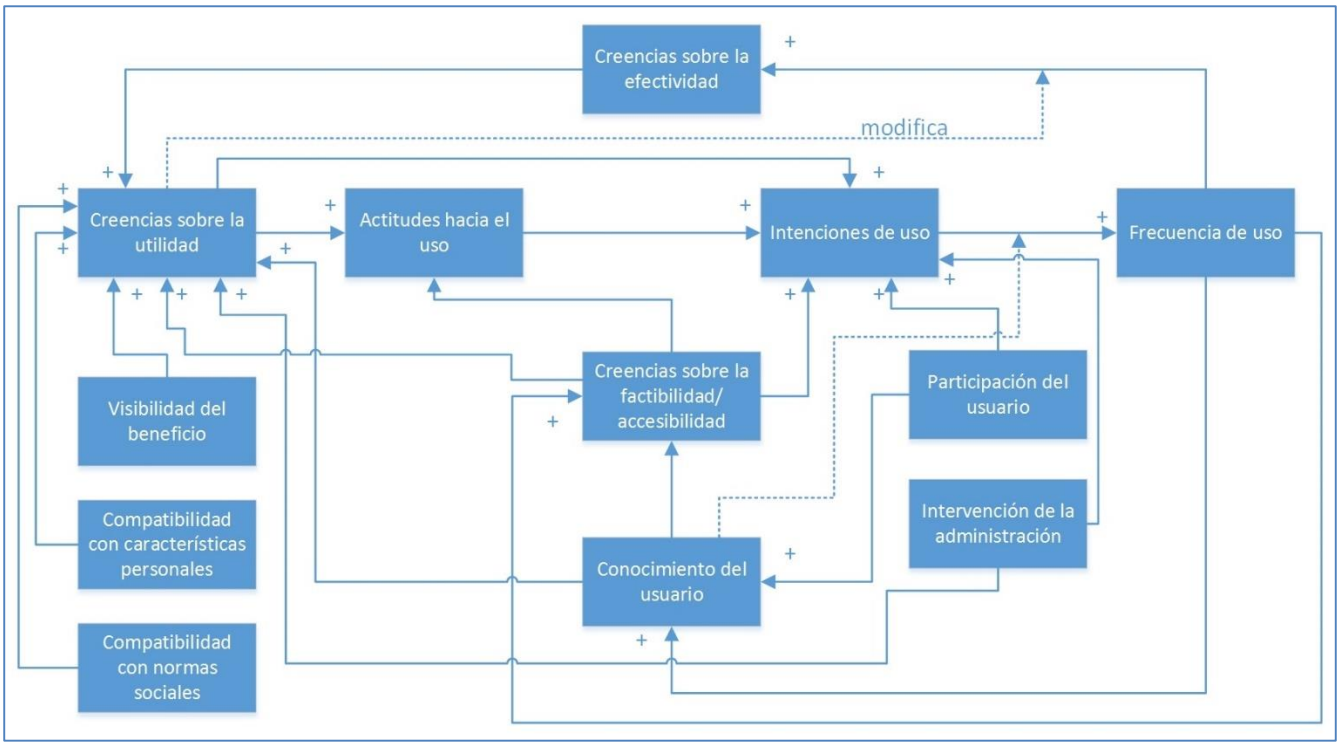


Figura 2.12. Modelo de Saga y Zmud para la implantación de TIC en las organizaciones. Adaptada de Saga & Zmud (1994) citado por Quijano (2007).

Este modelo se toma como apoyo en el diseño del instrumento de validación del *Sistema de Planeación* que se propone, debido a que algunos de los aspectos que considera tienen una importancia esencial para determinar si es factible su uso en un área de gestión de TIC y sobre todo si es útil.

2.4 Estrategia de trabajo

En este capítulo se han revisado distintos enfoques sobre las crisis socio-técnicas. En algunas se les considera que son situaciones que no se pueden evitar y por otro lado están las que indican que se pueden prevenir. Es a partir de éstas últimas en las que se basa el presente trabajo con el fin de establecer un procedimiento de planeación para la prevención de crisis socio-técnicas. Con base en las propuestas que afirman que las crisis se presentan como un proceso y no como un evento aislado se propone un *Sistema de Planeación* que permite identificar a las personas involucradas las señales que advierten la acumulación de sucesos que pueden afectar las actividades esenciales de la organización o que pueden desencadenar una crisis.

Para el desarrollo de los procesos de prevención los investigadores proponen una amplia serie de recomendaciones con el fin de abarcar la mayor cantidad de temas de importancia. Algunas de las ideas que se siguen para conseguir el objetivo de este trabajo son propuestas por varios autores de forma coincidente, y aunque descritas con distintos términos presentan la misma idea en esencia. Se toma en cuenta lo dicho anteriormente sobre el direccionamiento proactivo a causas sistémicas subyacentes de crisis potenciales, los mecanismos de detección de señales, la identificación de stakeholders y sus perspectivas (Jaques, 2010), así como su interacción simultánea y coherente (Hernantes et al., 2013); además del aprendizaje y des-aprendizaje de doble bucle como lo proponen Argyris and Schön en Carmeli & Schaubroeck (2008) para solventar las situaciones que causaron las fallas y no sólo los síntomas. Se retoma la idea de que es necesario considerar cómo se conectan distintas áreas u organizaciones y cómo es su forma de interacción para delinear efectos colaterales a corto y largo plazo; así como la necesidad de generar una cultura para reunir y compartir conocimiento técnico y de las situaciones humanas y organizacionales (Hernantes et al., 2013) ya que ésta estructura organizacional, de políticas y cultura determina la forma de responder a una crisis (Carmeli & Schaubroeck, 2008) y por extensión a desarrollar actividades de prevención.

Los modelos que considera en mayor medida la propuesta de esta tesis son el de *Reacción en cadena* de Tarn et al. (2008), sobre todo en lo que se refiere a las fases Quiesciente y Prodromal, así como el *Modelo de sistemas de control* por la robustez que tiene al proponer la toma de decisiones con base en la interacción humana-tecnología en distintos niveles de libertad con base en el grado de severidad de las situaciones y por considerar actividades de monitoreo de datos duros y de datos suaves, y acciones predefinidas para situaciones que se lleguen a presentar. De igual forma se toman ideas del *Modelo de fase de precondición* explicado en Ibrahim M. Shaluf et al. (2002) y del *Modelo de desastres socio-técnicos* descrito en Aini & Fakhrul-Razi (2010) con respecto a lo que describen de las fases previas a las crisis.

La estrategia de investigación que se siguió para el desarrollo del *Sistema de Planeación* se conforma por cuatro fases propias, enmarcadas en el *Subsistema Planeación* que es parte de la *Estructura del Proceso de Planeación* propuesta en Gelman & Negroe (1982).

Las actividades de la primera fase de la estrategia consistieron de la revisión de literatura científica y fuentes de divulgación de información respecto a las TIC y las crisis asociadas a TIC. Específicamente las investigaciones giraron en torno a los siguientes temas:

- Importancia a nivel internacional de las TIC.
- Utilización de TIC en México.
- Caracterización de las crisis.
- Crisis relacionadas a TIC y sus causas.
- Gestión de crisis en las organizaciones.

La segunda fase de la estrategia etapa también fue de investigación, particularmente en lo que respecta a las perspectivas en las que se ha abordado la prevención de las crisis en las organizaciones y en las áreas de tecnología con el fin de identificar los aspectos esenciales que se han tratado y aquellos que han sido descuidados, así como conocer los resultados y/o experiencias que han tenido distintos autores en sus investigaciones al respecto. También se realizó investigación sobre el enfoque sistémico socio-técnico y sobre el desarrollo organizacional. Los objetivos de esta fase consistieron en integrar una base de conocimiento de la cual partir para la generación del *Sistema de Planeación para la prevención de crisis en áreas de TIC* bajo el enfoque socio-técnico.

En la tercera fase de la estrategia se desarrolló propiamente el *Sistema de Planeación para la prevención de crisis de origen socio-técnico en áreas de gestión de TIC*. Se comenzó por indicar y elaborar definiciones esenciales para el enfoque en el que se desarrollaría la propuesta. En esta fase se establecieron los módulos generales que deberían conformar el *Sistema de Planeación* a partir de las funciones necesarias según se concibió la prevención de las crisis en áreas de TIC y bajo la consideración de los modelos y enfoques de prevención de crisis revisados. El desarrollo de los componentes generales fue secuencial casi en su totalidad, desde la etapa A hasta la etapa D del *Sistema de Planeación*, según se indican y profundizan en el capítulo 3 de esta tesis. Para la especificación de cada módulo se aplicó el principio de *construcción por descomposición* para desarrollar los elementos que lo integrarían, una vez que se planteó el objetivo a lograr para el módulo en turno de desarrollo se idearon los elementos que lo integrarían y sus relaciones (Gelman & Negroe, 1982). En algunos casos fue necesario modificar algunos de estos componentes generales debido a cuestiones que se presentaron con los otros elementos del sistema con los que se relacionaban.

La cuarta y última fase de la estrategia se enfocó en actividades de validación del S*istema de Planeación* propuesto, desde el diseño del instrumento de validación, su aplicación y el análisis de la información recabada. Para desarrollar el instrumento de validación fue necesario hacer una investigación sobre cómo diseñar y estructurar cuestionarios con el objetivo de recabar información verdaderamente útil y de forma confiable; particularmente este procedimiento atendió el modelo de la interacción simbólica del comportamiento pregunta-respuesta entre el entrevistador y el entrevistado, descrito en Foddy & Mantle (1994). Con el fin de agilizar la aplicación del instrumento de validación a expertos en el tema se contemplaron varias opciones y finalmente se optó por poner a su disposición a través de Internet

un video explicativo del *Sistema de Planeación* propuesto y el cuestionario a contestar. Por último se llevaron a cabo actividades de análisis de la información. La figura 2.13 representa las fases de la estrategia de investigación recién descrita.

Figura 2.13. Estrategia de trabajo.

Por otra parte, en la figura 2.14 se presenta esquemáticamente la correspondencia de las fases de dicha estrategia de trabajo con el S*ubsistema Planeación* explicado en Gelman & Negroe (1982). La primera fase desarrollada coincide con la etapa de *Diagnóstico*, la segunda corresponde a la etapa de *Prescripción*, y la tercera y cuarta fases representan las acciones de la etapa de *Instrumentación*.

El *Sistema de Planeación* para la prevención de crisis de este trabajo se basa en el enfoque socio-técnico debido a que éste pretende una mejora en los factores sociales, tecnológicos y económicos, mediante un funcionamiento armónico de los elementos de la organización, lo cual lo hace compatible con aspectos esenciales del desarrollo organizacional. De esta forma se busca que se generen planes de atención a aquellos riesgos con causas socio-técnicas en áreas de gestión de TIC que puedan desencadenar una crisis, que éstos consideren afinidad entre los individuos y las actividades que deben desempeñar, y flexibilidad en las estructuras para adaptarse a los ambientes cambiantes en que se ven envueltas las áreas de la organización. En este sentido se trabaja en las coincidencias en la estructuras de las organizaciones con las propuestas de grupos auto-regulados y figuras y actividades de supervisión para la generación de los planes, sus prácticas y desempeño de otras actividades relacionadas. Otras

guías que se siguen en su mayoría son las propuestas del Instituto Tavistock para la definición de actividades satisfactorias y el método de desarrollo de soluciones mediante el enfoque socio-técnico (Jackson, 2000) para la propuesta del sistema de prevención y para la definición de las actividades que se deberán llevar a cabo.

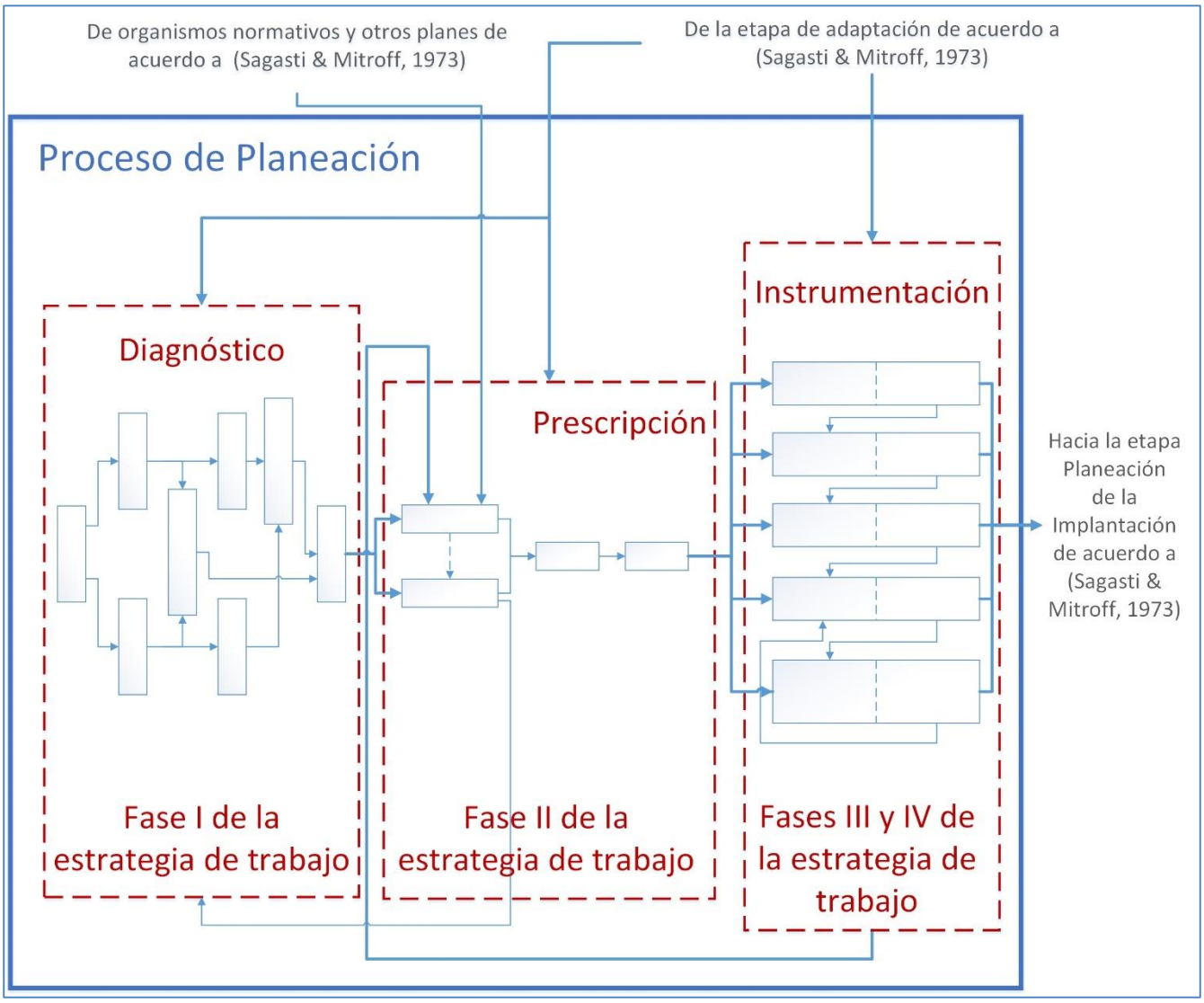


Figura 2.14. Correspondencia de la estrategia de trabajo con el Proceso de Planeación guía para el desarrollo de la tesis. Basado en (Sagasti & Mitroff, 1973).

Conforme a como se estructura el *Sistema de Planeación* propuesto de esta tesis, la fase de desarrollo de los planes de atención a riesgos, descrita de forma detallada en el siguiente capítulo, tiene como objetivo servir como elemento de ayuda en la conducción planificada del sistema de administración de TIC, en el sentido que se refiere en Gelman & Negroe (1982). Se propone que de acuerdo con el tipo de riesgo del área de gestión de TIC que se deberá atender se defina en primer lugar el objetivo y alcance del plan y a partir de éste se determinen cuestiones que lo permitan alcanzar, como por ejemplo

actividades generales y sub tareas específicas, tiempos y recursos necesarios para realizarlas, así como el personal involucrado, entregables e hitos de cada etapa. Se pretende que con los planes que se genere con el *Sistema de Planeación* se siga en la medida de lo posible los 6 elementos que corresponden a la Planeación Táctica de acuerdo con Morrisey (1996), y que se citan a continuación.

1. Identificación de áreas de resultados críticas (ARC). Aquellas en las que se tiene que lograr resultados durante el periodo para el que se planea.
2. Análisis de cuestiones críticas. Se trata de un análisis y propuesta de alternativas a problemas específicos que tendrán un alto impacto en el periodo siguiente de planeación.
3. Indicadores críticos de rendimiento. Factores que se pueden medir dentro de las ARC y que sirven como referencia para saber el grado en que se logran los objetivos.
4. Objetivos. Representan los resultados específicos que se alcanzarán en el periodo del plan. Se les debe determinar una fecha límite para alcanzarlos.
5. Planes de acción. Acciones específicas para lograr cada objetivo: actividades relacionadas y no relacionadas entre sí, o una serie de objetivos más pequeños a corto plazo. Describen tiempos específicos para las tareas, recursos necesarios y responsabilidades asignadas.
6. Revisión del plan. Asegura los objetivos deseados mediante las preguntas: ¿Qué es lo que probablemente cambiará? ¿Cómo y cuándo se sabrá? Y ¿Qué se hará? Implica un monitoreo de las acciones con el fin de aplicar acciones correctivas o planes de contingencia si es necesario.

Es importante aclarar que si bien se propone que el desarrollo de estos planes se haga de forma táctica, las medidas que se tomen con ellos pueden referirse a cuestiones más allá de lo táctico en el área de gestión de TIC y en la organización a la que pertenece.

Por otro lado, las actividades y resultados de la estrategia que se plantea también se pueden mapear al Proceso de la Investigación de Operaciones (Sagasti & Mitroff, 1973) explicado anteriormente. Bajo esta perspectiva, la *situación problema* que existe en la realidad equivale a las crisis en las organizaciones de forma general y a sus efectos; se refiere también a la importancia de las TIC a nivel internacional, y a nivel país en los sectores públicos y privados, e implica los conceptos de crisis y de desastres además de las propuestas formales para atenderlas. Sobre estos temas se realizó la investigación inicial y a partir de dicha base de información se empezó el proceso de *conceptualización* para dar orden y forma a los temas de importancia para definir e la directriz que determina el desarrollo de la tesis, es decir, el objetivo. Como resultado de estas actividades se delimitó el tema de estudio y se generó un modelo conceptual. Posteriormente se desarrollaron de forma más precisa análisis e investigación sobre los temas delimitados a través del objetivo para identificar los aspectos más importantes a considerar para el *Sistema de Planeación* propuesto. En esta etapa se encontraron otras variables de importancia que fue necesario incluir en el modelo conceptual.

El *proceso de modelado* para generar el *modelo científico* consistió de aplicar la composición por descomposición para definir las fases generales y las sub-fases del *Sistema de Planeación* para la prevención de crisis socio-técnicas en áreas de TIC, además de haber seguido un proceso de planeación

de acuerdo con el Subsistema Planeación de Gelman & Negroe (1982). También se ocuparon los puntos que propone el enfoque socio-técnico, el desarrollo organizacional, la atención de las señales en las fases precursoras del desastre (la identificación de riesgos), la estructura de las áreas de gestión de TIC, sus objetivos, sus relaciones y actividades e importancia en las organizaciones, así como los métodos que ocupa para realizar sus actividades. El modelo científico corresponde al *Sistema de Planeación* desarrollado con esta tesis.

Para el proceso de *validación* del modelo científico fue necesaria la participación de expertos en áreas de gestión de TIC. Este proceso de validación terminó con el desarrollo de conclusiones con base en el análisis de la información recabada. En la figura 2.15 se representa gráficamente el alcance de este trabajo con respecto al Proceso de la Investigación de operaciones de Sagasti & Mitroff (1973).

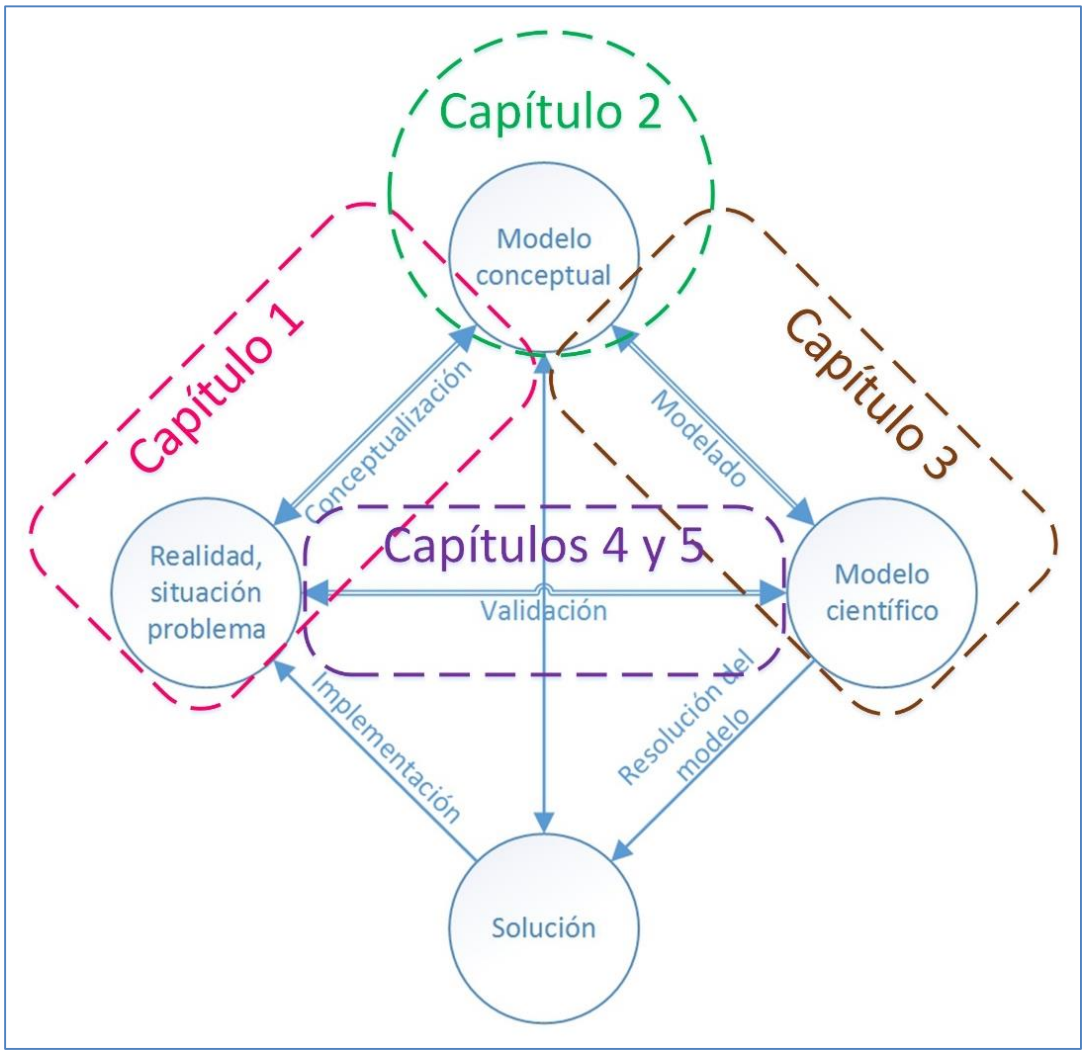


Figura 2.15. Alcance de esta tesis con respecto al Proceso de la Investigación de operaciones de Sagasti & Mitroff (1973).

Capítulo 3. Sistema de Planeación para la prevención de crisis socio-técnicas en áreas de gestión de TIC

Algo común en varias de las propuestas de gestión de crisis socio-técnicas revisadas en el capítulo anterior es la presencia de eventos que vaticinan una crisis. De dichos eventos se menciona que pueden acumularse, o incluso permanecer aislados, y que con el paso del tiempo pueden llegar a generar un estado de peligro en las funciones de la organización (Tarn et al., 2008); sin embargo también se menciona que es necesario cambiar la forma de manejar las crisis y no sólo esperar a que se presenten y entonces actuar. Se habla de cambiar los paradigmas actuales con respecto a las formas de trabajo y de acción para solucionar los problemas en las instituciones, como por ejemplo el trabajo por separado de distintas áreas sobre un mismo tema y/o la poca comunicación entre ellas, o también los deficientes o nulos procesos de retroalimentación sobre cierto evento o comportamiento; dentro de las propuestas una recurrente es la de realizar revisiones en busca de pistas de que se puede dar una crisis si las condiciones actuales se mantienen (Chapman, 2005; Manion & Evan, 2002). Se maneja la idea de las crisis no como un evento que se presenta de forma aislada, sino como parte de un proceso en el que en las etapas iniciales se presentan advertencias de que una situación de crisis se puede presentar.

Es a través de dichas advertencias, que se presentan como eventos o situaciones de riesgo, que se puede vislumbrar que una crisis se presentará si no se actúa para corregir o controlar dichas circunstancias.

En este capítulo se describe un S*istema de Planeación* para la prevención de crisis generado con base en principios del enfoque socio-técnico y del desarrollo organizacional. Metodológicamente se ocupó para su desarrollo la *construcción por descomposición*, procedimiento que parte de la consideración de un sistema y sus fines esenciales para después descomponerlo en subsistemas con base en funciones específicas pero manteniéndolos interconectados y organizados adecuadamente para asegurar el funcionamiento apropiado del sistema en su conjunto (Gelman & Negroe, 1982).

En este caso a partir de la definición de este sistema y de sus objetivos fundamentales deseados en un estado futuro se concibieron las funciones necesarias que ayudarían a conseguir las metas generales y los subsistemas necesarios para desempeñar dichas actividades. El mismo procedimiento, a manera de un comportamiento de tipo fractal, se aplicó en cada uno de los subsistemas que se consideró que deben de existir en un primer nivel de descomposición para establecer las funciones que deberían de llevarse a cabo en su interior para conseguir su razón de ser y así idear, delimitar y dar forma a sus propios subsistemas que lo deberían de componer.

La prevención de crisis que se propone se basa en la identificación de situaciones de riesgo mediante un diagnóstico inicial, la selección de las más importantes y el desarrollo de planes y su ejecución. Como una primera estrategia de prevención está el desarrollo de planes para eliminar las causas del riesgo o en caso de no ser posible mitigarlas para que no evolucionen. Como segunda estrategia se propone el desarrollo de planes de acción que contemplen una respuesta a la presencia de dichas situaciones de riesgo, iniciando con un monitoreo de las variables que indiquen si se ha presentado o *materializado,* y continuando en caso de que se superen los valores límite establecidos con la ejecución de acciones encaminadas a solucionarlos. Como parte del plan general de prevención de crisis se propone una etapa para el diseño de los controles de la ejecución que permitan evaluar los resultados obtenidos y a partir de dichas condiciones se tomen otras medidas o se replanteen si es que es necesario. También en esta etapa se propone realizar revisiones parciales de cómo se ejecutan los planes y de ser conveniente hacer modificaciones para la implantación o en las actividades a realizar.

Para entender este *Sistema de Planeación* es conveniente acordar una definición para el concepto de riesgo. En Antonio & Gaudenzi (2013) se indica que no existe un significado único para este término pues todo depende del contexto en que se utilice, y se proporcionan significados de varias fuentes como muestra de ello; por ejemplo, se cita la definición de riesgo presentada originalmente en Rowe (1977): "*la potencial realización de las consecuencias no deseadas y negativas de un evento*". Así se indica también una definición ISO correspondiente al año 2009: "*efecto de la incertidumbre en los objetivos*", en donde se vincula y limita el concepto a los objetivos. Se menciona que en otros casos se le caracteriza como algo dinámico y subjetivo por lo que se le asigna un carácter ambivalente al asociarse con eventos favorables y desfavorables. De esta forma se señala que en los intentos de definirlo se consideran los efectos, de tal manera que pueden existir *riesgos peligrosos* por tener consecuencias negativas o *riesgos de oportunidad* que generan beneficios.

Para los fines de este trabajo se considera la connotación negativa de los riesgos y a partir de esto se define al riesgo como:

> *Evento o situación que posibilita, aunque no de forma determinante, un daño, un desperfecto o un comportamiento no deseable en el ambiente donde se presenta*.

De forma específica, por el carácter socio-técnico que interesa en esta tesis, dichos *eventos o situaciones* se refieren a:

> *Procesos humanos (comunicación, toma de decisiones, y resolución de conflictos, por ejemplo) y a las relaciones y condiciones de trabajo generadas por los roles ocupacionales, por el uso de los componentes tecnológicos y por procesos administrativos que intervienen en el funcionamiento de un ambiente en particular, en este caso: un área de gestión de TIC.*

Antes de iniciar con la descripción del modelo conviene recordar algunas definiciones de importancia que se presentaron en los capítulos previos y establecer algunas otras, entre ellas la del S*istema de Planeación* propuesto en este trabajo.

Con base Ackoff (1971), de Rosnay (1979) y Forrester (1968) se presenta la siguiente definición de sistema:

> *Conjunto de elementos que tienen un propósito en común, que están relacionados entre sí de forma directa o indirecta a través de otros elementos o de sus atributos.*

Gestión de TIC:

> *Actividades de administración, de operación, de mantenimiento, de monitoreo y de control de sistemas técnicos y de procedimientos administrativos relacionados con actividades al interior del área de TIC que le permiten conseguir los fines para lo que fue concebida*.

Sistema de gestión de TIC:

> *Sistema donde intervienen factores técnicos y sociales para la gestión de TIC y que tiene por objetivo el desempeño adecuado de funciones tecnológicas que contribuyan a las tareas de la organización a la que pertenece, ya sea de forma directa o indirecta.*

Sistema de planeación para la prevención de crisis socio-técnicas en áreas de TIC:

> *Conjunto de directrices, recomendaciones y actividades sustentadas en los principios del enfoque sistémico socio-técnico y el desarrollo organizacional que permitan a las organizaciones prevenir crisis socio-técnicas con origen en su área de gestión de TIC, a través del desarrollo de planes de eliminación, de mitigación o eliminación de riesgos con el fin de evitar situaciones que puedan afectar el desarrollo adecuado de sus actividades*.

Los conceptos anteriores son esenciales para este trabajo, pues el sistema de gestión de TIC a través del desempeño de sus actividades ya sean técnicas o administrativas para la consecución de sus propios objetivos contribuye y afecta el desempeño de otros sistemas con los que está relacionado, por ejemplo sistemas de producción, sistemas de control de personal, o sistemas en donde se administran recursos, por ejemplo. Todas éstas áreas, incluyendo el área de gestión de TIC, forman parte de un suprasistema, es decir, la organización, institución o entidad a la que pertenecen; y además de tener metas propias sus acciones están alineadas a una directriz común: conseguir los objetivos de su suprasistema. En la figura 3.1 se expresa la ubicación del sistema de gestión de TIC y otros subsistemas de la organización a la que pertenecen.

Figura 3.1. Sistema de gestión de TIC y representación general de otros subsistemas de una organización.

Con base en Gelman & Macías (1983), este Sistema de gestión de TIC se considera como el *Sistema Afectable* de interés a este trabajo, el cuál puede verse impactado por *eventos perturbadores* o *calamidades*, es decir, los riesgos cuando se acumulan y/o evolucionan. Para el caso de esta tesis, los estados del sistema afectable (Sistema de gestión de TIC) se conciben de la siguiente forma:

- Normal. Desempeña sus actividades y consigue sus objetivos de forma adecuada.
- Deficiente. Presenta dificultades en el desempeño de sus actividades y en la consecución de sus objetivos; sin embargo con sus resultados contribuye a conseguir los objetivos de la organización a la que pertenece.

- Crisis. Las condiciones no le permiten realizar sus actividades y/o conseguir sus objetivos, por lo cual es incapaz de contribuir con las tareas de la entidad a la que pertenece e incluso puede comprometer de forma importante el desempeño de toda la organización o impedir su funcionamiento.

Para el caso de interés de esta tesis, se considera para este que el *Sistema Afectable* es equivalente al *Sistema Conducido*, y que las actividades del *Sistema de Planeación* propuesto deben llevarse a cabo por un *Sistema Conducente*, de acuerdo a la propuesta de Gelman & Negroe (1982). En primer instancia, quien puede desempeñar esta tarea es la coordinación de la misma área de gestión de TIC apoyada por roles de las áreas de la cual depende en la estructura organizacional o incluso por personal que la conforma. O puede considerarse un área independiente que cargue con dicha responsabilidad, de tal forma que el área de gestión de TIC se vea afectada lo menos posible en el desarrollo de sus actividades. En cualquier caso, se propone que participen en el sistema conducente quien desempeñe el rol de coordinador del área de gestión de TIC, quien coordine el área de la cual depende el sistema de gestión de TIC y sus integrantes en caso de ser necesario, ya sea en la dirección de la implantación del *Sistema de planeación* o como personal de apoyo. Esta propuesta considera actividades para las tres fases en las que el sistema conducente puede estar: a) Preparación, b) Respuesta y c) Recuperación (Gelman & Macías, 1983). Sin embargo, se avoca principalmente a la primera, pues en allí en donde tienen lugar las acciones de prevención de crisis. En la figura 3.2 se representan las fases del *Sistema Conducente* y la relación con los estados del *Sistema Conducido* (Área de gestión de TIC) a través del tiempo en el proceso de atención a crisis del *Sistema de Planeación*.

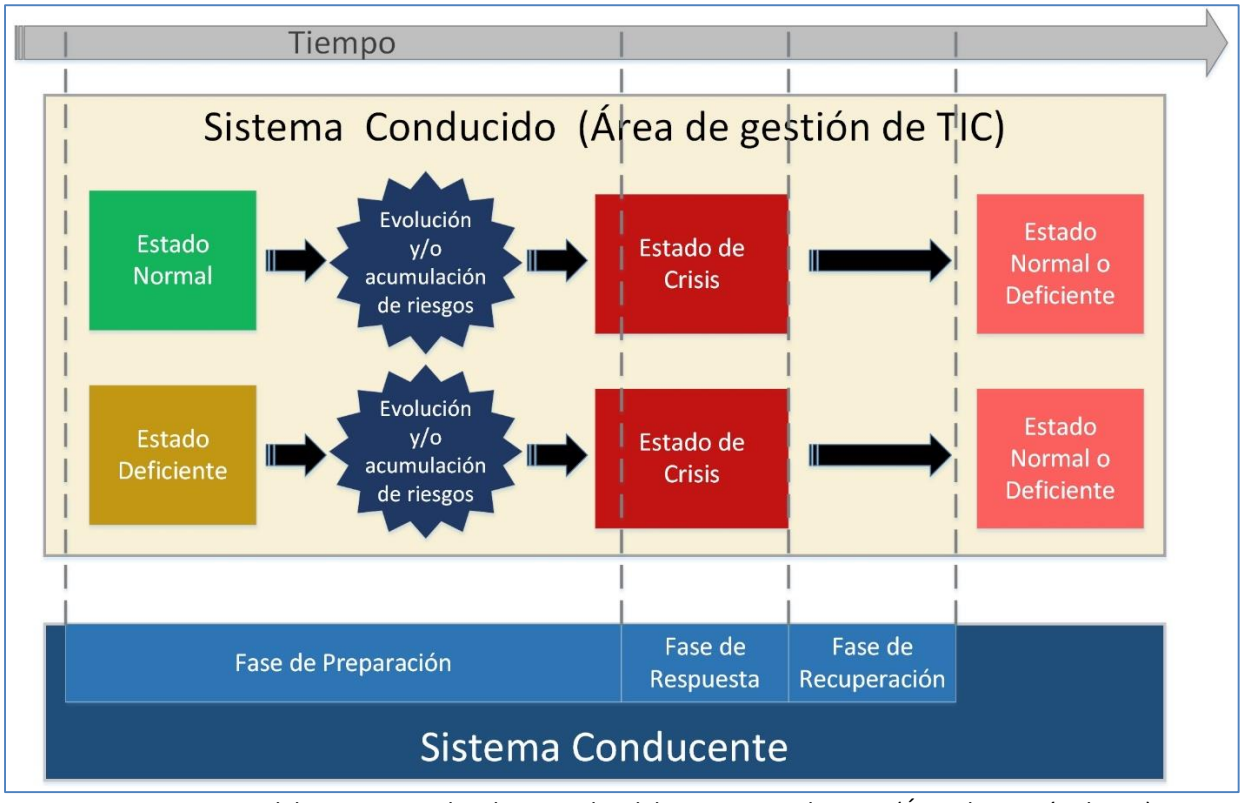


Figura 3.2. Fases del Sistema Conducido y estados del Sistema Conducente (Área de gestión de TIC).

El S*istema de Planeación* que se propone para su ejecución por el sistema conducente se compone de 4 etapas generales:

A. Diagnóstico. Considera una revisión del sistema de administración de TIC en la organización y de las demás áreas relacionadas para la detección de riesgos presentes o latentes que pudieran ocasionar una situación de crisis.
B. Análisis general de riesgos. Jerarquiza y los riesgos y selecciona aquellos para los que se busca el desarrollo de planes de acción.
C. Desarrollo del plan de prevención. Define los objetivos a conseguir para los riesgos seleccionados y describe la forma para desarrollar planes de eliminación, mitigación o respuesta a riesgos.
D. Monitoreo, evaluación y control de la ejecución. Describe las acciones a realizar para controlar la ejecución del proyecto y alcanzar los objetivos de los planes de acción desarrollados.

En la figura 3.3 se muestran estas etapas y además se aprecia un quinto componente que afecta a todas ellas: las condiciones y/o restricciones a las que se sujeta la organización.

Figura 3.3. Elementos que integran el S*istema de Planeación* para la prevención de crisis socio-técnicas.

Las relaciones entre los componentes del sistema y el sentido del flujo de la información se indican a través de flechas. Las de tono verde indican relaciones obligatorias, mientras que las de tono rosado se utilizan para especificar una relación y flujo cuya existencia depende de que se presenten ciertas condiciones en el modelo. Dichas condiciones se describen en el apartado que detalla cada etapa. De forma similar, en las figuras que representan los componentes de cada fase de *Sistema de Planeación* se utilizan flechas de color azul que indican relaciones y flujos obligatorios entre los elementos internos de cada etapa. Para los esquemas que detallan la cuarta fase, se ocupan círculos de color que representan un punto de unión de varios flujos de acciones y a partir de los cuales se sigue un flujo en común del proceso.

A continuación se detallan las fases del *Sistema de Planeación*.

3.1 Diagnóstico socio-técnico del sistema y su entorno

Esta fase del S*istema de Planeación* es esencial debido a que con ella se establece tipo de riesgos a atender. La perspectiva bajo la cual se deben realizar los diagnósticos propuestos es el enfoque socio-técnico y el desarrollo organizacional. Con las actividades que componen esta etapa se caracteriza el sistema en el que se pueden presentar los riesgos y se determinan las relaciones entre las áreas involucradas. Además, con la información que se genera de ella se está en posibilidad de plantear cómo una crisis provocada por la materialización de uno o más riesgos puede afectar a toda la institución. Los análisis que se realizan en esta etapa se listan a continuación.

1. Sistema y suprasistema.
2. Importancia de los sistemas técnicos en la organización.
3. Desempeño y capacidades.
4. Desarrollo organizacional.

En el esquema de la figura 3.4 se presentan estos 4 tipos de diagnósticos como piezas de rompecabezas para destacar la dependencia y unión entre ellos. Esta unión se debe a que existen análisis específicos que permiten concluir en más de un rubro, los cuáles se detallan en los siguientes apartados.

Figura 3.4. Diagnósticos generales que componen la primera etapa del *Sistema de Planeación*.

3.1.1 Sistema y suprasistema

El paso inicial para el diagnóstico es identificar los componentes tecnológicos y humanos que integran el sistema y las relaciones que hay entre ellos. De igual forma es necesario identificar con qué otros sistemas tienen interacción y cómo se afectan entre sí. Se pretende obtener información que responda las siguientes cuestiones:

- ¿Cuáles son los sistemas y subsistemas tecnológicos y administrativos que lo componen?
- ¿Con qué otros sistemas se relaciona el área de gestión de TIC?
- ¿Cómo es la relación de cada sistema que integra el área de gestión de TIC con otros sistemas técnicos y de procedimientos de la misma área y de otras áreas de la organización?

Identificación del sistema de administración de TIC y de sus subsistemas

Es necesario definir las actividades primarias de las áreas de TIC en las que va a tener efecto el proceso general de planeación para la prevención de crisis. En este sentido se debe dejar claro cuál es el área, departamento, jefatura, dirección o gerencia de la organización y sus subcomponentes. Primero es necesario listar dichas unidades estratégicas (en lo que respecta a las TIC en la organización), después

tener claro cuál es su razón de ser, cuáles son sus aspiraciones, y sus objetivos (misión, visión, objetivos). Éstas deben de expresarse de forma concisa y clara.

Es necesario definir el sistema encargado de las actividades de administración de TIC y los subsistemas por las que se compone, así como la relación entre éstos. En una descripción más particular, se profundiza en los elementos de la siguiente forma: Quiénes conforman dichos sistemas, qué actividades se realizan al interior, cuáles son las relaciones en cuanto a estructura laboral entre ellos, con qué otras áreas de la institución se tiene relación ya sea como colaborador, entregando resultados o recibiendo insumos.

A través de este diagnóstico se pretende averiguar si las áreas del sistema de administración de TIC tienen una directriz de acción justificada y posible de seguir para las personas que laboran en él. El saber los fines para los cuáles se trabaja da certeza a quienes se desempeñan en esa área de que sus labores son útiles y que contribuyen a algo más grande e importante que sólo la realización de actividades inmediatas y aparentemente aisladas.

Por otro lado, se busca que al conocerse las relaciones internas del sistema de administración de TIC por el mismo sistema y por otros sistemas de la organización, las personas afectadas por las actividades de dicha área conozcan cómo se relacionan y las funciones primarias que desempeña cada uno para acudir con la persona adecuada en el caso en que sea necesario atender una situación específica. Este diagnóstico tiene también como objetivo ser útil para saber cuáles son las relaciones más frecuentes o necesarias entre los subsistemas y con base en ello realizar propuestas de mejora en los acuerdos, en la comunicación, trabajo en equipo, entre otras consideraciones.

Diagnóstico de la estructura organizacional

Para el diseño, la toma y aprobación de decisiones es necesario tener claro de quién depende el sistema de administración de TIC en lo que respecta a la organización y líneas de mando. Debe incluirse en el diagnóstico la estructura formal de la organización en la que se ubica el sistema que se encarga del manejo de las TIC. En este caso se recomienda incluir un organigrama de la entidad a la cual pertenece.

El diagnóstico, aparte de indicar la estructura debe concluir sobre quienes participan en los proyectos y/o actividades del sistema de administración de TIC y sobre la importancia que tienen éstos en la definición de las directrices que se siguen. Con base en lo descrito en el capítulo 2 se observa que es importante que los roles de toma de decisiones superiores conozcan las actividades que se realizan y los planes de prevención de crisis, además de que incluso participen en el diseño de dichas actividades.

Por otro lado, también es importante concluir sobre la estructura organizacional funcional, en caso de que sea distinta a la estructura organizacional formal, que tienen influencia en el desarrollo de las actividades del sistema de administración de TIC.

Diagnóstico de restricciones operación

Es necesario especificar cuáles son las condiciones a las que se debe ajustar el sistema que se encarga de la administración general del TIC en lo que respecta a reglamentos administrativos y técnicos de la organización, externos e internos al sistema y existentes en los ambientes transaccional y/o transformacional.

Sobre estos se debe concluir en cuanto a sus fines, su compatibilidad con los fines del sistema de administración de TIC, si son claros, si son actuales, si realmente benefician el desarrollo de las tareas o las limitan, qué implicaciones en el desarrollo de las actividades tienen, si son obligatorios o si deben de seguir aplicándose.

3.1.2 Importancia de los sistemas técnicos en la organización

El fin de este tipo de diagnósticos es obtener bases para definir escenarios en consideración al desempeño del sistema de administración de TIC y de sus subsistemas. Se pretende que con la generación de dichos escenarios se pueda identificar el impacto de la materialización de algún riesgo que afecte a los elementos involucrados en este análisis, ya sean técnicos o humanos.

Se pretende que las conclusiones describan la importancia de los sistemas técnicos y del personal que los lleva a cabo, en las actividades primarias de la organización, y el estado de desempeño actual que se tiene para esos criterios bajo las perspectivas del enfoque socio-técnico y del desarrollo organizacional.

Diagnóstico de sistemas técnicos de cada subsistema de administración de TIC

A los diagnósticos ya mencionados se debe agregar el de los factores técnicos con el fin de identificar cuál es el estado de cada sistema administrado de TIC y los riesgos presentes. Este tipo de diagnóstico se tiene que ajustar a los lineamientos definidos por el área de TIC y por las características propias del mismo sistema técnico; sin embargo debe contemplar al menos los siguientes aspectos generales que van enfocados a su administración y uso:

- Identificación de cuáles son los medios por los cuáles cada sistema da señales de monitoreo. En caso de que no exista un hay que idear una forma de monitoreo o desarrollarla.
- Histórico del comportamiento de los sistemas técnicos.
- Documentación sobre el sistema técnico que incluya forma de uso, actividades de administración, mantenimiento, ejecución, reinstalación, monitoreo u otra actividad importante relacionada.
- Respaldo de los sistemas y configuraciones, respaldos de las bases de datos.

- Servidores de respaldo o espejos de aplicaciones.
- Fuentes de energía de respaldo al menos de los sistemas esenciales.
- Respaldo y acceso controlado de contraseñas.
- Acceso físico y lógico controlado a instalaciones de tecnología.
- Redundancia de rutas de comunicación de red. De equipos. De personas que puede administrar una aplicación.

Como se puede ver, este análisis específico también proporciona información sobre el primero de los 4 diagnósticos que conforman esta etapa, el de *Sistema y su suprasistema*.

Diagnóstico del grado de dependencia entre sistemas técnicos de los subsistemas de administración de TIC

Se busca que con este diagnóstico sea posible determinar la importancia de los sistemas técnicos en los procesos que se llevan a cabo en el sistema de administración de TIC con base en las relaciones que tienen con otros. También se pretende que con la información recabada sea posible definir cuáles son los sistemas técnicos más utilizados o cuáles son esenciales en las actividades primarias de cada subsistema de TIC para darles una atención mayor en su administración o en su operación.

Para este fin se pueden utilizar distintos métodos como herramienta. Se propone uno donde se asigne calificaciones cualitativas según el grado de dependencia basado en el siguiente criterio:

- Indispensable: Un sistema no realiza su función principal sin el insumo de otro sistema tecnológico.
- Mediana: Un sistema realiza su tarea primaria a pesar de no recibir el insumo de otro sistema pero no puede realizar otras tareas que dependen de ese insumo.
- Débil: Un sistema realiza su tarea primaria a pesar de no recibir el insumo de otro sistema.

Para la identificación de estos elementos se podría ocupar un esquema conceptual donde las relaciones se expresaran por líneas de colores según su intensidad y con base en un valor asignado a la intensidad de cada línea el concepto adquiriera una categoría de importancia o dependencia por las dependencias que tiene o por qué tan importante es para otros elementos del sistema.

Diagnóstico de la importancia e impacto sistemas técnicos hacia el entorno del sistema de TIC

De cada uno de sistemas técnicos se debe concluir sobre su importancia para las actividades primarias de la organización a través de las relaciones que tiene ese sistema con las otras áreas. Para esto puede aplicarse un método similar al de dependencias entre sistemas, sólo que ahora se propone hacerlo con

dependencias que tienen otras áreas de la organización con ese sistema y la intensidad que tienen, por ejemplo indispensable, mediana o débil.

Con este diagnóstico también se intenta saber cómo contribuyen al desarrollo de la empresa los sistemas tecnológicos y de forma indirecta los roles ocupacionales que se desempeñan en ellos. La idea principal es que se concluya sobre la importancia que tiene el área de gestión de TIC con base en sus relaciones y las de sus subsistemas con el ambiente externo, que es una de las actividades en las que enfatiza el enfoque socio-técnico.

Se contempla realizar también un sub-diagnóstico de impacto que consistiría en plantear escenarios de casos donde alguno de los subsistemas de TIC falle y a través de sus relaciones con otros subsistemas del área o externos describir qué funciones de la organización se verán afectadas. De este diagnóstico las conclusiones indicarían la importancia de los subsistemas de TIC para la organización en general. Podría ser un punto de partida sobre cuáles son los subsistemas de TIC en los que se tiene que enfatizar en el plan de prevención de crisis.

Diagnóstico de dependencias hacia roles-personas de los sistemas técnicos

El fin de este diagnóstico es identificar para cada uno de los sistemas técnicos cuáles son las dependencias o relaciones que tienen con el personal y cómo es el tipo de relación: Operación-uso, administración-supervisión, mantenimiento-reparación-desarrollo. La intención es que se pueda saber en primer lugar de cuántas y cuáles personas o roles depende su correcto funcionamiento y en segundo lugar a cuántas le sirve.

De igual forma que el análisis recién mencionado, las líneas pueden identificarse por un color y recibir una calificación. Con la suma de los puntajes de todas las líneas que llegan al sistema técnico se puede identificar cuáles son los que dependen de más personas o roles y hacia a quién es esa dependencia. Con esto se busca saber si las operaciones de sistemas técnicos están limitadas a ciertas personas o roles.

Se recomienda que las conclusiones sean en relación a la importancia de ciertos roles para el desempeño de las tareas de administración de los sistemas técnicos.

También se busca que a partir de las relaciones entre roles y sistemas que este análisis en particular intenta encontrar, sea posible determinar la importancia de cada sistema técnico para la organización e incluso concluir sobre las capacidades necesarias para operar cada uno, por lo cual sirve como eslabón con el siguiente tipo de diagnóstico general: el de *Desempeño y capacidades*.

3.1.3 Desempeño y capacidades

Diagnóstico de responsabilidades de roles-personas

Con este diagnóstico se pretende determinar la cantidad de carga de trabajo y/o responsabilidades que tiene cada rol-persona. Con este análisis se debe concluir respecto a la asignación de las responsabilidades, sobre lo adecuado de la cantidad, si éstas van acorde al rol o si son adecuadas y sobre si existe el reconocimiento oportuno del desempeño de tales encomiendas.

Como herramienta puede realizarse un esquema conceptual de las personas-roles y la cantidad de sistemas que administran o que su funcionamiento depende de él. Las líneas que indican relaciones pueden referirse a tareas de administración-supervisión o de mantenimiento-reparación-desarrollo. Con una asignación de puntos a cada tipo de encomienda se puede estimar la carga de trabajo.

Diagnóstico de habilidades y aptitudes de personas-roles

El diagnóstico debe evaluar si la descripción de las aptitudes y habilidades de las personas-roles que se necesitan en el sistema de administración de TIC y en sus subsistemas existe o si está actualizada.

Con esta identificación de aptitudes y habilidades para cada rol se debe hacer un cruce con las actividades que realiza quien lo desempeña y en concordancia con el *Diagnóstico de responsabilidades de personas-roles* y se debe calificar si sus aptitudes y habilidades son las adecuadas para el desempeño de dichas funciones. En este caso quien debe evaluar y dictaminar si se cuenta con las habilidades necesarias debe ser el coordinador del área y en caso de ser posible contar con asesoría de personal de recursos humanos. Para asignar una calificación se tiene que evaluar capacidades técnicas, de trabajo, de superación, de resolución de problemas, de trabajo en equipo, etc. Esta información se puede obtener de pruebas de evaluación realizadas previamente en caso de existir. Las pruebas deben de ser recientes. El coordinador del área es quien debe definir cuál es el tiempo máximo en que las pruebas caducarán.

Diagnóstico de desempeño de la gestión y de funciones

Más que evaluar los resultados en el sistema de administración de TIC, este diagnóstico tiene por objetivo evaluar el desarrollo de las funciones desde el punto de vista de la gestión y de la forma en cómo se llevan a cabo. Para esto es necesario ocupar registros existentes sobre el desarrollo de las actividades relacionadas al sistema técnico en cuestión y a cada una de ellas. Se pretende identificar cuáles han sido las causas de gestión y/o desempeño por las que la actividad primaria de uno de estos sistemas ha estado a punto de no conseguirse o no se ha conseguido, identificar situaciones de riesgo repetitivas o condiciones de administración de la actividad que han puesto en riesgo la consecución de

las tareas de cada subsistema de TIC. En este diagnóstico es necesario incluir también las experiencias en la toma de decisiones de suprasistemas que afectan directamente al sistema de TIC.

Este diagnóstico permite concluir respecto deficiencias en el personal para el desarrollo de las actividades que tienen asignadas, pero también genera información sobre deficiencias organizacionales, por lo cual enlaza al *Diagnóstico de desempeño y capacidades* con el de *Desarrollo organizacional*.

Diagnóstico de conocimientos

Debe diagnosticar si los conocimientos que se tienen sobre los subsistemas de administración de TIC y de los procedimientos en los que se desempeñan las actividades son actuales pero sobre todo si son útiles. En este sentido se evalúa si las personas que trabajan dentro del sistema de TIC tienen conocimientos adecuados para las actividades que realizan, si existen y la calidad de los medios en donde se plasme el conocimiento o pasos generales o esenciales para desarrollar o administrar u operar alguna actividad, o donde se indique el funcionamiento de sistemas técnicos y si estos están actualizados con respecto a las últimas versiones existentes. Se evalúan los medios y técnicas para transferencia de conocimientos en el caso de cambio roles o de personas en el sistema. De igual forma se pretende evaluar las oportunidades de capacitación de los integrantes del sistema en nuevas tecnologías o en la profundización de las que se usan actualmente. Otro de los objetivos es evaluar también la actualidad de las soluciones utilizadas en los sistemas técnicos, saber si ocupan tecnologías actuales o que no estén a punto de caer en desuso.

3.1.4 Desarrollo organizacional

Diagnóstico en la coordinación, comunicación, integración

A través de este diagnóstico se debe concluir si las actividades de coordinación para la realización de las tareas en los subsistemas de TIC se realizan de forma eficiente o si ha presentado fallas o tropiezos e identificar las causas. El mismo objetivo se tiene para las actividades y medios de comunicación, en el afán de determinar si el uso de los mecanismos es eficiente. El otro aspecto a evaluar es el de actividades de integración entre los grupos de trabajo al interior del sistema, en caso de existir, y saber si están dando los resultados adecuados.

Diagnóstico de las condiciones de trabajo

El objetivo de este diagnóstico es evaluar si quienes desarrollan las actividades consideran que existen las condiciones adecuadas para el desempeño de las actividades, condiciones físicas como instalaciones

y equipo, luz, servicios como agua, baños, comida, temperatura, espacio, ventilación, zonas de descanso, reconocimiento y valoración por las actividades, permisos, trato de los jefes; e identificar qué tan importantes son esos factores para el desempeño de las tareas de los trabajadores. En esto se incluye la evaluación de si se tienen las herramientas adecuadas a las actividades que se realizan y la compatibilidad con las habilidades de quienes las usan, así como la revisión de licencias de uso de elementos en los subsistemas de TIC.

Diagnóstico de mejora en los procesos humanos

El análisis va enfocado a si existen, si son adecuadas y eficientes las técnicas de mejora o capacitación para el desarrollo de los procesos humanos (comunicación, toma de decisiones, resolución de problemas y liderazgo) y evaluar la participación e interés de los stakeholders que toman las decisiones durante el desempeño de las fases clave en los subsistemas de TIC. También en identificar sesgos subjetivos en la toma de decisiones que afecten el desempeño de las tareas.

Generalidades de los diagnósticos

En el caso de las 3 actividades en las que enfatiza el enfoque socio-técnico, a través del cruce de información entre *Diagnóstico de responsabilidades de roles-personas*, *Diagnóstico de dependencias hacia roles-personas de sistemas técnicos* y el *Diagnóstico de la importancia e impacto de sistemas técnicos hacia el entorno del sistema de TIC* se puede intuir la forma en que el componente tecnológico y la relación entre el trabajo y los roles ocupaciones contribuyen al desempeño de la empresa. En este sentido es importante encontrar cuáles son las relaciones que tienen importancia destacable en la consecución de actividades esenciales de la institución. Es importante porque al identificar estas triadas de *"componente tecnológico – rol – actividad esencial en la empresa"*, se está en posibilidad de hacer énfasis en el diseño de estrategias de prevención de crisis al respecto.

De los distintos diagnósticos se puede concluir acerca del estado de los subsistemas del área de TIC en lo que respecta a sus interrelaciones, se puede ubicar a los elementos que son nodos de conexión de múltiples subsistemas, los que forman parte de procesos de generación de servicios.

De estas rutas de procesos e incluso de los subsistemas identificados es necesario explicar cuáles son las formas de coordinación entre los integrantes de los grupos que llevan a cabo dichas actividades, cuáles son las formas de consenso, de comunicación y de reporte de tareas realizadas y de generación de bases de datos de conocimiento al respecto de las funciones que realizan para dicho subsistema. Para la forma en cómo se realizan estas actividades es necesario evaluar y concluir qué tan efectivas han sido en el tiempo en que han sido ocupadas, efectivas tanto para la función como para las actividades administrativas o de documentación asociadas.

3.2 Análisis general de riesgos

El objetivo de esta fase es que a partir de la información generada con el diagnóstico de cada una de las categorías ya mencionadas se describan los riesgos en los que se puede ver envuelto el sistema de administración de TIC y se seleccionen aquellos que se deben de atender de acuerdo a las condiciones de la organización.

Un esquema de las actividades que se proponen para esta etapa y las relaciones con otras fases se presentan en la figura 3.5.

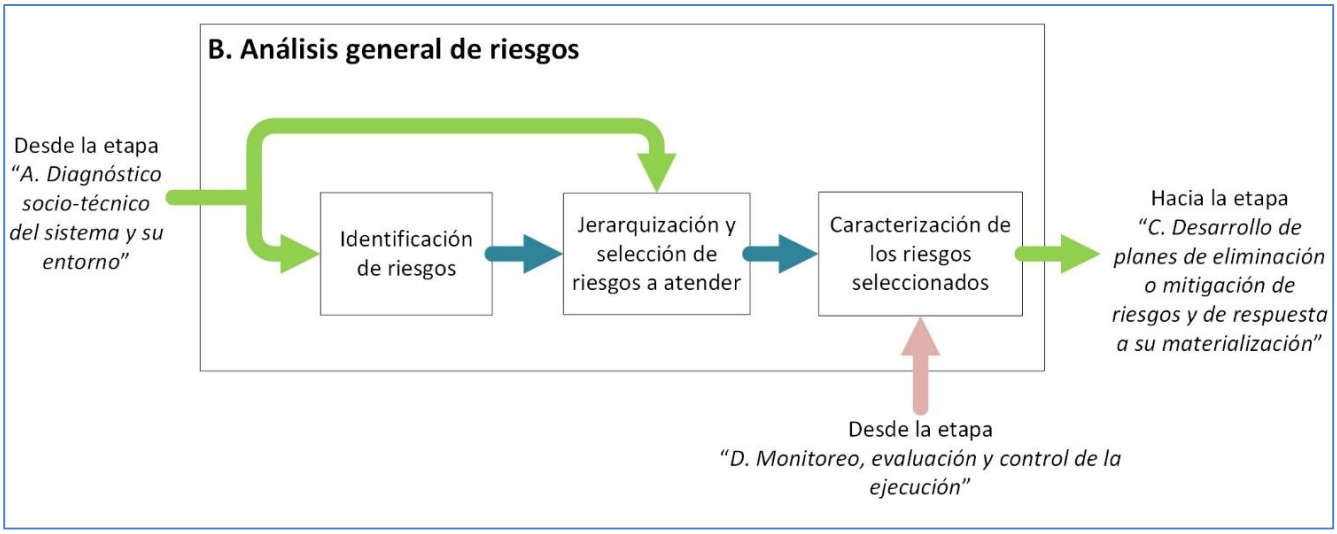


Figura 3.5. Etapa B. Análisis general de riesgos del *Sistema de Planeación*.

3.2.1 Identificación de riesgos

Existen varios métodos para la identificación de riesgos[1], pero un aspecto clave es que se ocupe como base el conocimiento que se tiene del sistema; en este caso dicho conocimiento es el obtenido mediante un enfoque socio-técnico en el diagnóstico previo. Para esta tarea puede utilizarse alguna técnica que se conozca por quienes realicen el plan de prevención de crisis, sin embargo es preferible que sea algún método que siga los principios del enfoque socio-técnico, por ejemplo:

- Trabajo en equipo o en grupos.
- Integrantes de los grupos con distintas especializaciones o formaciones.
- Grupos auto-organizados.
- Sin considerar restricciones para la formulación de riesgos.

[1] En Antonio & Gaudenzi (2013) se describe el Proceso de Evaluación del Riesgo, y se profundiza en los métodos y herramientas que se pueden utilizar en cada una de las etapas que lo componen. La primera, la de *Identificación de Riesgos* tiene como objetivo generar una lista completa de riesgos basados en aquellos eventos que puedan crear, mejorar, prevenir, degradar, acelerar, o retrasar el logro de los objetivos.

- Un ambiente colaborativo entre quienes participan en la actividad.
- Los participantes deben saber que su aporte es significativo para el desarrollo del plan debido a la importancia de esta tarea.

Es necesario que se identifiquen riesgos para todas las categorías de las que se desarrolló el diagnóstico, y preferible que se haga de cada uno de los sub-elementos analizados. Probablemente de algunos sea más fructífera la actividad pero para mantener una perspectiva integral es necesario que se haga un esfuerzo mayor para identificar riesgos donde sea más difícil.

Algunos ejemplos de riesgos que se pueden identificar para los diagnósticos propuestos se muestran en la tabla 3.1.

Sistema y su entorno	Importancia de los sistemas técnicos en la organización	Desempeño y capacidades	Desarrollo organizacional
Visión, misión y/u objetivo ambiguos o inexistentes.	Monitoreo inexistente de sistemas técnicos.	Cargas de trabajo no adecuadas para los roles.	Métodos de coordinación y comunicación deficientes.
Desconocimiento de las áreas integrantes del sistema de gestión de TIC y/o sus funciones.	Documentación inexistente de operación ni de mantenimiento o actualización de los sistemas técnicos.	Responsabilidades no adecuadas para los tipos de rol.	Condiciones de trabajo no adecuadas para el desempeño de actividades.
Desconocimiento de quiénes son los integrantes de las áreas de gestión de TIC y las actividades que realizan.	Inexistencia de respaldos de información generada por los sistemas ni de los sistemas mismos.	Capacidades no compatibles con actividades asignadas.	Inexistencia de promociones ni reconocimientos.
Desconocer de qué área se depende organizacionalmente, sus integrantes y las actividades que realizan.	Acceso físico y lógico a personal no autorizado a los sistemas técnicos.	Transmisión de conocimientos inexistente o ineficiente.	Desintegración.
Desconocer con qué áreas se interactúa y/o las actividades de éstas.	Desconocimiento de cómo intervienen los sistemas técnicos en el desarrollo de las actividades sustantivas internas y de la organización.	Dependencia hacia una persona o grupo reducido.	Falta de capacitación.
Desconocer la estructura organizacional funcional.	Desconocimiento de cómo interviene el personal que administra sistemas técnicos en el desarrollo de actividades sustantivas internas y de la organización.	Capacidades de coordinación ineficiente.	Desinterés de stakeholders esenciales.
Burocracia excesiva.	Actividades primarias dependientes totalmente de aplicaciones únicas sin opción a sustitución o desactualizadas.	Capacidades de comunicación limitadas.	Intereses particulares se sobreponen a intereses de la organización.

Tabla 3.1. Ejemplos de riesgos que se pueden concluir a partir del diagnóstico del plan general de prevención.

3.2.2 Jerarquización y selección de riesgos a atender

Una vez que se cuenta con una lista de riesgos lo siguiente es realizar su jerarquización por importancia[2]. En este proceso de ordenamiento se debe tomar en cuenta las conclusiones de los diagnósticos pero sobre todo considerar las que se refieren a los sistemas o actividades del área de gestión de TIC que son importantes para las actividades esenciales de la organización. Esta consideración no implica un menosprecio de las demás conclusiones, ya que están relacionadas con ésta de forma implícita por medio de alguno de sus componentes y así, al clasificar los riesgos de esta forma se incluyen implícitamente los riesgos asociados con cada caso en particular por las otras clasificaciones.

Además de la importancia de los sistemas y actividades del área de gestión de TIC para la organización entera, en la selección de riesgos a atender intervienen otros factores propios de éstos, de la misma institución y de la situación por la que se atraviesa. Entre estos se encuentran:

- Probabilidad de ocurrencia de los riesgos.
- Impacto de los riesgos.
- Urgencia de las actividades de la institución.
- Ética de la organización.
- Responsabilidad social.
- Imagen ante la sociedad.
- Ingresos que generan las funciones en riesgo.
- Recursos humanos con los que se cuenta.
- Tiempo de acción disponible.
- Presupuesto.
- Cantidad de relaciones que tiene con otros el sistema en riesgo.

Para el procedimiento de selección de riesgos, en caso de que no sea posible para la organización atender todos, se propone aplicar principios de la técnica ZOPP en lo que respecta a la definición del árbol de objetivos, árbol de problemas y selección de alternativas sin llegar a desarrollar la matriz de planeación (Sánchez, 2003). Al menos en esta fase del desarrollo de plan de prevención.

[2] En Antonio & Gaudenzi (2013) se describe el Proceso de Evaluación del Riesgo, y se profundiza en los métodos y herramientas que se pueden utilizar en cada una de las etapas que lo componen. Este proceso considera una fase de *Análisis de Riesgos*, la cual implica una comprensión de los riesgos y los impactos tanto positivos como negativos, y genera información para la evaluación del riesgo y la toma de las decisiones sobre las estrategias y los métodos de tratamiento con base en los diferentes tipos y niveles de atención de riesgos, mitigación, reducción y prevención. Contempla también una fase de *Evaluación de Riesgos*, en la que se define un proceso que se utiliza para comparar los resultados del *Análisis de Riesgos* con ciertos criterios de la organización y así determinar los niveles de riesgo tolerables.

3.2.3 Caracterización de los riesgos seleccionados

Una vez que se han seleccionado los riesgos sobre los que se debe planear, se debe retomar la información que se genera en los diagnósticos de la primera fase para precisar las características de cada uno de éstos. Es necesario detallar con respecto a cada riesgo la siguiente información en caso de aplicar:

- Un nombre para identificar el riesgo.
- El sistema donde se presenta ese riesgo: procedimiento técnico, procedimiento administrativo, sistema técnico, sistema social.
- Cómo se supervisa, coordina o monitorea el desempeño del sistema donde se presenta ese riesgo.
- Requerimientos especiales para llevar a cabo las actividades donde se puede presentar ese evento.
- Condiciones especiales que debe reunir el personal que realiza las actividades en donde se presenta ese riesgo.
- La actividad en particular donde se puede presentar el riesgo, ya sea una actividad que no cambia con el paso del tiempo, que sí cambia su ejecución con el paso del tiempo, que se lleva a cabo de manera temporal o que siempre se debe de ejecutar.
- Otros subsistemas involucrados ya sea como causa o como afectable por el riesgo.
- Las personas que están involucradas: Quiénes, experiencia, habilidades técnicas.
- El efecto que tiene el riesgo en caso de presentarse por sí solo.
- Si es un evento desencadenante de otros riesgos.
- Las condiciones para que este riesgo desencadene una crisis: Conjunción con otro evento, desatención por más de un tiempo determinado, evolución del riesgo, cambio de condiciones en las que se desarrolla.
- Si es un riesgo presente actualmente.
- Periodicidad con que se presenta el riesgo.
- Si implica actividades individuales o el grupo.
- Si es un riesgo potencial.

Y además de especificar tal información, señalar qué condiciones pueden generar el evento, como por ejemplo:

- Condiciones técnicas: Energía, información, condiciones climáticas, espacio en disco duro, capacidad de procesamiento, etcétera.
- Condiciones físicas y lógicas de seguridad de trabajadores y de la tecnología empleada.
- Procedimientos operativos o de administración.
- Trabajadores en particular.
- Carencia de habilidades para desarrollar las actividades.

- Responsabilidad inherente al desempeño de actividades.
- Condiciones físicas del lugar del trabajo.
- Almacenamiento de información.
- Disponibilidad de insumos.
- Periodos en los que se realizan las actividades.
- Tiempo que lleva el personal realizando la actividad.
- Compensación al personal.
- Carga de trabajo.

3.3 Desarrollo de planes eliminación o mitigación de riesgos y de respuesta a su materialización

El objetivo de esta etapa es la generación de actividades encaminadas a evitar una crisis en el sistema de administración de TIC. Haciendo referencia a los modelos de desarrollo de desastre citados en el capítulo 2, dichas actividades se enmarcan en las fases pre-crisis identificadas de la siguiente manera:

- Fases Quiesciente y antes de la acumulación de eventos en la fase Prodromal, según lo indicado en Tarn et al. (2008).
- Fases 1 a 4 del modelo de Ibrahim-Razi para la fase de precondición de desastres (Ibrahim M. Shaluf et al., 2002) .
- Fases 1 a 3 del modelo de desastres socio-técnicos explicados en Aini & Fakhrul-Razi (2010).

Para cada uno de los riesgos seleccionados para atender se debe generar un plan de acción a incluir junto con los demás en un plan general. La idea es generar un plan coordinador que reúna cada uno de los planes que resuelvan un riesgo, o más de uno en caso de ser posible. Esta situación depende de las condiciones de los riesgos seleccionados así como de la institución misma. Con base en las características de los riesgos seleccionados para atender se propone desarrollar inicialmente dos planes, el primero debe ser un *plan de eliminación* o un *plan de mitigación*, y el segundo debe ser un *plan de respuesta* al riesgo para el caso en que el primer tipo de plan no se pueda concluir a tiempo o no consiga los resultados esperados y el riesgo se presente. En caso de que por las características del riesgo no sea posible desarrollar el primer tipo de plan, ya sea de mitigación o eliminación, se propone desarrollar solamente el plan de respuesta al riesgo[3].

[3] En Antonio & Gaudenzi (2013) se describe el Proceso de Evaluación del Riesgo, y se profundiza en los métodos y herramientas que se pueden utilizar en cada una de las etapas que lo componen. Este proceso considera una fase de *Análisis de Riesgos*, la cual implica una comprensión de los riesgos y los impactos tanto positivos como negativos, y genera información para la evaluación del riesgo y la toma de las decisiones sobre las estrategias y los métodos de tratamiento con base en los diferentes tipos y niveles de atención de riesgos, mitigación, reducción y prevención.

De forma general, sin importar el tipo de medidas a tomar en el plan de acción es necesario incluir como obligatorio el informe de la situación a:

- Responsables del sistema donde se presenta el riesgo.
- Responsable en la estructura organizacional del área donde se encuentra el área de administración de TIC.
- Personal que interviene directamente en el sistema donde se presenta el riesgo.
- Personal que interviene indirectamente en el sistema donde se presenta el riesgo.

En la figura 3.6 se presenta en forma de bloques las actividades que se realizan en esta etapa y las relaciones de flujo de información que se tiene con otros componentes generales del plan. A continuación se describen dichas sub-etapas.

3.3.1 Definición de objetivos de los planes para los riesgos seleccionados

Considerando la caracterización de los riesgos seleccionados se realiza un análisis en el que es esencial identificar en primer lugar si el evento es generado por cuestiones operativas, por cuestiones de gestión o por cuestiones de coordinación. De acuerdo con las condiciones que originan el riesgo, con las condiciones del área de administración de TIC y de la organización se debe decidir el tipo de plan a desarrollar. Para tomar esta decisión se debe reflexionar sobre el grado de control que se tiene sobre las causas de los riesgos para cambiar los factores que pueden ocasionar una crisis, si está al alcance del área de administración de sistemas de TIC actuar en dichas fuentes, y considerar también la estructura organizacional relacionada y las restricciones de tiempo, presupuesto y administrativas. Además, es necesario explorar las posibilidades de la organización e incluso contar con la participación en dicho análisis de al menos el coordinador del sistema de administración de TIC, el responsable del área de la cual depende este sistema de gestión de TIC, y en caso de ser conveniente por el tipo de riesgo, del responsable directo del subsistema donde se puede presentar el riesgo.

Se pretende que con este análisis se formulen opciones generales para conseguir el estado ideal ante el riesgo en cuestión. En caso de que las condiciones para alcanzarlo sean poco factibles se debe pensar en las condiciones mínimas necesarias para conseguir un estado satisfactorio. Para cualquiera de estos dos casos es necesario también concluir si es posible eliminar el riesgo mediante un plan para modificar las condiciones que lo generan; de ser el caso se realizará un plan de eliminación de riesgo. Si la situación es tal que se puede alcanzar el estado ideal o el estado mínimo satisfactorio pero no es posible eliminar el riesgo se desarrollará un plan de mitigación de riesgo. Como ya se ha mencionado, además de desarrollar un plan de mitigación o de eliminación del riesgo el *Sistema de Planeación* que se propone considera hacer también un plan de respuesta en caso de que el riesgo se presente. Solamente en caso de que se tenga la certeza de que las condiciones para lograr el estado mínimo satisfactorio

ante el riesgo en cuestión no se pueden alcanzar, se propone hacer únicamente el plan de respuesta a la materialización de riesgo.

A manera de conclusión, con los resultados de esta fase se debe definir el objetivo a alcanzar en los planes de acción, ya sean de eliminación o mitigación de riesgos, o de respuesta a la materialización de un riesgo.

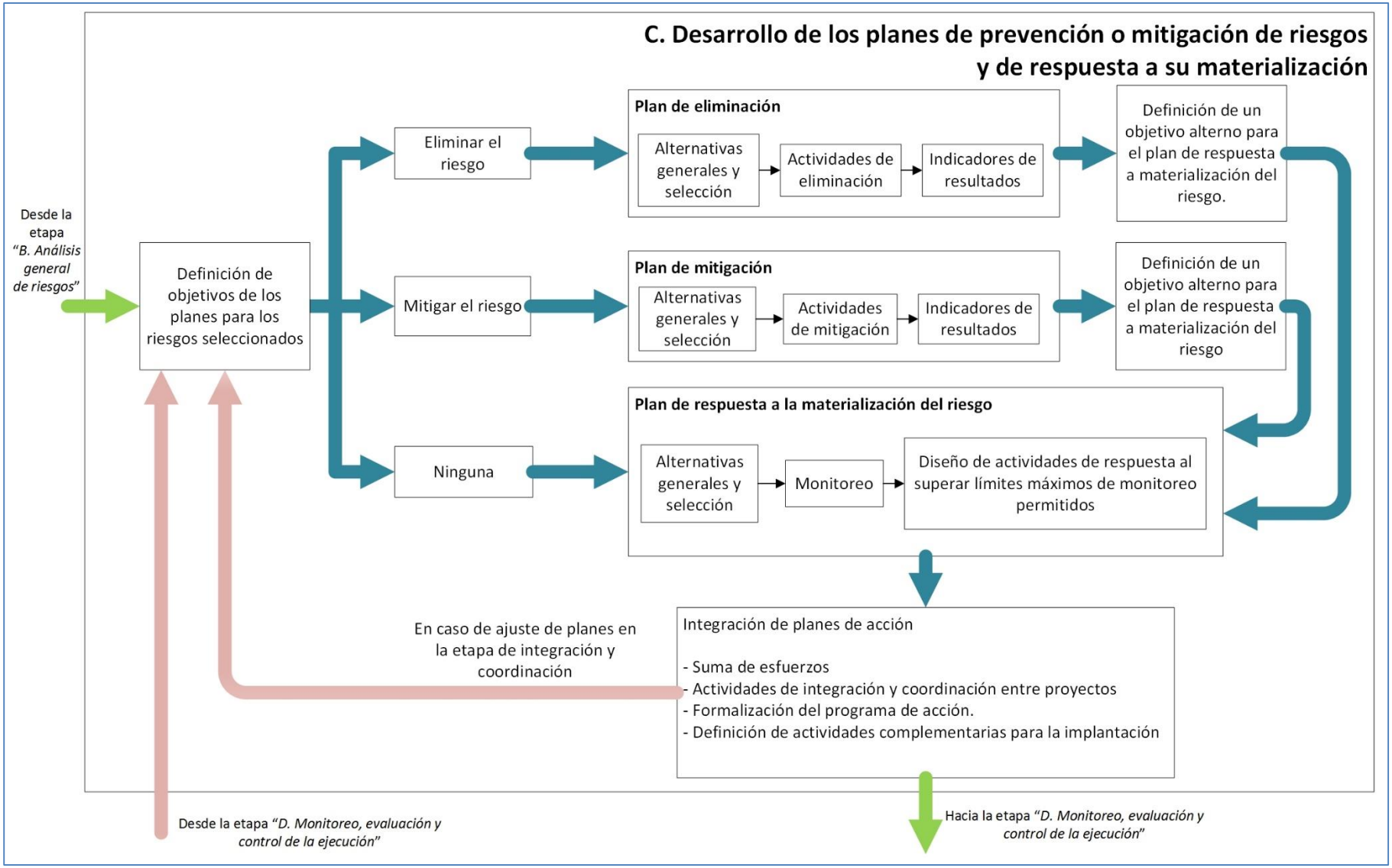


Figura 3.6. Etapa C. Desarrollo de planes de eliminación o de mitigación de riesgos y de respuesta a su materialización.

3.3.2 Desarrollo de los planes de eliminación y mitigación del riesgo

El desarrollo de estos planes debe basarse en los principios del enfoque socio-técnico y del desarrollo organizacional, buscando la integración de los elementos humanos, técnicos y procedurales que intervienen en las actividades del área de administración de TIC. Como se menciona en el capítulo 2 de este documento, la mejora en los sistemas socio-técnicos no implica tener los mismos niveles de desarrollo o importancia entre los factores que los integran sino lograr un estado de armonía entre ellos (Jackson, 2000).

Las actividades a generar para cada plan dependen mucho de las características del riesgo o los riesgos a abordar. De aquí la importancia de caracterizar los riesgos e identificar si es un evento que se origina en el ámbito de gestión, en el ámbito operativo o en la coordinación entre ambos niveles.

Independientemente del plano donde se originan los riesgos, pueden existir factores técnicos, humanos o administrativos, e incluso las combinaciones de ellos, ya sea de forma aislada en los subsistemas o funciones o por la interacción de éstos.

Sin duda cada plan a desarrollar será único debido a las condiciones que se presentan en cada situación, sin embargo, los pasos generales que se proponen para estructurarlo son:

1. Ubicar el elemento, sistema o actividad donde puede materializarse el riesgo. Por ejemplo una persona puede bajar su rendimiento, un sistema técnico puede presentar errores o dejar de funcionar (correo electrónico, servidor Web, fuente de energía), algún procedimiento puede no llevarse a cabo (informe de resultados, respaldo de información, actualización de computadoras), desobedecer un reglamento (permitir el acceso a lugares físicos y lógicos a personas no autorizadas), una interacción entre elementos humanos y técnicos (no dar aviso a las áreas dependientes de los sistemas técnicos de su mantenimiento, deficiencias en la especificación a seguir en proyectos de TIC).

2. Describir la causa del riesgo. Por ejemplo inconformidad de los trabajadores (prestaciones, falta de reconocimiento por sus actividades, exceso de trabajo), formatos de reporte deficientes (información innecesaria o escasa, difíciles de entender o llenar), burocracia excesiva, condiciones de trabajo no adecuadas (herramientas no adecuadas, cambios de temperatura, iluminación o ventilación deficiente), habilidades técnicas o sociales deficientes (dificultad para trabajar en grupo, desconocimiento de tecnologías, buen desempeño en situaciones de estrés laboral), procesos de administración no efectivos (habilidades de planeación, manejo de grupos, coordinación con otras áreas).

3. Idear alternativas de solución y bajo la consideración de las condiciones o restricciones del área de TIC o de la institución misma seleccionar alguna de ellas para diseñar el plan respectivo. En este proceso de selección deben de participar el coordinador del área de administración de TIC,

su jefe inmediato, las personas relacionadas directamente con el riesgo en caso de ser conveniente y otras personas que asesoren según el tipo de riesgo y las alternativas planteadas. En dicha selección se deben considerar factores de eficacia, eficiencia, recursos humanos involucrados, disponibilidad de tiempo, cambios en sistemas relacionados, presupuestos.

4. Diseñar las actividades que conformen la alternativa seleccionada para eliminar o controlar las causas de riesgo. El diseño de las alternativas de solución deben seguir en la medida de lo posible los postulados del enfoque socio-técnico y desarrollo organizacional referidas en el capítulo 2:

    - Cuatro categorías de intervención del desarrollo organizacional (Lalonde, 2011).
    - Desafíos para la gestión de crisis de Quarantelly (Lalonde, 2011).

    También se recomienda que con el fin de evitar la aparición de riesgos al interior del área de gestión de TIC, las actividades generales se diseñen en consideración a:

    - Las seis características propuestas por el instituto Tavistock para garantizar la satisfacción de los trabajadores.
    - Los Diez principios de Chern para el desarrollo de soluciones mediante el enfoque socio-técnico (Jackson, 2000). A excepción del que indica que debe de haber una especificación crítica mínima de la forma en que el trabajo se lleva a cabo; debido a la naturaleza de algunas cuestiones técnicas propias del área de gestión de TIC.

    Además de seguir las directrices generales del enfoque socio-técnico: Fomento del trabajo en equipo y en grupos semiautónomos, ayuda mutua, desarrollo de habilidades múltiples mediante la asignación de actividades diversas y rotación del trabajo, atención inmediata a los problemas que se generan, diseño de estructuras laborables flexibles, mejora de los mecanismos de comunicación y transferencia de conocimientos, capacitación continua.

    Es importante considerar que las soluciones pueden incluso cambiar paradigmas arraigados en la forma de trabajo, lo que en el capítulo 2 de esta tesis se denomina *aprender* y *desaprender* modelos de pensamiento en favor de nuevos; además de que las propuestas deben orientarse a una solución de segundo orden o aprendizaje de doble bucle en el que se busca actuar sobre las causas que originan las fallas y no sólo corregir los errores (Carmeli & Schaubroeck, 2008).

5. Calendarización de actividades. Es importante establecer tiempos para la realización de las tareas que conforman cada actividad general y así llevar un control de avance. De la misma forma, al segmentar las actividades generales en tareas más simples es posible asociar recursos

humanos, presupuestos, tiempo de trabajo, dependencias con otras tareas o actividades y establecer hitos.

6. Definir indicadores para verificar que se alcanzan los objetivos. Para cada plan es necesario establecer indicadores que permitan saber si tras la ejecución del plan se ha conseguido el objetivo respectivo. Dependiendo del caso es posible definir sólo un indicador o varios complementarios entre sí. Tomando como referencia general el diseño de indicadores en la técnica ZOPP en (Sánchez, 2003), es necesario expresar 4 dimensiones principalmente:

   - Identidad. Qué es lo que se mide.
   - Ubicación. Dónde se lleva a cabo la medición.
   - Tiempo. Periodo en el que se hace la medición.
   - Magnitud. Qué valor debe tener para que se acepte el cumplimiento del objetivo.

   Por ejemplo:

   Riesgo: Interpretación errónea entre el equipo de programación de las indicaciones para el desarrollo módulos de un sistema de software.
   Causa identificada: El líder de proyecto no explica bien los requerimientos a los desarrolladores.
   Objetivo: Eliminar este riesgo en todos los sistemas de software que se programen en el área respectiva.

   Para el desarrollo del indicador:
   Identidad: Se disminuyen las interpretaciones equivocadas de requerimientos en el desarrollo de aplicaciones de software.
   Ubicación: Departamento de Desarrollo de Software. En los procesos de comunicación de requerimientos entre el líder de proyecto y el equipo de desarrollo.
   Tiempo: De septiembre de 2016 en adelante.
   Magnitud: No debe haber errores de interpretación de requerimientos.

   Indicador: *Disminución al 0% de las interpretaciones equivocadas de requerimientos para el desarrollo de aplicaciones de software que se presentan en los procesos de comunicación entre el líder de proyecto y el equipo de desarrollo, a partir del mes de septiembre del año 2016.*

3.3.3 Desarrollo de los planes de respuesta al riesgo

El objetivo de este plan es diseñar acciones a llevar a cabo en caso de que por las características del riesgo, las condiciones del área de administración de TIC y las restricciones de la institución de riesgo no se pueda hacer un plan de mitigación o de eliminación de dicho evento. Sin embargo, este plan de acción también debe diseñarse para los casos donde se haya determinado inicialmente hacer un plan de mitigación o eliminación del riesgo, debido a que se pretende tenerlo bajo control un riesgo o evitarlo pero no se tiene la garantía de que los planes vayan a alcanzar sus propósitos de forma total o en el tiempo previsto. Para estos casos recién mencionados es necesario precisar un segundo objetivo al alcanzar, un objetivo alterno en caso de que no se consiga el correspondiente a la mitigación o eliminación del riesgo.

El desarrollo de este plan se compone de 2 fases.

a) Monitoreo. Es necesario establecer cuáles son las variables cualitativas y/o cuantitativas con las cuales se debe monitorear el sistema o la situación en la que se puede presentar el riesgo. Después se debe definir un valor o cualidad límite que indique cuando el riesgo se presente. Es muy importante definir también las siguientes condiciones del monitoreo:

    - El procedimiento para realizarlo. Además de la técnica de monitoreo es recomendable idear algún mecanismo de monitoreo automático, semiautomático o manual para realizar el monitoreo. La decisión que se tome respecto a la forma de monitoreo debe depender esencialmente del tipo de evento y de los recursos de la organización.
    - Los lapsos de tiempo entre cada monitoreo. Como en los otros casos este valor depende principalmente del tipo de riesgo a monitorear. Para establecer este valor es necesario contar con asesoría de quienes participan en las actividades relacionadas directamente, de compañeros, de supervisores, o de un asesor de recursos humanos.
    - Definir el formato en que se almacenan los valores del monitoreo.
    - Alertas. Qué alertas se tienen que emitir al aproximarse a un valor crítico y al superarlo.
    - Los responsables de hacer el monitoreo, a quién se le debe dar aviso de las alertas y quién tiene acceso a la información de monitoreo.

b) Diseño de actividades de respuesta en caso de que se supere el valor máximo para las variables monitoreadas. Su objetivo es cesar el riesgo que ha alcanzado niveles peligrosos y que puede originar una situación de crisis por sí solo o en combinación con otros eventos. Las actividades pueden consistir desde aislar el sistema en que se presenta el riesgo, eliminar la causa de riesgo o el sistema donde se presente aunque esto repercuta en el desempeño de otras actividades o genere otros riesgos menores pero manejables, o incluso suplantar el sistema con uno que realice la misma actividad o una equivalente.

De inicio pareciera que para el diseño de estas actividades es difícil apegarse a las condiciones del enfoque socio-técnico o de desarrollo organizacional por tratarse de acciones que buscan a toda costa evitar el desarrollo del riesgo o su acumulación junto con otros eventos para que no se presente una crisis mayor en sistema de administración de TIC o en la organización, en una especie de situación de emergencia pre-crisis; pero esto no es así. De hecho es necesario tener incluso más cuidado en seguir para este plan las directrices para la integración y coordinación entre los sistemas donde se presenta el riesgo que señalan el enfoque socio-técnico y el desarrollo organizacional debido a que como es necesario actuar de forma rápida, se debe cuidar el tipo de tareas propuestas por los efectos colaterales que pueden ocasionar y por el menor tiempo de reaccionar antes de que se presente una crisis como tal.

De esta manera, para el desarrollo del plan se pueden ocupar los pasos propuestos para la generación de los planes de mitigación o eliminación del riesgo pero teniendo en cuenta el nuevo objetivo y pequeñas variaciones:

1. Ubicar al elemento donde se materializa el riesgo.
2. Identificar la causa del riesgo.
3. Idear alternativas de solución y bajo la consideración de las condiciones o restricciones del área de TIC o de la institución misma seleccionar alguna de ellas para diseñar el plan respectivo.
4. Diseñar el plan para la alternativa seleccionada para eliminar la causa de riesgo. Además de tener las consideraciones ya descritas para hacer el plan de mitigación o eliminación de riesgos, debe profundizarse en los efectos que puede tener cada alternativa propuesta. En este sentido es necesario generar escenarios que describan las posibles consecuencias y explorar si desencadenan otros factores de riesgo y estimar la magnitud de éstos, si tienen solución o si son controlables, el tiempo y recursos para solucionarlos. La selección de la alternativa debe basarse en aquella que genere un panorama con el menor número de contratiempos para el sistema de administración de TIC y para la organización en general.
5. Calendarización de actividades.
6. Definir indicadores para verificar que se alcanzan los objetivos.

3.3.4 Integración de planes de acción

Con esta fase se pretende integrar los planes de acción de atención a los riesgos en un programa general donde se definan actividades complementarias necesarias para su implantación, donde se busque sumar esfuerzos entre los planes o reducir costos sin afectar la eficiencia de cada uno, se le proporcione un carácter más formal para fines de organización y/o administración, se integren o ajusten los calendarios o se identifiquen aspectos de importancia no previstos inicialmente como efectos secundarios, restricciones administrativas, condiciones presupuestarias o tiempos asociados con la

administración que modifiquen su ejecución. Esta revisión y aprobación final requiere de la participación de stakeholders involucrados según el tipo de actividades incluidas en el plan, incluyendo obligatoriamente al coordinador del sistema de administración de TIC. En caso de que exista una contraposición entre los planes de acción o que no pueda ser llevado a cabo alguno o varios de ellos, es necesario optar por otra de las opciones generadas como alternativas o generar una nueva regresando a las bases planteadas en la fase de *Análisis de cada riesgo y definición del objetivo del plan.*

3.4 Monitoreo, evaluación y control de la ejecución

El objetivo de esta etapa es llevar a cabo un monitoreo de los planes diseñados para la atención de los riesgos durante su ejecución y a partir de esto realizar los ajustes necesarios de la implantación o de los mismos planes, o incluso optar por otros si es que después de llevarlos a cabo no se consiguen los objetivos propuestos. Se divide en dos rubros, uno que indica las actividades de monitoreo, evaluación y control de la ejecución para los planes de eliminación o mitigación de riesgos y otro que describe lo propio para los planes de respuesta a la materialización de algún riesgo. Se presentan los componentes generales de esta etapa en la figura 3.7 y después se detalla cada una de ellos.

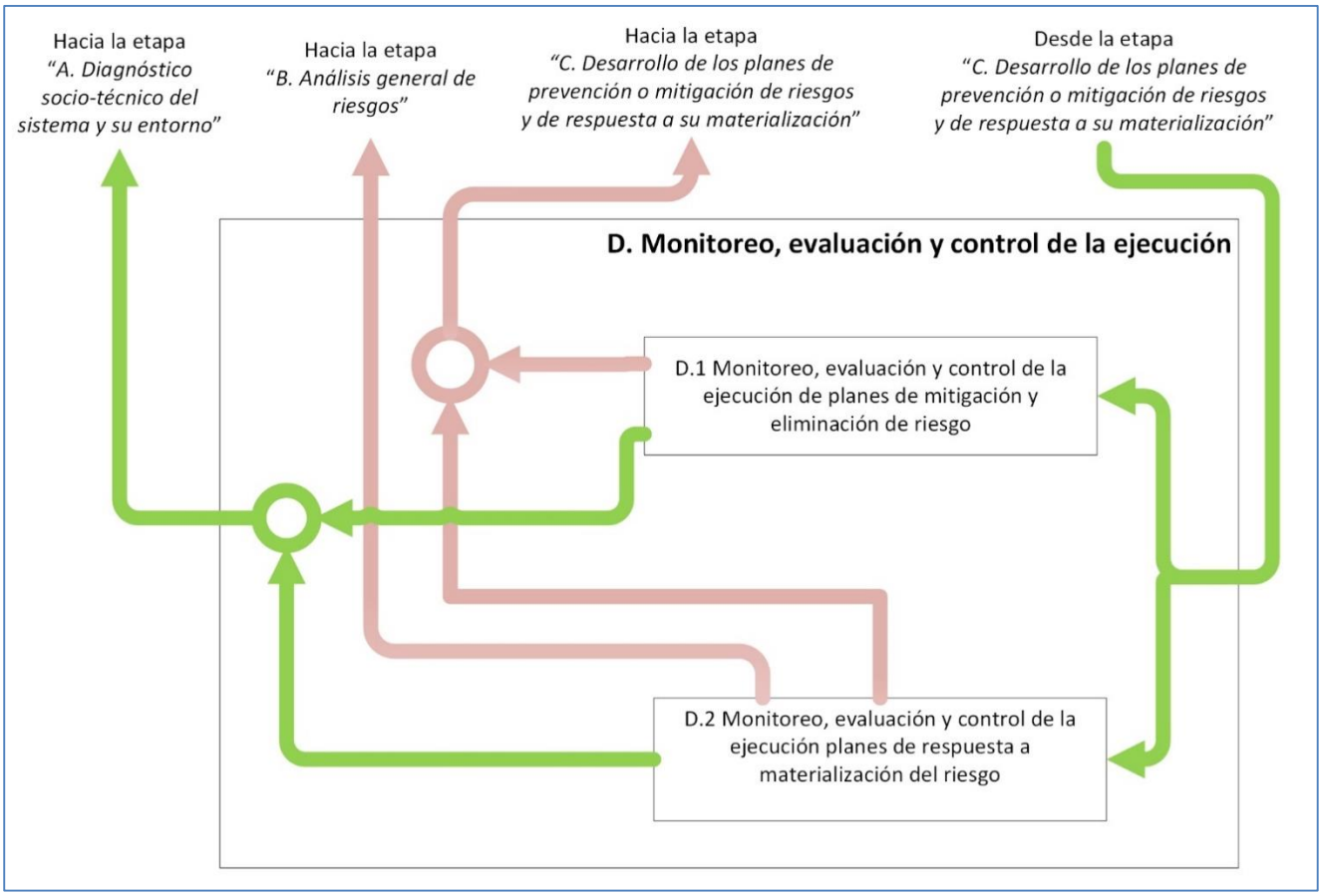


Figura 3.7. Actividades generales de la etapa "D. Monitoreo, evaluación y control de la ejecución" del *Sistema de Planeación*.

3.4.1 Monitoreo, evaluación y control de la ejecución para los planes de eliminación o mitigación de riesgos

Las actividades para monitorear, evaluar y controlar la ejecución de los planes de eliminación de riesgos son las mismas que las que se usan para los de mitigación. La figura 3.8 describe en qué consiste dicha actividad particular de la etapa *D. Monitoreo, evaluación y control de la ejecución*.

En esta sub etapa se lleva a cabo la implantación del plan tal cual se diseñó y al final se evalúa si se ha conseguido el objetivo mediante el análisis de los indicadores diseñados en la fase *C. Desarrollo del plan de prevención*. Si los resultados son aceptables termina la ejecución del plan y se está en posibilidad de iniciar de nuevo con la planeación de prevención para identificar otros riesgos o retomar aquellos que quedaron descartados temporalmente en la etapa *B. Análisis generales de riesgos*. En el caso de que en la evaluación de los indicadores se concluya que los resultados no son satisfactorios se debe realizar nuevamente el procedimiento de diseñar otra alternativa de acción con la que se pueda cumplir con el propósito para el riesgo en cuestión, esto implica retomar las actividades de la etapa *C. Desarrollo del plan de prevención* desde la tarea inicial para el análisis del riesgo que no se pudo atender satisfactoriamente. En este caso se puede retomar alguna de las alternativas diseñadas previamente, pero que quedaron descartadas en la selección de sólo una para desarrollar el plan.

De forma simultánea a esta sub fase del *Sistema de Planeación*, debe llevarse a cabo el monitoreo de los indicadores de cumplimiento del plan según lo establecido, por ejemplo, avance en fases del plan, conseguir hitos definidos dentro tiempo, o el uso de recursos según lo presupuestado. En caso de que no se cumplan estos lineamientos con respecto a lo planeado deben hacerse modificaciones a la forma de ejecución para volver al rumbo indicado y continuar con la implantación; y en caso de que las condiciones en las que se desarrolle no lo permitan se deben realizar ajustes necesarios al plan e intentar su implantación después de dichas adaptaciones. En caso de que no sea posible cambiar la ejecución del plan o modificarlo, debe realizarse nuevamente el diseño de otra alternativa de acción con la que se pueda cumplir con el propósito para el riesgo en cuestión, esto implica reiniciar la etapa *C. Desarrollo del plan de prevención*. También, en este caso se debe retomar alguna de las alternativas diseñadas previamente para ese riesgo, pero que quedaron descartadas en el proceso de selección.

De igual manera, se propone llevar a cabo al mismo tiempo la ejecución del *Plan de respuesta a la materialización del riesgo* diseñado para ese plan de mitigación o para ese plan de eliminación que se esté ejecutando. Esto obedece a que es necesario monitorear el sistema en busca de advertencias y con ello prevenir una crisis. En el momento en que el monitoreo de las variables definidas para ese riesgo detecte que se ha sobrepasado el límite permitido se debe dejar de implantar el plan de mitigación o eliminación respectivo y tiene que empezar a ejecutarse el plan de respuesta a la aparición de dicho evento.

3.4.2 Monitoreo, evaluación y control de la ejecución para los planes de respuesta a materialización de riesgos

Esta es la segunda actividad general de la etapa *D. Monitoreo, evaluación y control de la ejecución*. Las acciones que la componen se presentan a manera de esquema en la figura 3.9. Inicia con el monitoreo de los indicadores acordados durante el diseño para saber si el riesgo se presenta en el sistema de administración de TIC. En caso de que se superen los valores límites establecidos se debe ejecutar el plan de respuesta. Una vez que se haya llevado a cabo se es necesario realizar una evaluación de los indicadores de cumplimiento del objetivo del plan y tomar una acción a partir de los resultados. Si los resultados son favorables y con la ejecución del plan no se generaron riesgos colaterales, termina la ejecución del plan y se está en posibilidad de iniciar de nueva cuenta el proceso de planeación de prevención para trabajar en otros riesgos. En el caso de que se generen otros riesgos debido a la implantación del plan se debe realizar el proceso de caracterización de esos riesgos y posteriormente diseñar alternativas de acción planeación para tratarlos, es decir, desarrollar de nuevo desde el último módulo de la etapa *B. Análisis generales de riesgos*.

En el caso de que no se consigan resultados aceptables del cumplimiento del objetivo es necesario iniciar nuevamente con el desarrollo de un plan de respuesta al riesgo presentado a partir del primer módulo de la etapa *C. Desarrollo del plan de prevención* o retomar alguna de las alternativas descartadas previamente en el proceso de selección de esa etapa y desarrollarla como plan.

Al mismo tiempo que se ejecuta el plan de respuesta se debe llevar a cabo un monitoreo de los indicadores de cumplimiento del plan (metas alcanzadas, uso de recursos según lo planeado, avance en el proyecto en tiempo) para verificar que durante el desarrollo de este no haya inconvenientes en su ejecución. En caso de presentarse contratiempos en la marcha se tienen que hacer modificaciones en la forma de ejecución o incluso en el mismo plan en cuanto a tiempos, actividades o en recursos, por mencionar algunos factores; y posteriormente llevarse a cabo la adecuaciones realizadas. Si no es factible realizar cambios en el plan o en la manera de ejecutarlo es necesario diseñar un nuevo plan llevando a cabo otra vez las acciones de la etapa *C. Desarrollo del plan de prevención*.

Este tipo de planes siempre deben ejecutarse mientras se siga considerando que no se puede eliminar el riesgo. También es necesario definir un periodo de actualización en el que se revise si sigue existiendo el riesgo como tal y si no se puede eliminar o mitigar en las nuevas circunstancias. Esto implica una posible actualización de los planes.

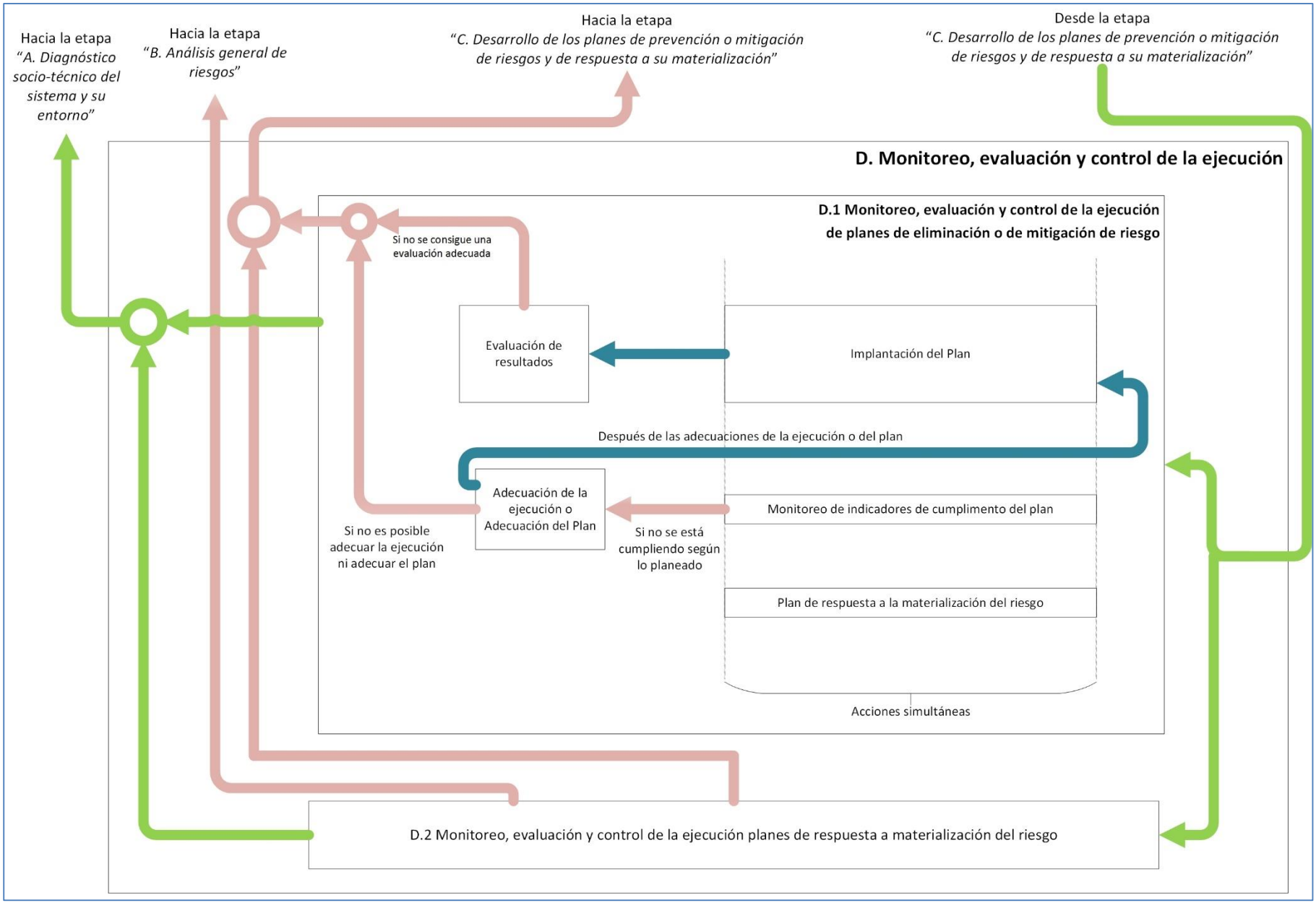


Figura 3.8. Monitoreo, evaluación y control de la ejecución para los planes de eliminación o mitigación de riesgos.

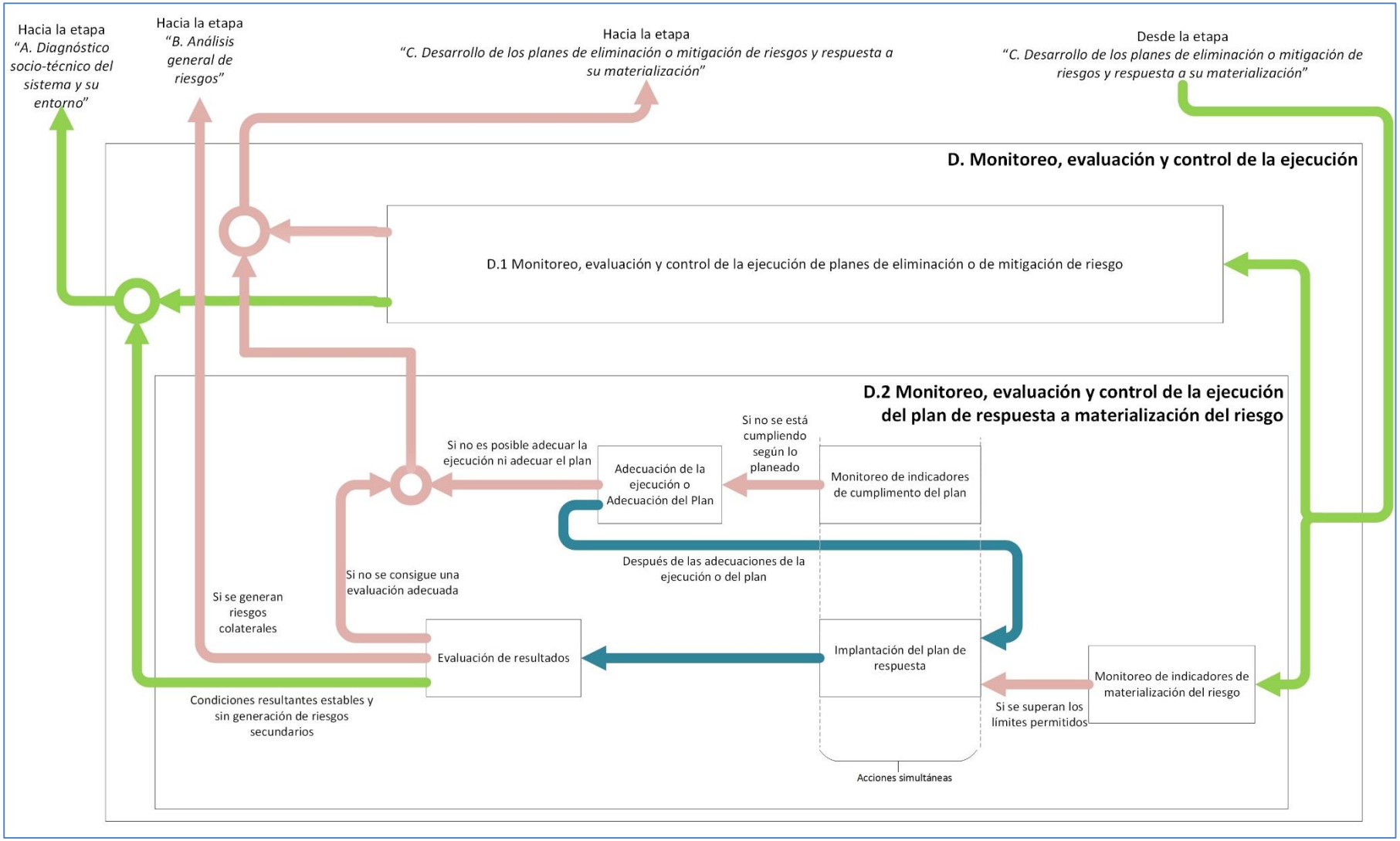


Figura 3.9 Monitoreo, evaluación y control de la ejecución para los planes de respuesta a materialización de riesgos.

Capítulo 4. Validación del Sistema de Planeación para la prevención de crisis socio-técnicas en áreas de TIC

En este capítulo se analiza la información recabada al respecto del *Sistema de Planeación* propuesto en el apartado anterior y se presentan los resultados de una validación general inicial. Los datos para este análisis se recabaron por medio de un cuestionario que contestaron expertos en el área de gestión de TIC. Primero se describe cómo fue desarrollado y aplicado el instrumento de validación así como los fines que se persiguen con las cuestiones que lo integran y al final del capítulo se presentan conclusiones al respecto.

4.1 Instrumento de validación

4.1.1 Criterios a validar y estructura

El instrumento de validación pasó por varias etapas de desarrollo. Desde la depuración y refinación de la cantidad de preguntas que lo integraban, la revisión y redacción en repetidas ocasiones de cada pregunta para asegurar que cumplía con el objetivo pensado, así como de las opciones predefinidas

para el caso de las cuestiones cerradas, el formato en el que se presentaría, la información previa para aplicarlo y el medio en que se distribuiría.

Desde el principio se tomó en cuenta qué es lo que se pretendía obtener con dicho instrumento, es decir su objetivo: *Conocer la opinión de expertos en TIC sobre el sistema planeación propuesto desde 2 puntos de vista; el primero, y más importante para los fines de este trabajo por el poder de decisión y experiencia que tienen al respecto, es el que corresponde a personas que desempeñan funciones de gestión de áreas de TIC; y el segundo, el que pertenece a quienes se desempeñan en dichas áreas y experimentan situaciones donde se pueden generar las crisis socio-técnicas*.

A partir del modelo de implantación tecnológica de Saga & Zmud (1994) consultado en Quijano (2007) se definieron los criterios a analizar. Se utilizó como porque considera factores de importancia común a validar; en específico se utilizó su fase aceptación, pues para los fines de este trabajo interesa saber qué tan conveniente es el *Sistema de Planeación* para llevarse a cabo en un área de gestión de TIC. En la figura 4.1 se indican las variables que intervienen en la *fase de aceptación* referida, y se ordenan y resaltan las que para esta tesis tienen más peso para la validación del *Sistema de Planeación* propuesto.

Figura 4.1. Variables que intervienen en la etapa de aceptación del modelo de Saga y Zmud. Se resaltan aquellas que son de interés para la aceptación del modelo del *Sistema de Planeación* para la Prevención de Crisis en TIC.

A partir de las variables seleccionadas se tuvo en mente recopilar de forma general información que gira en torno a los siguientes criterios:

- Utilidad. Qué tanto es el beneficio que trae el seguir las directrices de acción que se proponen en consideración a los fines que persigue. Y saber las razones de dicho nivel de utilidad.
- Compatibilidad / Adecuado. Qué tan apropiado es el *Sistema de Planeación* propuesto en consideración a las condiciones presentes en un área de gestión de TIC.
- Factibilidad. Conocer si el *Sistema de Planeación* puede de llevarse a cabo en áreas de gestión de TIC, y saber el grado en que se puede ejecutar y las razones de ello.
- Mejoras. Identificar en qué aspectos es necesario mejorar el *Sistema de Planeación* y las justificaciones correspondientes con base en las recomendaciones.

En este caso, se considera que las variables sobre las C*reencias sobre la accesibilidad* y *Creencias acerca de si es fácil de* usar, se ven incluidas en el criterio de *Factibilidad* a evaluar, ya que éste determina qué tantas facilidades tiene el sistema para ser implantado en una institución. Por otra parte, el criterio de *Utilidad* tiene una referencia directa con las variables del modelo que afectan las *Creencias sobre utilidad: Visibilidad del beneficio y Compatibilidad con características personales (y del área de TIC)*.

También se tuvo en mente generar el instrumento para saber de forma particular si lo que se propone en cada módulo del *Sistema de Planeación* contribuye a alcanzar los objetivos para los que está diseñado. En este sentido fue necesario establecer claramente los objetivos de cada uno de los 4 bloques principales del *Sistema de Planeación* antes de desarrollar las preguntas.

El cuestionario se integra por 8 preguntas abiertas (el entrevistado puede desarrollar su respuesta sin restricciones) y 18 preguntas de respuesta cerrada (el entrevistado selecciona una de las respuesta predefinidas). Las preguntas abiertas están enfocadas a que el entrevistado indique de manera libre su opinión sobre el *Sistema de Planeación* en general, las etapas del modelo que lo representan, las ideas base sobre las que se sustenta, y los factores a considerar para llevarlo a cabo. Las preguntas cerradas tienen como fin captar la opinión de los expertos respecto a un tema específico, ya sea sobre el modelo propuesto o sobre el sustento teórico en el que basa, aunque esto no se exprese de manera directa en dichas interrogantes.

Las preguntas de respuesta predefinidas cubren un amplio rango de opciones, incluso extremas pero lógicas y posibles en lo que respecta a los criterios a evaluar. Se prestó especial cuidado para que los valores de separación en la escala para cada caso fueran representativos de distintos niveles de opinión; en cada una de las cuestiones se indicó brevemente la escala en la que se presentarían las respuestas predefinidas, su significado y se evitó indicar opciones que representarán una opción de indecisión por parte del encuestado, sin que esto significará qué no pudiera expresar una respuesta con un valor intermedio entre las disponibles. De igual manera se atendió que el orden en que se presentaron las respuestas predefinidas fuera representativo del valor que representaban con respecto a los valores límites. En la tabla 4.1 se muestra la cantidad de preguntas abiertas y la cantidad de preguntas cerradas por el tema al que se refieren del *Sistema de Planeación*. En la tabla 4.2 se presentan la correspondencia de los criterios principales a evaluar con cada pregunta y criterios secundarios que también se pueden evaluar con el tipo de información que se obtiene.

Tema que se evalúa del *Sistema de Planeación*	Preguntas cerradas	Preguntas abiertas	Total de preguntas
Fase A. Diagnóstico del Sistema y su entorno	8	1	9
Fase B. Análisis general de riesgos	0	1	1
Fase C. Desarrollo del plan de prevención	3	2	5
Fase D. Monitoreo, evaluación y control de la ejecución	2	0	2
Sistema de Planeación en general	5	4	9

Tabla 4.1. Cantidad de preguntas con las que se evalúa el *Sistema de Planeación* y cada fase que lo integra.

Criterio principal que se evalúa	No. de Pregunta	Criterio secundario que permite evaluar
Compatibilidad/Adecuado	2	Utilidad
	4	Utilidad
	7	Utilidad
	8	Utilidad
	11	Factibilidad
	18	Utilidad
	19	Factibilidad
Factibilidad	12	Adecuado
	13	Adecuado
	16	---
	17	---
	21	---
Mejoras	9	Adecuado
	10	Utilidad
	20	---
	24	Utilidad
	26	Utilidad
	15	Utilidad
Utilidad	3	Adecuado
	5	---
	6	Adecuado
	22	---
	23	---
	1	Adecuado
	25	---
	14	Adecuado

Tabla 4.2. Correspondencia de las preguntas del instrumento diseñado con los criterios a evaluar.

4.1.2 Aplicación del instrumento

Los expertos que contestaron la encuesta se desempeñan en ámbitos privados y públicos. Las características que se buscaron en dichas personas son las siguientes:

Expertos en áreas de gestión de TIC.

- Desenvolverse laboralmente en un área de administración de TIC.
- Ser expertos en su actividad de TIC que realizan (al menos 3 años desempeñando las actividades actuales).
- Haber desempeñado actividades operativas de TIC en algún momento.
- Dirigir o coordinar actividades y equipos de trabajo en proyectos o actividades cotidianas de TIC.
- Realizar procedimientos administrativos en su organización con respecto a la gestión de TIC.
- Participar en la toma de decisiones respecto a las actividades de TIC en la organización.
- Desempeñar sus actividades de TIC como parte de un equipo.
- Formación profesional mínima de nivel licenciatura en un área de TIC.
- Activos laboralmente al momento de aplicarse el instrumento de validación.

Para que cada experto estuviera en condición de contestar el instrumento era necesario que conocieran los planteamientos esenciales del *Sistema de Planeación*, sus objetivos, sus alcances y las condiciones para las que está pensado aplicarse. Con el fin de que cada uno contara con la misma información de los temas ya mencionados se optó por elaborar un video explicativo García (2015b) sobre los objetivos de esta tesis, acerca de la justificación del tema que trata y sobre los puntos esenciales del Sistema explicado en el tercer capítulo 3 de este trabajo. Dicho video se puso a disposición de los entrevistados a través del sitio web de videos compartidos *YouTube*, sin embargo no es un material público y no se puede encontrar por medio de un buscador de Internet, sólo se puede ver al contar con el *Uniform Resource Locator* (URL) exacto, el cual se proporcionó a cada uno de las personas a encuestar. Además de esta fuente de información se les proporcionó datos de contacto como teléfono fijo, móvil y correo electrónico para que pudieran realizar consultas en caso de que necesitaran información adicional.

La forma de aplicar la encuesta fue similar. Una vez que se establecieron de forma definitiva los reactivos que la compondrían y las respuestas predefinidas para las preguntas cerradas, se pensó en una forma ágil en la que pudieran contestarla los expertos teniendo en cuenta las actividades laborales que realizan y los tiempos de los que dispondrían. Se optó por aplicar la encuesta a través de Internet García (2015a) y para ello se optó por la herramienta *Google Forms* debido a su maleabilidad para adecuarse a la forma de las cuestiones definidas, por su fácil uso, por su carácter gratuito, por el formato digital en el que maneja las respuestas recabadas y la facilidad en general para trabajar con los datos. También en este caso la única vía para acceder a la encuesta es con la URL exacta que sólo fue distribuida entre las personas a consultar.

La manera en cómo se pudieron llevar a cabo los métodos para explicar el *Sistema de Planeación* y para aplicar el instrumento de validación diseñado fue posible por la formación profesional y laboral sobre cuestiones de TIC de las personas a entrevistar. Se aprovecharon dichos medios digitales de difusión sin el problema de que no se pudieran comunicar ni entender los temas referidos. Este método permitió que los entrevistados revisaran el video las veces que fuera necesario y en los tiempos que mejor les ajustarán según sus actividades. Por otro lado, el contestar la encuesta en línea permitió que los entrevistados no se sintieran presionados por la presencia física del entrevistador y por el tiempo destinado (y limitado) para responder, ya que los pudieron contestar en tiempos establecidos por ellos mismos y con la opción de meditar más sus respuestas y estructurarlas de forma escrita de mejor manera.

4.2 Análisis de la información

En este apartado se realiza un análisis de la información obtenida con el instrumento y se presentan conclusiones al respecto. Las respuestas se revisan con base en los criterios establecidos al inicio de este capítulo sobre el *Sistema de Planeación*: Utilidad, Adecuado, Factibilidad y Mejoras

4.2.1 Utilidad

En la pregunta 25 se cuestiona directamente sobre la utilidad del *Sistema de Planeación* y en todas las respuestas de los expertos se reconoce que ésta existe. Son varias las razones que se expresan acerca de esto. Algunas se refieren a que su utilidad radica en que no hay muchos modelos que aborden los riesgos en TIC desde el enfoque socio-técnico; a que permite identificar qué actividades no se están realizando o a cuales se debe prestar más atención considerando aspectos sociales, quienes las realizan, la forma en que las hacen, y no sólo tener en cuenta el cumplimiento de las metas. Por otro lado se acepta su utilidad debido a que considera cuestiones fundamentales para la gestión de TIC y buenas prácticas y porque contribuye a mejorar tiempos de respuesta ante una crisis o desviación de un proceso sustantivo. Otra de las razones que corroboran su utilidad es que propone un enfoque proactivo para evitar contingencias y no reactivo como en la mayoría de las instituciones.

Algunas de las opiniones de los entrevistados reconocen la utilidad del modelo de forma conceptual por lo que aporta en los planes de atención a crisis, pero destacan que para poder aplicarlo es necesario saber el costo que éste tendría no sólo en el aspecto financiero sino también en los recursos de tiempo y personal. Ante esto vale la pena mencionar que por ser un sistema general de planeación no es posible establecer un costo, pues éste dependerá de la situación de la organización que lo aplique y del tipo de riesgos que se tengan. Otra opinión apunta que su utilidad dependerá de la forma en cómo se aplique, pues puede llegar a fallar si no se respetan las indicaciones de forma correcta o incluso si el uso de las

TIC en las organizaciones no es de manera integral, situación para la que propone que sería un buen caso de estudio para aplicar el Sistema planteado.

Otras de las preguntas del cuestionario tenían como objetivo validar ciertos componentes del Sistema de Prevención de Crisis a partir de la utilidad de los conceptos base en los que se fundamentan. En estos casos cabe destacar las respuestas a la pregunta 5 (figura 4.2) en la que los expertos opinaron con respecto a la utilidad de identificar si una sobrecarga de obligaciones puede afectar el desempeño adecuado de las tareas. Seis de los once expertos consideran que esta situación tendría un 0.8 de probabilidades de ocasionar un riesgo para el desarrollo adecuado de las actividades, dos afirman que esto de seguro generará un riesgo, dos más afirman que existe 0.6 y uno indica que hay 0.2 de probabilidades de que esto sea cierto. La variación de las opiniones puede deberse a los enfoques con los que cada entrevistado tomó la pregunta, sin embargo, lo que es cierto con seguridad es que aunque sea un área donde por lo general se trabaja bajo presión, la mayoría de los encuestados (poco más del 70%) está de acuerdo con que el trabajo con estas condiciones puede generar un desempeño deficiente que puede generar riesgos de importancia en el área de TIC, con lo cual se concede que este diagnóstico es útil para los fines generales del Sistema.

De forma similar, otras de las opiniones de los expertos de las que se puede concluir sobre la utilidad de un aspecto en específico del modelo son las que se dan para la pregunta número 14 y que se grafican en la figura 4.3. En este caso se pregunta sobre lo adecuado de los pasos generales para el desarrollo de los planes de atención a crisis. A este respecto los entrevistados se muestran entre *Medianamente de acuerdo* (27.3%) y *De acuerdo* (72.7%), con lo que se concluye que como pasos generales tienen al menos una confianza media de su utilidad para los fines que persiguen. Como en otras respuestas, los factores que intervienen en estos resultados se refieren a disponibilidad de tiempo y recursos, y a que básicamente dependen de la situación de cada organización y en particular, de cada área de gestión de TIC.

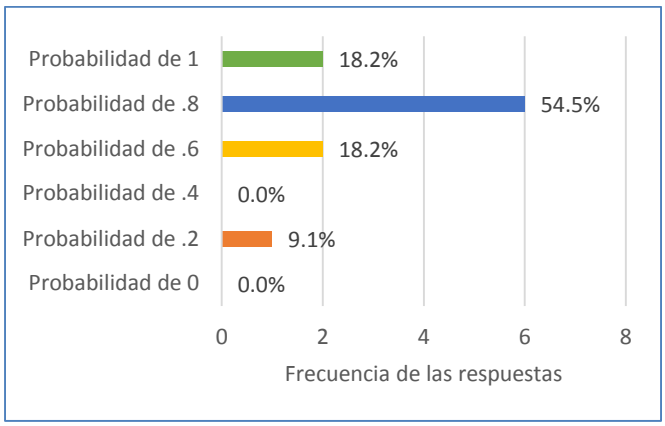


Figura 4.2. Respuestas a la pregunta 5 del cuestionario.

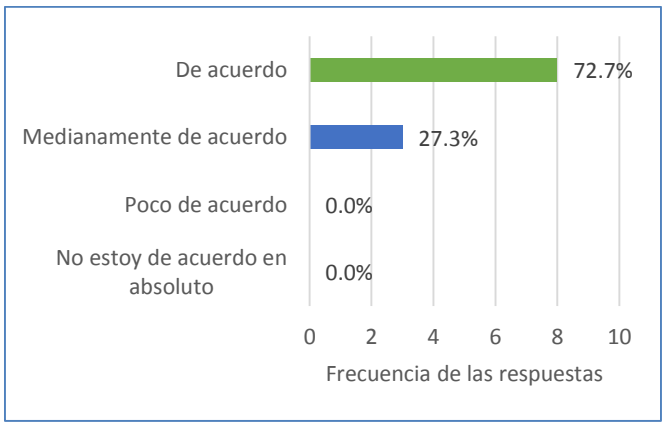


Figura 4.3. Respuestas a la pregunta 14 del cuestionario.

Conviene también hablar sobre las respuestas a la pregunta 23 a causa de la importancia del tema que refiere. En ellas, la mayoría de quienes contestaron el instrumento afirman que es necesario contar con planes de prevención de crisis causadas por aspectos socio-técnicos. Sólo uno de los once entrevistados lo consideraron medianamente necesario, como se indica en la gráfica de la figura 4.4. De estos resultados se puede concluir que la situación de cada organización es muy particular y sus necesidades se ven afectadas por múltiples factores, entre ellos se incluye la robustez de los mecanismos que se ocupen en el desempeño de las actividades al interior de la organización. Es importante destacar que entre los expertos consultados se reconoce la utilidad de considerar que los factores socio-técnicos afectan el desempeño de las actividades de un área de gestión de TIC, y que la mayoría de ellos reconoce que la atención y el cuidado de dichos elementos contribuyen a tener mayor certeza para conseguir resultados satisfactorios.

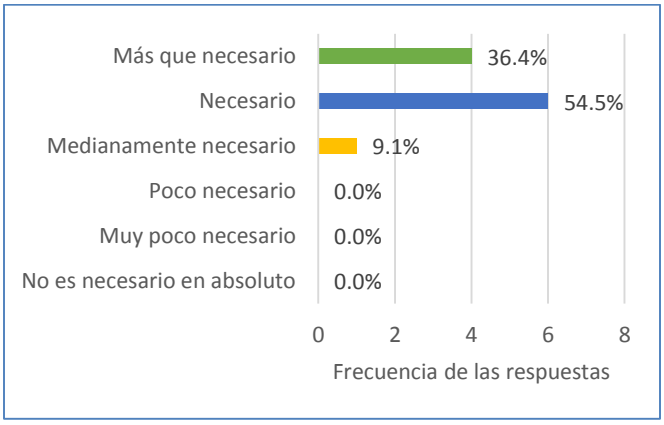


Figura 4.4. Respuestas a la pregunta 23 del cuestionario.

Las respuestas a las preguntas 1, 3, 6 y 22, con las que también se evalúa este criterio se resumen en la figura 4.5. En todas ellas las opiniones reconocen la utilidad de las propuestas.

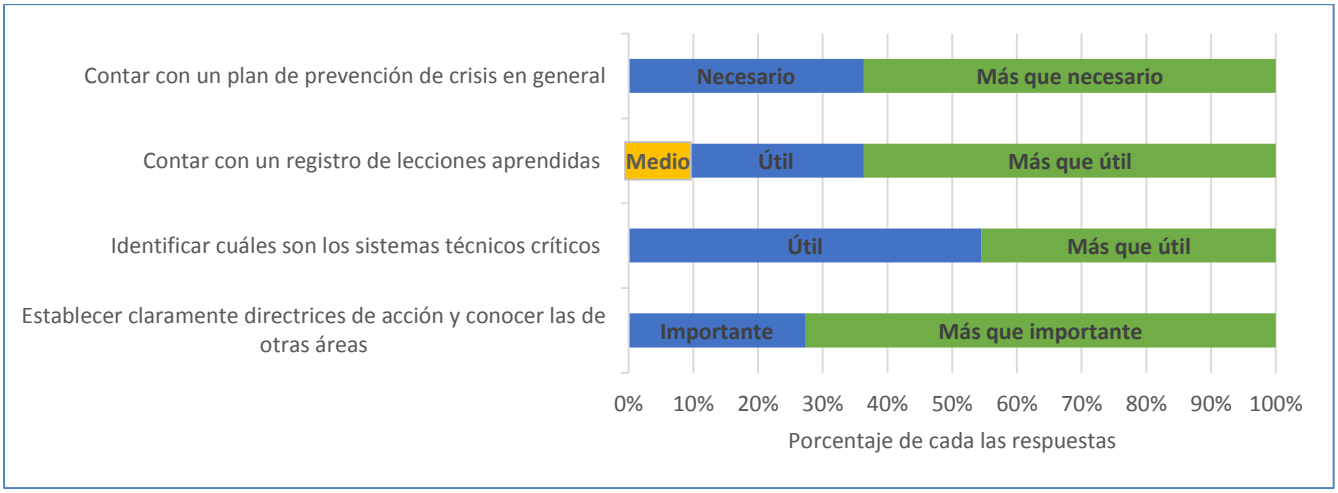


Figura 4.5. Porcentaje de respuestas a cuatro preguntas que evalúan el criterio de utilidad.

4.2.2 Compatibilidad/Adecuado

Con las respuestas a la pregunta 18 (figura 4.6) se puede ver que los expertos consideran adecuado el enfoque que se le da a este *Sistema de Planeación*, pues consideran que para llevar a cabo satisfactoriamente las actividades de un área de TIC es necesaria una armonía entre la importancia y cuidado que se le debe de dar a los factores técnicos y sociales en un área de gestión de TIC. Sólo uno de los once entrevistados concede una importancia parcial de este enfoque para un área donde se gestionan TIC, sin embargo reconoce que puede afectar su desempeño en cierto grado. Es resto de las opiniones concuerda en que es *Necesario* o *Más que necesario* darle importancia a este tipo de elementos.

Una razón de peso que también determina si es adecuado llevar cabo el modelo propuesto es que no se vea afectado el desempeño del área de gestión de TIC en sus actividades habituales para alcanzar las metas que tiene establecidas. De forma general se propone generar soluciones en 3 ámbitos: sistemas técnicos, cultura organizacional y procedimientos de trabajo. En específico se les preguntó a los expertos qué tan factible era que en un área de gestión de TIC se ejecutaran acciones correctivas en esos 3 ámbitos sin que se viera disminuida su eficiencia, y las respuestas fueron variadas como se muestra en la figura 4.7. De dichas respuestas se concluye que al llevar a cabo actividades que se generen con los planes de atención a crisis se afectará el desempeño del área de TIC debido a los factores sociales y técnicos que están involucrados. Uno de los objetivos deseables aparte de los propios de cada plan que se desarrolle, es que la operación habitual se vea perturbada lo menos posible; y para ello tendrán que proponerse, seleccionarse y desarrollarse soluciones de manera muy cuidadosa, como se expresan los expertos en sus comentarios abiertos en las respuestas de las preguntas abiertas 11, 20, 24 y 25.

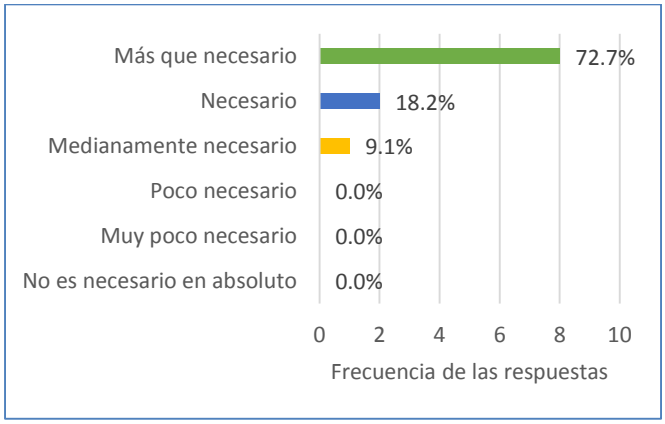


Figura 4.6. Respuestas a la pregunta 18 del cuestionario.

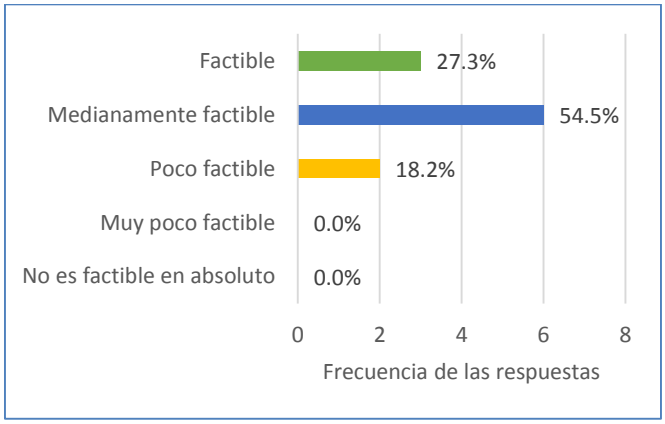


Figura 4.7. Respuestas a la pregunta 19 del cuestionario.

Uno de los puntos esenciales del *Sistema de Planeación* es la conformación de los planes de atención a los riesgos, para los cuales se propone que las acciones que los conformen intervengan en los procesos humanos con respecto a sus comportamientos y los medios para realizar las tareas encomendadas, que

modifiquen la estructura tecnológica y la forma de organización habitual, y que consideren la disposición de recursos humanos (contratación, despido y rotación de personal). Las opiniones de los expertos respecto a este tipo de acciones señalan que son compatibles y convenientes para el área de gestión de TIC, y otros apuntan que no sólo eso, sino que son deseables y necesarios. Con las respuestas recabadas en las respuestas de la pregunta número 11, los entrevistados afirman que para llevar a cabo estas acciones se depende las condiciones de cada área de gestión de TIC y de la organización a la que pertenezca, particularmente por los factores de recursos financieros de los que se disponga y del tiempo disponible para llevar a cabo tales acciones ya que por la realización de las tareas diarias es difícil atender este tipo de cuestiones.

Algunos de los expertos indican que es posible llevar a cabo este tipo de acciones pero con una planeación adecuada para que afecten de forma mínima la operación del negocio, idea que va de acuerdo con el desarrollo propuesto de los planes de atención al riesgo. Aseveran que se necesita el respaldo por otras áreas de la institución en su formulación y aplicación, en particular de la alta dirección; incluso se llega a hablar de que su aplicabilidad dependerá del grado de madurez de la empresa, y que su factibilidad se incrementará si se cuenta con un gobierno corporativo establecido y un gobierno de TI alineado a los objetivos de la organización.

Las respuestas a las otras de las preguntas del cuestionario cuyo objetivo es permitir saber si es adecuado el modelo para aplicarse en un área de TIC se resumen en las gráficas de la figura 4.8, en donde se aprecia que lo propuesto por cada una de ellas es considerado adecuado por quienes contestaron el instrumento de validación.

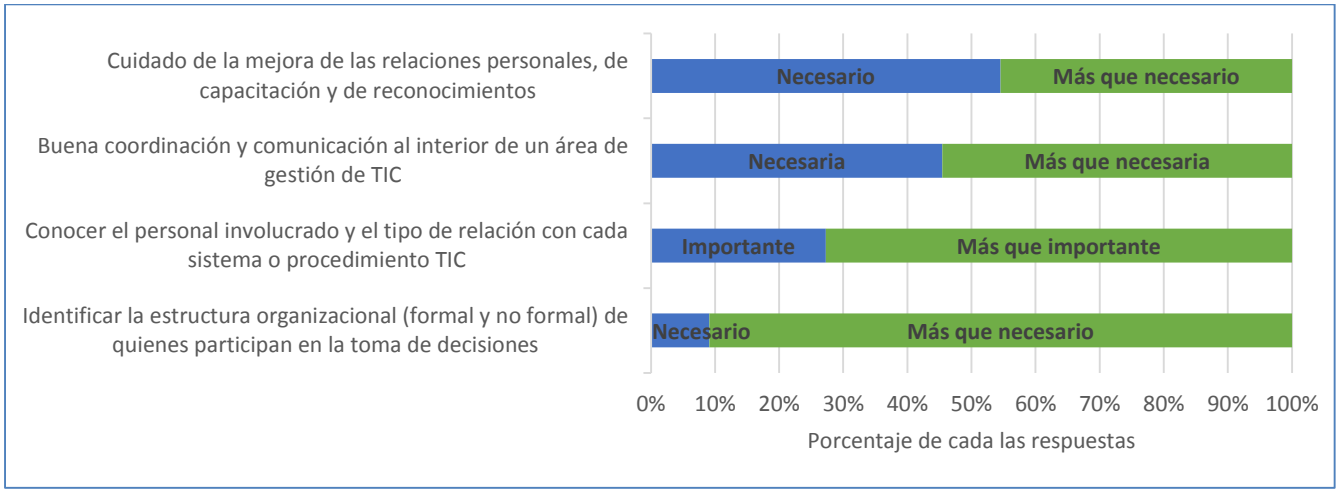


Figura 4.8. Porcentaje de respuestas a cuatro preguntas que evalúan el criterio de adecuado.

Con base en lo anterior se concluye que de forma general el sistema planteado en este trabajo es adecuado para un área de TIC, que sin duda se verá afectado su desempeño pero que es conveniente este tipo de acciones para prevenir otro riesgos que pueden tener consecuencias más graves, como se expresa en otras preguntas abiertas del instrumento. Por esto se menciona que para llevarlo a cabo es

necesario considerar las condiciones en lo que respecta a presupuestos y tiempo para realizar las actividades cotidianas en la consecución de sus objetivos. Se destaca también la opinión de expertos donde se apunta que es conveniente que la organización tenga un nivel de madurez alto para que estas acciones sean más compatibles con el área de gestión de TIC.

4.2.3 Factibilidad

Varias de las preguntas del cuestionario tenían por objetivo evaluar la factibilidad de aspectos particulares del modelo de atención de riesgos. De las respuestas que se reunieron se puede concluir que no tienen un mismo nivel de factibilidad y que las calificaciones que se dan a cada uno de estos aspectos varían de un experto a otro. La principal razón de esto es que cada área de gestión de TIC tiene características que la diferencian de las demás e incluso de ella misma en momentos diferentes, como se puede deducir de las respuestas a cuestiones abiertas que los mismos entrevistados dieron. Sin embargo es importante señalar que estas respuestas se agrupan en su mayoría en 2 opciones que los entrevistados contestaron. Se concluye, con base en la revisión de las opiniones de los consultados, que las actividades que se llevan a cabo en un área de gestión de TIC son compatibles con las ideas básicas del enfoque sistémico socio-técnico y que el llevarlas a cabo es *Medianamente factible* (figura 4.9); además se identifica con la pregunta 17 del instrumento que es entre *Medianamente factible* (54.5%) y *Factible* (45.5%) que en las actividades de la definición y aprobación de planes de atención a riesgos en TIC participen personas de niveles superiores en la estructura organizacional como se propone en el modelo, de lo que se concluye, con refuerzo de lo expresado en otras preguntas abiertas, que hay mayor probabilidad de que se les pueda convencer de que es necesaria su participación y apoyo en este tipo de cuestiones de prevención. Algo que es de llamar la atención es que en un área de tecnología, por contradictorio que pudiera parecer, cambiar las formas de trabajo arraigadas en favor de nuevos modelos de pensamiento es en general *Medianamente factible* con tendencia a *Poco factible* (figura 4.10); la razón de esto, a decir de los entrevistados, es la carga de actividades del día a día y la presión laboral por conseguir las metas fijadas que no dan espacio para efectuar o probar cambios radicales.

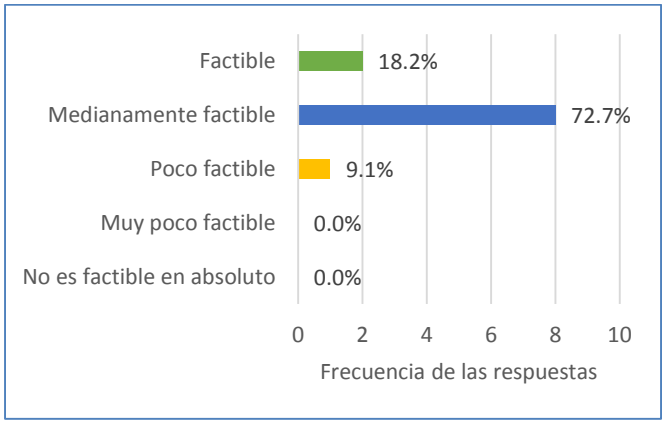


Figura 4.9. Respuestas a la pregunta 13 del cuestionario.

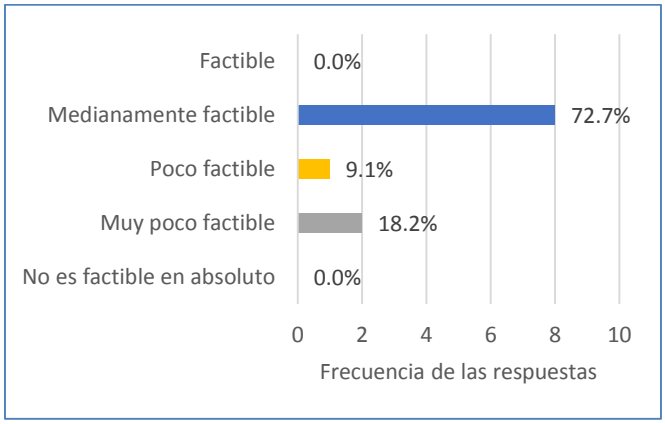


Figura 4.10. Respuestas a la pregunta 12 del cuestionario.

La factibilidad de aplicar en general el Sistema de Prevención de Crisis se evaluó directamente con la pregunta 21 del instrumento diseñado. Las opiniones se agrupan en 3 clases (figura 4.11). Dos de los expertos afirmaron que es *Poco factible* que se pueda realizar en un área de gestión de TIC, cinco lo consideraron *Medianamente factible* y los 4 restantes lo vieron *Factible* de realizar.

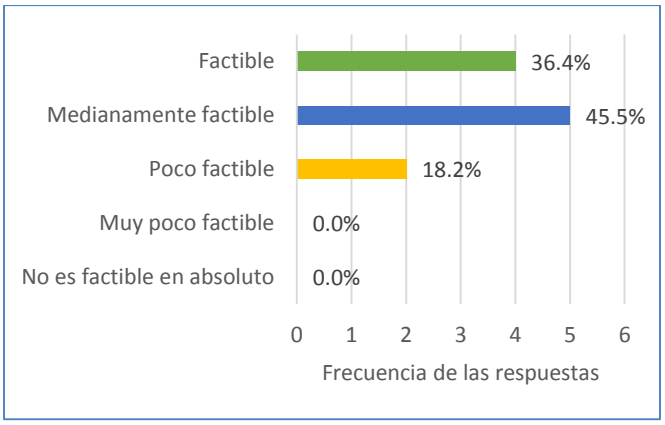


Figura 4.11. Respuestas a la pregunta 21 del cuestionario.

Con el análisis de todo el cuestionario se concluye nuevamente que esta variabilidad en las respuestas es porque los expertos consideran que la situación de cada área de gestión de TIC y de cada organización hace factible en distinto grado el llevarlo a cabo y no sólo por la disponibilidad de recursos financieros, de personal o de tiempo, sino incluso por las políticas bajo las que se rigen las organizaciones.

4.2.4 Mejoras

A lo largo del cuestionario se incluyeron algunas preguntas con el objetivo de conocer las mejoras que los expertos harían sobre el modelo en general o sobre una parte específica.

En lo que se refiere a la fase del Diagnóstico socio-técnico y su entorno se podría incorporar un módulo que permita profundizar en la capacidad actual del área de gestión de TIC para responder a las necesidades de la organización. La importancia de esta actividad radicaría en vislumbrar los riesgos ante una posible incapacidad actual o a largo plazo para cubrir las necesidades de TIC que la institución maneje o planeé con respecto a sus directrices, y que sin duda sería necesario atender. Las actividades de este nuevo diagnóstico en particular enlazarían el diagnóstico del *Sistema y su entorno* y el diagnóstico de *Desempeño y capacidades* explicados en el capítulo. Otra de las mejoras recomendadas se refiere a incluir un diagnóstico de satisfacción del personal de TIC, para evaluar el grado del gusto por las actividades que realiza, por trabajar en la institución, y el grado de satisfacción laboral entre jefes y subalternos. Si bien es cierto que este último punto se refiere brevemente en el módulo del *Diagnóstico de las condiciones de trabajo*, allí no se le da la importancia requerida. Este nuevo módulo

de *Diagnóstico de satisfacción* se puede incluir en el módulo general del diagnóstico de *Desarrollo organizacional*. A partir de otras recomendaciones es útil indicar específicamente, como parte del *Diagnóstico de desempeño de la gestión y de funciones,* que se realicen actividades de diagnóstico de la integración de manuales administrativos de operación y de generación de lecciones aprendidas. Uno más de los consejos para mejorar esta parte del sistema señala que es importante saber cuál es el grado de madurez de la organización, ya que este podría ser un factor clave para el comportamiento socio-técnico en el área de TIC o incluso determinar la certeza con la que las actividades se realizan. Entre las mejoras posibles, otra que atañe a la fase de diagnóstico del modelo y a la generación de los planes de atención de riesgo se refiere a la importancia de conocer el estado de los grupos de trabajo existentes en el área de gestión de TIC, de identificar a los tipos de grupos que existen y las personalidades de quienes los integran con el fin de identificar riesgos por las condiciones existentes en su interior, para detectar áreas de mejora en cada equipo y para optimizar su desempeño o disminuir o eliminar riesgos latentes o posibles de presentarse. Esto en particular se había abordado de forma parecida con el *Diagnóstico de la estructura organizacional* para saber quiénes eran los actores que participaban en la toma de decisiones, sin embargo este nuevo giro crea un diagnóstico muy importante que se debe de realizar por las razones recién expuestas.

Las recomendaciones con respecto a la fase de *Análisis general de riesgos* las recomendaciones van encaminadas a los criterios a considerar para la selección de riesgos para los cuales se deben desarrollar planes de atención. Todos los entrevistados respaldan la idea de considerar los sistemas críticos para la organización y para la selección de los riesgos tener en cuenta el impacto y la probabilidad de ocurrencia para decidir cuáles atender; algunos agregan que esta selección debe basarse en aspectos financieros y de gestión administrativos-presupuestales, en la calidad de los servicios afectados y los tiempos de recuperación. Recomiendan que en dichas ponderaciones participen los dueños de los procesos de TIC y la alta dirección, tal cual lo propone el *Sistema de planeación*. Un aspecto que no se considera en el *Sistema de Planeación* es la participación de terceros en la administración de las TIC, en este caso se hace notar que se debe considerar si los sistemas técnicos cuentan con soporte por parte de un proveedor relacionado y saber específicamente en qué consiste éste, la fecha de vencimiento, costos de renovación u otra información importante relacionada. Importa mucho al momento de asignar una prioridad el saber qué está cubierto por un tercero y que es lo que no. Por último apuntan que al momento de aplicar el modelo muy probablemente surgirán criterios de selección propios de la situación.

Entre las respuestas se hacen algunos comentarios con respecto a los pasos generales propuestos para el desarrollo de los planes de atención a riesgos. Éstos mencionan que es útil romper paradigmas establecidos, en rediseñar procedimientos acorde a las condiciones de las instituciones y no apegarse a un método definido o probado en circunstancias no necesariamente iguales a las que se viven (recursos, estructura organizacional, cultura laboral, idiosincrasia, condiciones físicas) sino hacer uno apropiado a la situación de la organización en el que aprecien resultados a mediano y largo plazo, con lo cual afirman que están bien los pasos como guía pero no como una obligación a seguir ya que cada

caso es único. Este comentario es bastante acertado y así se considera como esencia del modelo que por ser un sistema general para hacer planes de prevención tiene esta idea como parte de sus bases esenciales. Otra recomendación que resulta importante para los fines de este trabajo es considerar los planes como un proceso de mejora continua y plantear etapas en los planes para ir alcanzando los objetivos, inclusive en la estructura del modelo que se propone. Aportes como este último y otros referidos, como por ejemplo el asegurar que se cuenta con el personal adecuado en los tiempos correctos, los considera el sistema y se explican en el capítulo 3, sólo que no se proporcionó a los entrevistados todo el detalle del modelo dichas ideas se refirieron como mejoras. Sin embargo, bien es cierto que convendría hacerlos más evidentes o detallar más algunas acciones de las fases del modelo. Por otro lado están las opiniones que indican el utilizar alguna herramienta en particular e incluso dar ejemplos de su aplicación. En este sentido se prefirió no hacerlo en el modelo con el fin de mantener su generalidad, no limitarlo a técnicas particulares y para resaltar que las actividades particulares de cada área de TIC dependerán de cómo se manejen y de su situación. Un aspecto que se recomendó tener en cuenta como algo esencial en el desarrollo de los planes de atención a riesgos es el considerar el respaldo del área directiva de la institución a lo largo del proceso, pero sobre todo entre la generación de alternativas de acción y la especificación de actividades, para asegurar que se cuenta con la aprobación de quienes tienen en última instancia el poder de decisión sobre el *Sistema de Planeación*.

En cuanto a consideraciones necesarias para poder aplicar el *Sistema de Planeación*, la mayoría de los expertos refiere que es esencial contar en primer lugar con el apoyo de la alta dirección y como actividades de convencimiento recomiendan evidenciar fallos en la operación actual y las consecuencias que pueden presentarse si se ve afectada el área, así como detallar las áreas de oportunidad encontradas y los beneficios que se obtendrán al atenderlas ya sea a mediano o a largo plazo. Algunos expertos hacen énfasis en no todas las recomendaciones para las actividades que conformen los planes de eliminación, mitigación o respuesta a riesgos no serán aplicables en todas las organizaciones, pues las políticas internas y razones estructurales pueden ser muy rígidas o numerosas, como por ejemplo las normatividades sobres aspectos de TIC en el sector gubernamental.

Otro punto importante es hacer partícipes, en un grado coherente a la situación, al resto del personal que se verá afectado por el diseño de los planes ejecución de los planes, además de capacitarlos adecuadamente. De igual forma es necesario conseguir facilidades con respecto a las actividades habituales, por ejemplo en las fechas de entrega de compromisos o en el uso de recursos. Otra idea importante que se mencionó en los comentarios fue que sería conveniente indicar las condiciones mínimas que debería reunir la organización en cuanto a estructura o gobernabilidad para que el sistema sea funcional, ya que sólo se indica que la institución debe contar con un área formal para la gestión de TIC.

Entre las opiniones recabadas se hace énfasis en que se debe cuidar que la ejecución del plan no mengüé el desempeño en otras actividades del área de administración de TIC y se propone que lo ideal

sería manejarlo como un proyecto independiente y dedicar recursos financieros y humanos exclusivos a tales actividades.

Refiriéndose a la práctica del modelo en algunas recomendaciones se hace hincapié en que la planeación en particular de cada caso tiene que definir el momento justo para ejecutar las actividades, que los planes que se hagan con base en el modelo tienen que concluir sobre cómo se va a afectar al área de TIC en su rendimiento. De forma similar otras opiniones hacen énfasis en que el modelo debe de precisar un análisis de los grupos de trabajo porque de la manera en cómo estén constituidos y cómo se comporten depende el éxito de una implantación, y que incluso grupos de trabajo bien conformados en cuanto a capacidades e integrantes pueden potencializar el éxito. Como en otros puntos mencionados, también se da como opinión que existen mayores probabilidades de buenos resultados del modelo mientras la organización sea más madura y que tenga sus directrices bien definidas. En otros comentarios varios de los entrevistados indican que el modelo se puede llevar a cabo en conjunto con mecanismos de gestión de calidad como normas ISO e incluso prácticas para la gestión de servicios y procedimientos de TIC como ITIL o COBIT.

CONCLUSIONES

En la parte final del capítulo 1 se estableció el objetivo general de esta tesis:

> *"Desarrollar un Sistema de planeación para la prevención de crisis con origen socio-técnico en áreas que se dedican a la gestión de las Tecnologías de la Información y Comunicación, con base en los principios del enfoque socio-técnico y de la estructura organizacional."*

Con las actividades indicadas en este trabajo escrito se consiguió dicho objetivo. En el capítulo tres se define formalmente y se describe detalladamente el Sistema Planeación para la Prevención de Crisis socio-técnicas en áreas de TIC, primero grosso modo con el señalamiento de los módulos principales y los flujos de actividades a seguir y después de forma específica con el detalle de cada uno de ellos.

El sistema que se propone consiste de 4 etapas principales:

1. *Diagnóstico socio-técnico del sistema y su entorno*.
2. *Análisis general de riesgos*.
3. *Desarrollo de planes de eliminación o mitigación de riesgos y de respuesta a su materialización*.
4. *Monitoreo, evaluación y control de la ejecución*.

Este *Sistema de Planeación* se sustenta en los principios del enfoque socio-técnico y cuestiones de desarrollo organizacional, tratados en el capítulo dos de este trabajo escrito. Con base en ellos se especificaron las características del tipo de acciones que podrían integrar los planes de atención a riesgos, de tal manera que se cumplió con el objetivo implícito de utilizar e integrar estos conocimientos en el sistema. Cada una de las fases del modelo se diseñó, a partir de dicha teoría y de la experiencia personal, contemplando el funcionamiento general de un área donde se gestionan TIC, la forma en como están integradas, en cómo se llevan a cabo sus actividades y en las condiciones administrativas y organizacionales a las que se sujeta su funcionamiento. Con esto se cubrió la parte del objetivo que se refiere al área de aplicación. Es destacable que conforme se fueron estructurando y relacionando estos lineamientos, la idea de su aplicabilidad a áreas de una organización no dedicadas específicamente a

TIC fue siendo evidente, precisamente por el carácter socio-técnico en el que se sustenta. De forma general, varias partes del modelo pueden ser válidas para áreas administrativas de una organización haciendo ciertas modificaciones. Por ejemplo los diferentes tipos de diagnóstico no son restrictivos a áreas de tecnologías de la información, ya que sus sistemas objetivos pueden cambiarse de sistemas técnicos a procedimientos o sistemas burocráticos. Esto también aplica para el módulo de análisis general de riesgos. Las otras dos grandes etapas del sistema sí se sujetan más a las condiciones de un área de gestión de TIC por el tipo de actividades que las componen, los fines que persiguen los planes a generar y los elementos que ocupan como insumos.

Los expertos consultados señalan que el enfoque socio-técnico es poco tratado en investigaciones formales para su aplicación en áreas de gestión de TIC, y reconocen que es de gran importancia para el funcionamiento de un área que por lo general es analizada sólo desde el punto de vista técnico. Esto ya se adelantaba en lo tratado en el capítulo uno a partir de la revisión de la literatura formal existente respecto a la atención de crisis en organizaciones.

Si bien, el fin principal de este trabajo era la formulación del *Sistema de Planeación*, no era conveniente limitar los alcances hasta ese punto, sino que se debían ampliar para validarlo. Por lo cual se buscó la revisión por personas expertas en el tema de gestión de TIC, desde la perspectiva considerada en este trabajo. De esta forma se generaron otros productos, también de gran importancia en esta tesis: un instrumento de validación y el análisis de la información recabada. Con ellos se concluye sobre tres aspectos de interés:

- La utilidad del *Sistema de Planeación* para un área de gestión de TI.
- La compatibilidad con su forma de operación.
- La factibilidad de llevarlo a cabo y las mejoras que se le deben de hacer.

Así es posible afirmar que el *Sistema de planeación* es de gran utilidad para un área de gestión de TIC. Las opiniones concuerdan con la idea expresada en el capítulo uno, que afirma que es muy importante garantizar que las actividades que se realizan en su interior se lleven a cabo de manera adecuada pues contribuyen a conseguir los objetivos de la entidad a la que pertenecen y en algunos casos son imprescindibles por el negocio de la organización; por lo tanto es necesario contar con mecanismos que permitan asegurar su funcionamiento, como planes de recuperación de desastres. En un aspecto relacionado a esto último es donde los entrevistados encontraron una razón principal de la utilidad del modelo, ya que por lo general los planes que se tienen en departamentos de tecnología para atender crisis se enfocan en el restablecimiento de operaciones ante un evento inesperado que afecte sus actividades, y en el caso de esta tesis el plan es proactivo y no reactivo a situaciones que pueden generar una crisis en TIC. La utilidad que confieren los expertos entrevistados a este *Sistema de planeación* también se debe a que el tipo de riesgos que es de su interés son los que se presentan en un plano social propio de un área donde las actividades en su mayoría son técnicas y por consecuencia los planes de rescate y normas que los rigen de por lo general atienden este campo únicamente.

También se concluye que la compatibilidad y factibilidad de llevar a cabo las acciones propuestas para generar planes de atención a riesgos en un área de gestión de TIC depende de las condiciones de las entidades y de los departamentos de TIC, es decir, el *Sistema de Planeación* debe adaptarse a las condiciones de cada caso en particular. Factores como la disponibilidad de recursos humanos, financieros y de tiempo, así como las formas de operación propias del área de TIC y de la organización determinan lo adecuado de las actividades que se indican en el modelo y de las tareas que se proponen deberían de integrarse en los planes que se generen con él y las que corresponden al monitoreo de los mismos cuando se ejecuten.

Los resultados particulares para estos criterios de acuerdo con los expertos entrevistados, indican un nivel adecuado de compatibilidad del *Sistema de Planeación* y en su mayoría una factibilidad media y alta de poder implantarse en un departamento de gestión de TIC. Algo interesante en este sentido es que para llevar a cabo el tipo de planes como el sistema propuesto se tienen que afrontar otros retos más allá de lo racional y justificado del diseño del sistema y sus acciones, y de lo referente a lo operativo en la ejecución del plan; es necesario lograr un convencimiento y apoyo de quienes toman las decisiones de ejecutarlo y además buscar formas de que las metas cotidianas del área no dejen de cumplirse. De esta forma es posible concluir que los resultados para estos dos criterios son de la situación general actual, y que por el reconocimiento cada vez mayor de la importancia de las TIC en las organizaciones, estas circunstancias van a cambiar y se tendrá un panorama más favorecedor para adquirir nuevas formas de gestionar áreas de TIC, incluida la prevención.

Hay varias cuestiones por mejorar, precisar y modificar en una siguiente etapa de desarrollo, primero atendiendo las recomendaciones de quienes contestaron el instrumento. De dichas opiniones referidas en el último apartado del capítulo cuatro habrá que incluir o ampliar las especificaciones del *Sistema de Planeación* y algunas hacerlas explícitas en el modelo. Con dichos comentarios se confirma que existe un interés real de quienes están involucrados en estos temas de gestión de áreas de TIC y además que están de acuerdo con que la utilidad del modelo es amplia.

Hasta el momento se ha llevado a cabo una validación del *Sistema de Planeación* propuesto. El paso siguiente es su verificación mediante un caso de estudio. Para esto será necesario encontrar una organización que cuente con área de administración de TIC y que esté dispuesta a seguirlo. Es necesario precisar que antes de llevarlo a cabo será necesario hacer un análisis inicial de la entidad para planear cómo se llevará a cabo la intervención, estableciendo las necesidades en cuanto a recursos necesarios y definiendo un tiempo aproximado para llevarla a cabo. Se debe explicar claramente el alcance de la intervención a los dueños del sistema donde se intervendrá y demás interesados, así como plantearles la manera en que se les solicitará su apoyo durante la verificación. Durante la implantación deberá llevarse un registro de las decisiones tomadas, de los tiempos ocupados al realizar las tareas indicadas en cada uno de los módulos, de los resultados obtenidos y del comportamiento de quienes participan en las acciones que se llevarán a cabo. De igual forma será necesario llevar una bitácora de las situaciones no contempladas y la manera en cómo se les hizo frente.

Además del punto de vista de quien o quienes lleven a cabo la intervención es importante obtener la opinión de quienes laboran en el área de gestión de TIC incluyendo el jefe del departamento, también de la alta dirección o de quienes depende dicha área en la estructura organizacional, así como de las demás áreas o departamentos en la organización. Para reunir dicha información podría definirse un cuestionario o realizar entrevistas directas.

Las conclusiones de dicha intervención deberán desarrollarse al menos con respecto a los siguientes puntos base: la utilidad conseguida con la intervención, la facilidad de llevar a cabo las actividades propuestas, la cooperación del personal del área de gestión de TIC, los recursos y tiempos ocupados en la intervención, las dificultades encontradas para llevar a cabo los pasos del modelo y la manera en cómo se vio afectado el desempeño del área de gestión de TIC, mejoras recomendadas por quienes participan en la ejecución del *Sistema de Planeación*, el desempeño de quien dirija la intervención y de quienes participen en ella. Por último, con base en los resultados y conclusiones de la intervención se deberán hacer las modificaciones necesarias al *Sistema de Planeación*.

En lo que respecta al tema formativo, este trabajo es de gran valor porque permitió aplicar distintos conocimientos adquiridos durante la maestría, desde fundamentos teóricos de enfoques científicos para la definición de los sistemas involucrados y para estructurar el producto principal, hasta cuestiones más prácticas como herramientas para la generación del instrumento de validación, la manera de aplicarlo y de recabar la información. Estos conocimientos contribuyeron desde las primeras etapas de construcción de la tesis como tal, al principio para adquirir conocimientos a través de literatura formal sobre el tema de interés y después para ir delimitando y delineando la perspectiva sobre la que se atendería. Lo más importante en este sentido es que permitió dotar al trabajo que se desarrollaba del carácter de investigación a nivel de maestría y no sólo producir un trabajo profesionalizante; es decir, generar un producto de valor en el campo de la Ingeniería de Sistemas y no limitarse a la aplicación de conocimientos adquiridos en este rubro a un caso particular.

ANEXOS

Anexo I. Expertos que contestaron el instrumento de validación.

1. Alejandro Velázquez Mena.
   Departamento de Ingeniería en Computación, División de Ingeniería Eléctrica, Facultad de Ingeniería, UNAM.
   Jefe de la carrera de Ingeniería en Computación.
   Gestión del personal académico y planeación de horarios de asignaturas, gestión de proyectos externos e internos a la Facultad de Ingeniería.

2. César Arián Ortega Arias.
   Banco de México (BM).
   Responsable de infraestructura de cómputo.

3. Fernando Ballesteros Talavera.
   Centro Nacional de Prevención de Desastres (CENAPRED), SEGOB.
   Subdirector de Cómputo para la Prevención de Desastres.
   Coordinación de actividades de servicios informáticos que tiene a cargo la Subdirección de Cómputo del CENAPRED: Red LAN, Seguridad Informática, Desarrollo de Sistemas Informáticos, Administración de Servidores y Soporte Técnico.

4. José Ángel Haro Juárez.
   Poder Judicial de la Federación (PJF) / Consejo de la Judicatura Federal (CJF).
   Análisis, mejora, documentación de los procesos de las direcciones y órganos jurisdiccionales. Levantamiento de requerimientos, gestión de proyectos de TI, arquitectura de software, análisis, diseño y desarrollo de software.

5. Jorge A. Solano Gálvez.
   Laboratorio de Microsoft, División de Ingeniería Eléctrica, Facultad de Ingeniería, UNAM.
   Responsable de la administración del laboratorio de Microsoft y consultor por parte de la FI en proyectos externos.

6. Julio César Saynez Fabián.
   Gerencia de Operación de Fibra Óptica (GOFO), Comisión Federal de Electricidad (CFE).
   Administración de Base de Datos, Servidores Web.

7. Ma. Alejandra Zúñiga Medel.
   Centro Nacional de Prevención de Desastres (CENAPRED), SEGOB.
   Jefa de Departamento de Sistemas de Información sobre Riesgos.
   Administradora de servidores y aplicaciones de información geoespacial.

8. Óscar Zepeda Ramos
   Centro Nacional de Prevención de Desastres (CENAPRED), SEGOB.
   Director de Análisis y Gestión de Riesgos.
   Diseñar, desarrollar, implementar, evaluar y actualizar el Atlas Nacional de Riesgos (ANR).

9. Pablo Lorenzana Gutiérrez.
   Equipo de Respuesta a Incidentes de Seguridad en Cómputo (UNAM-CERT), DGTIC-UNAM.
   Auditorías tecnológicas y documentales apegadas a mejores prácticas de Seguridad de la Información.

10. Raúl Chora Ayuso.
    RDA, Teléfonos de México (TELMEX).
    Supervisión de equipamiento, fibra óptica para clientes empresariales. Administración de personal sindicalizado, administración de proveedores, equipamiento en central y cliente de dispositivos de infraestructura para enlazar, gestionar y liberar enlaces.

11. Tanya Arteaga Ricci.
    División de Ingenierías Civil y Geomática, Facultad de Ingeniería, UNAM.
    Jefa de la Unidad de Cómputo.
    Responsable y administradora de sistemas informáticos, servidores, red de datos y soporte técnico. Responsable del plan de Servicio Social y Becarios.

Anexo II. Instrumento de validación del Sistema de Planeación.

Evaluación de un modelo de planeación para la prevención de crisis socio-técnicas en TIC

De antemano le agradezco su tiempo y disposición para contestar esta encuesta.

El objetivo es conocer la opinión de expertos en la gestión de áreas de Tecnologías de la Información y Comunicación con respecto a un modelo de prevención de crisis con base en un enfoque sistémico socio-técnico y desarrollo organizacional. La información que obtenga por este medio me ayudará a mejorar esta propuesta que hago como parte de mi trabajo en la Maestría de Planeación en el Posgrado en Ingeniería de la UNAM.

Le solicito amablemente que antes de contestar estas preguntas vea el video donde explico el modelo que propongo. Dicho video se encuentra en la siguiente dirección de Internet: https://youtu.be/bI3_TYUwi7g. También lo incluyo al final de esta página.

Con gusto le haré llegar en forma electrónica los resultados de este trabajo en caso de que usted así lo desee.

Mis datos de contacto para asuntos relacionados a este trabajo son:
Ing. Heriberto García Ledezma
heriberto@fi-b.unam.mx
hega07@gmail.com

Sin más por el momento, nuevamente gracias.

Video donde explico el modelo del Sistema de planeción para la prevención de crisis sociotécnicas en TIC

Continue »

14% completed

Evaluación de un modelo de planeación para la prevención de crisis socio-técnicas en TIC

* Required

Fase A del modelo. Diagnóstico del sistema y su entorno.

1. ¿En qué grado es importante para un área de gestión de TIC establecer claramente sus directrices de acción (ya sea visión, misión, objetivos, metas o una combinación de ellas) y conocer las de las áreas con las que se relaciona a través los servicios o productos que proporciona?

Considere los siguientes valores para indicar su respuesta:
0 = No importa en absoluto
1 = Muy poco importante
2 = Poco importante
3 = Medianamente importante
4 = Importante
5 = Más que importante

*

	0	1	2	3	4	5	
No importa en absoluto	○	○	○	○	○	○	Más que importante

2. ¿En qué grado es necesario para llevar a cabo satisfactoriamente las actividades de un área de gestión de TIC, el identificar la estructura organizacional (formal y no formal) de quienes participan en la toma de decisiones en la entidad donde se encuentra y al interior de ella misma?

Considere los siguientes valores de la escala:
0 = No es necesario en absoluto
1 = Muy poco necesario
2 = Poco necesario
3 = Medianamente necesario
4 = Necesario
5 = Más que necesario

*

	0	1	2	3	4	5	
No es necesario en absoluto	○	○	○	○	○	○	Más que necesario

.....

3. ¿Qué tan útil es para cumplir satisfactoriamente la razón de ser de un área de gestión de TIC, el determinar cuáles son sus sistemas técnicos más importantes con base en las relaciones que tienen con otros sistemas internos y con otras áreas a la organización?

Considere los siguientes valores de la escala:
0 = No es útil en absoluto
1 = Muy poco útil
2 = Poco útil
3 = Medianamente útil
4 = Útil
5 = Más que útil

*

	0	1	2	3	4	5	
No es útil en absoluto	○	○	○	○	○	○	Más que útil

.....

4. Pensando en la identificación de riesgos por dependencia hacia determinados roles o personas. ¿Qué tan importante es conocer el personal involucrado con cada sistema o procedimiento de las áreas de administración de TIC y establecer el tipo de relación que tienen con el sistema, ya sea una relación de operación o uso, una relación de administración o supervisión, o una relación de mantenimiento o reparación o desarrollo?

Considere los siguientes valores de la escala:
0 = No importa en absoluto
1 = Muy poco importante
2 = Poco importante
3 = Medianamente importante
4 = Importante
5 = Más que importante

*

	0	1	2	3	4	5	
No es importante en absoluto	○	○	○	○	○	○	Más que importante

.....

5. ¿Qué tan probable es que una sobrecarga de responsabilidades en las personas que realizan actividades de operación o gestión de TIC pueda generar un riesgo para el desarrollo adecuado del área?

Considere los siguientes valores de la escala:
0 = 0%
1 = 20%
2 = 40%
3 = 60%
4 = 80%
5 = 100%.

*

	0	1	2	3	4	5	
0%	○	○	○	○	○	○	100%

.....

6. ¿Qué tan útil es para un área de administración de TIC tener un registro sobre el desarrollo de las actividades al interior de las áreas de TIC y de los sistemas que allí se manejan para identificar las causas de gestión y/o desempeño por las que la actividad primaria ha estado a punto de no conseguirse o no se ha conseguido?

Considere los siguientes valores de la escala:
0 = No es útil en absoluto
1 = Muy poco útil
2 = Poco útil
3 = Medianamente útil
4 = Útil
5 = Más que útil

*

	0	1	2	3	4	5	
No es útil en absoluto	○	○	○	○	○	○	Más que útil

.....

7. ¿En qué medida es necesaria una buena coordinación y comunicación entre las personas que conforman un área de gestión y operación de TIC para realizar sus actividades de forma adecuada?

Considere los siguientes valores de la escala:
0 = No es necesaria en absoluto
1 = Muy poco necesaria
2 = Poco necesaria
3 = Medianamente necesaria
4 = Necesaria
5 = Más que necesaria

*

	0	1	2	3	4	5	
No es necesaria en absoluto	○	○	○	○	○	○	Más que necesaria

.....

8. Para llevar a cabo satisfactoriamente las actividades de un área de TIC, ¿En qué grado considera necesario que se cuiden aspectos de mejora en las relaciones personales al interior del área, de la capacitación del personal y de reconocimiento de su trabajo?

Considere los siguientes valores de la escala:
0 = No es necesario en absoluto
1 = Muy poco necesario
2 = Poco necesario
3 = Medianamente necesario
4 = Necesario
5 = Más que necesario

*

	0	1	2	3	4	5	
No es necesario en absoluto	○	○	○	○	○	○	Más que necesario

9. Con la primera fase del modelo que propongo se pretende diagnosticar la situación del área de gestión de TIC con respecto a su entorno en la institución o empresa a la que pertenece y con respecto a los sistemas y personas que la conforman. Este diagnóstico analiza cómo la parte social involucrada puede afectar la parte técnica.
Con base en su experiencia en gestión de TIC desde el punto de vista técnico, administrativo y de convivencia en sus actividades con otras personas del área, ¿qué actividades o consideraciones agregaría o modificaría en esta etapa para mejorar los resultados del tipo de diagnóstico propuesto?

*

« Back Continue »

42% completed

Evaluación de un modelo de planeación para la prevención de crisis socio-técnicas en TIC

Fase B del modelo. Análisis general de riesgos.

10. En la segunda etapa del modelo se analizan los resultados de los diagnósticos de la fase previa y se asume que no es posible atender todos los riesgos identificados. Como factores de selección de los riesgos a atender se propone considerar a los que se refieren a los sistemas o actividades del área de gestión de TIC que son importantes para las actividades esenciales de la organización y tomar en cuenta el impacto y la probabilidad de ocurrencia que tiene cada uno.
¿En un área de gestión de TIC es necesario hacer alguna consideración diferente para la selección de riesgos a atender? De ser así, ¿cuál sería?

« Back Continue »

57% completed

Powered by Google Forms

This content is neither created nor endorsed by Google.
Report Abuse - Terms of Service - Additional Terms

Evaluación de un modelo de planeación para la prevención de crisis socio-técnicas en TIC

* Required

Fase C del modelo. Desarrollo del plan de prevención.

11. Las actividades que se diseñen para afrontar los riesgos deben considerar una o más acciones acciones de los siguientes tipos:

- Intervenciones relativas a los procesos humanos con respecto a sus comportamientos y a los medios para lograr sus tareas y alcanzar sus objetivos. Por ejemplo, resolución de problemas de relaciones laborales, capacitación, estudios de realimentación y coaching.
- Intervenciones tecno-estructurales que buscan reconciliar consideraciones con respecto a la estructura y tecnología. Se propone el uso de organizaciones colaterales, sistemas de aprendizaje en paralelo, equipos semi-autónomos, por ejemplo.
- Intervención en la administración de recursos humanos. Disposición de recursos humanos (Cambio de personal).

Explique qué tan compatible y factible es el llevar a cabo este tipo de acciones con las condiciones en que se desarrollan las actividades en un área de gestión de TIC.

*

12. Entre las acciones para evitar riesgos se recomienda cambiar paradigmas arraigados en la forma de trabajo, (aprender y desaprender modelos de pensamiento en favor de nuevos) además de que las propuestas deben orientarse a una solución en la que se busca actuar sobre las causas que originan las fallas y no sólo corregir los errores
¿Qué tan factible es que se puedan llevar a cabo en un área de gestión de TIC acciones con estas características?

Considere los siguientes valores de la escala:
0 = No es factible en absoluto
1 = Muy poco factible
2 = Poco factible
3 = Medianamente factible
4 = Factible

*

	0	1	2	3	4	
No es factible en absoluto	○	○	○	○	○	Factible

.....

13. Una característica importante que se propone para evitar la aparición de riesgos en el área de gestión de TIC es que las actividades que se hagan al interior se diseñen con base en las seis características propuestas por el instituto Tavistock para garantizar la satisfacción de los trabajadores. Algunos aspectos del enfoque socio-técnico que se proponen para el diseño de actividades encaminadas a la prevención de riesgos son:

- Las actividades al interior del área de gestión de TIC deben ser demandantes, representar un reto para los trabajadores y proveer un continuo aprendizaje.
- Los individuos deben contar con una zona, al menos pequeña, de toma de decisiones.
- Se debe proporcionar reconocimiento y apoyo social para el individuo.
- Las tareas que realiza el trabajador y/o el producto que contribuye a generar debe estar relacionado con su vida fuera del lugar de trabajo.
- El trabajo debe ser visto como algo que contribuye a conseguir un futuro deseado.

¿Qué tan factible es que estas medidas se tomen en cuenta para el diseño de nuevas actividades y/o modificación de las existentes al interior del área de gestión de TIC?

Considere los siguientes valores de la escala:
0 = No es factible en absoluto
1 = Muy poco factible
2 = Poco factible
3 = Medianamente factible
4 = Factible

*

	0	1	2	3	4	
No es factible en absoluto	○	○	○	○	○	Factible

14. Los riesgos pueden generarse por factores técnicos, humanos, administrativos o las combinaciones de ellos. Para el desarrollo de los planes de eliminación, mitigación o de respuesta al riesgo se proponen las siguientes actividades:

1. Ubicar el elemento, sistema o actividad donde puede materializarse el riesgo.
2. Identificar la causa del riesgo.
3. Idear alternativas de solución y bajo la consideración de las condiciones o restricciones del área de TIC o de la institución misma seleccionar alguna de ellas para diseñar el plan respectivo.
4. Diseñar las actividades que conformen la alternativa seleccionada.
5. Calendarización de actividades.
6. Definir indicadores para verificar que se alcanzan los objetivos.

¿Qué tan de acuerdo están con estas recomendaciones?

Considere los siguientes valores de la escala:
0 = No estoy de acuerdo en absoluto
1 = Poco de acuerdo
2 = Medianamente de acuerdo
3 = De acuerdo

*

	0	1	2	3	
No estoy de acuerdo en absoluto	○	○	○	○	De acuerdo

15. ¿Qué mejoras o cambios haría a los pasos indicados en la pregunta anterior?

« Back Continue »

71% completed

Powered by Google Forms

This content is neither created nor endorsed by Google.
Report Abuse - Terms of Service - Additional Terms

Evaluación de un modelo de planeación para la prevención de crisis socio-técnicas en TIC

* Required

Fase D del modelo. Monitoreo, evaluación y control de la ejecución.

16. Se propone que de forma simultánea a la implantación del plan se lleve a cabo el monitoreo de las variables que indican si se presenta el riesgo. En caso de que se superen los valores límite se detendrá la ejecución del plan de eliminación o mitigación del riesgo y se pondrá en marcha de forma inmediata el Plan de respuesta a la materialización del riesgo.
¿Qué tan factible es llevar a cabo este monitoreo de variables para los sistemas, desempeño y relaciones laborales y actividades presentes en un área de gestión de TIC?

Considere los siguientes valores de la escala:
0 = No es factible en absoluto
1 = Muy poco factible
2 = Poco factible
3 = Medianamente factible
4 = Factible

*

	0	1	2	3	4	
No es factible en absoluto	○	○	○	○	○	Factible

17. En la definición y aprobación de planes se recomienda que participen al menos el administrador del área de TIC, el responsable inmediato superior en la estructura organizacional, y de ser conveniente, quienes desempeñan actividades relacionadas directamente con el riesgo en cuestón. Ya sea para hacer actividades desde el diagnóstico, replantear riesgos a atender o incluso cambiar o rediseñar planes de acción, según la situación presente.
Considerando a los participantes que de acuerdo a la situación de su área de TIC deben intervenir en la planeación, ¿qué tan factible considera que es llevar a cabo esta actividad continuamente?

Considere los siguientes valores de la escala:
0 = No es factible en absoluto
1 = Muy poco factible
2 = Poco factible
3 = Medianamente factible
4 = Factible

*

	0	1	2	3	4	
No es factible en absoluto	○	○	○	○	○	Factible

« Back Continue »

85% completed

Powered by Google Forms

This content is neither created nor endorsed by Google.
Report Abuse - Terms of Service - Additional Terms

Evaluación de un modelo de planeación para la prevención de crisis socio-técnicas en TIC

* Required

Aspectos generales

18. Un aspecto importante del enfoque socio-técnico es que considera una mejora en los factores sociales y técnicos, y aunque su propuesta no considera que dichos factores se deben atender de forma equitativa, sí considera importante lograr una armonía en dichos elementos y con ello mejorar el desempeño.
¿En qué medida considera necesario para llevar a cabo las actividades satisfactoriamente de un área de TIC que se tenga una armonía entre elementos técnicos y sociales?

Considere los siguientes valores de la escala:
0 = No es necesario en absoluto
1 = Muy poco necesario
2 = Poco necesario
3 = Medianamente necesario
4 = Necesario
5 = Más que necesario

*

	0	1	2	3	4	5	
No es necesario en absoluto	○	○	○	○	○	○	Más que necesario

19. Como parte del enfoque socio-técnico, los planes de mitigación, eliminación o de respuesta a la materialización de un riesgo consisten de acciones en sistemas técnicos, en la cultura organizacional, y de los procedimientos de trabajo del área de gestión de TIC. Considerando las condiciones y requerimientos de operación habituales de un área de gestión de TIC (tiempo disponible, recursos humanos capacitados, recursos financieros y herramientas que se emplean, por ejemplo).
¿Qué tan factible es llevar a cabo acciones de este tipo en un área de gestión de TIC sin que se vea disminuida su eficiencia?

Considere los siguientes valores de la escala:
0 = No es factible en absoluto
1 = Muy poco factible
2 = Poco factible
3 = Medianamente factible
4 = Factible

*

	0	1	2	3	4	
No es factible en absoluto	○	○	○	○	○	Factible

20. Considerando su área de gestión de TIC y las otras áreas de la organización, ¿qué necesitaría principalmente para llevar a cabo las actividades indicadas en modelo propuesto del Sistema de planeación para la prevención de crisis socio-técnicas en TIC?

*

21. De forma general, ¿en qué grado considera factible aplicar este Sistema de planeación para la prevención de crisis socio-técnicas en TIC?

Considere los siguientes valores de la escala:
0 = No es factible en absoluto
1 = Muy poco factible
2 = Poco factible
3 = Medianamente factible
4 = Factible

*

	0	1	2	3	4	
No es factible en absoluto	○	○	○	○	○	Factible

.....

22. ¿Para un área de gestión de TIC qué tan necesario es tener un plan de prevención de crisis en general?

Considere los siguientes valores de la escala:
0 = No es necesario en absoluto
1 = Muy poco necesario
2 = Poco necesario
3 = Medianamente necesario
4 = Necesario
5 = Más que necesario

*

	0	1	2	3	4	5	
No es necesario en absoluto	○	○	○	○	○	○	Más que necesario

.....

23. Considerando a la cultura organizacional como las experiencias, hábitos, creencias y valores compartidos por personas en una institución y que determinan la forma en cómo se relacionan y desempeñan sus actividades, ¿para un área de gestión de TIC qué tan necesario es tener un plan de prevención con causas en aspectos de cultura organizacional?

Considere los siguientes valores de la escala:
0 = No es necesario en absoluto
1 = Muy poco necesario
2 = Poco necesario
3 = Medianamente necesario
4 = Necesario
5 = Más que necesario

*

	0	1	2	3	4	5	
No es necesario en absoluto	○	○	○	○	○	○	Más que necesario

24. Además de lo ya indicado en respuestas previas ¿Qué otras recomendaciones haría para mejorar el modelo propuesto de forma general o en cada una de sus fases?

*

25. ¿Considera que este modelo del Sistema de planeación para la prevención de crisis socio-técnicas es útil para un área de administración de TIC? Por favor, explique su respuesta.

*

26. En caso de que desee hacer algún comentario extra sobre este cuestionario o sobre el trabajo en sí mismo, por favor hágalo en el siguiente campo.

« Back Submit

100%: You made it.

Never submit passwords through Google Forms.

REFERENCIAS

Ackoff, R. (1971). Toward a system of systems concepts. *Management Science*, *17*(11), 661-671. Recuperado a partir de http://proquest.umi.com.ezp-prod1.hul.harvard.edu/pdf/8f53c1c2729a66112dedc0bcd2ff7d6e/1279223398//share4/pqimage/pqirs102v/20100715151953697/21790/out.pdf

Aini, M. S., & Fakhrul-Razi, A. (2010). Development of socio-technical disaster model. *Safety Science*, *48*(10), 1286-1295. doi:10.1016/j.ssci.2010.04.007

Alexander, D. (2005). Towards the development of a standard in emergency planning. *Disaster Prevention and Management*, *14*(2), 158-175. doi:10.1108/09653560510595164

Alpaslan, C. M., Green, S. E., & Mitroff, I. I. (2009). Corporate Governance in the Context of Crises: Towards a Stakeholder Theory of Crisis Management. *Journal of Contingencies and Crisis Management*, *17*(1), 38-49. doi:10.1111/j.1468-5973.2009.00555.x

Antonio, B., & Gaudenzi, B. (2013). *Risk Management*. Milano: Springer Milan. doi:10.1007/978-88-470-2531-8

Argyris, C., & Schön, D. A. (1978). *Organizational Learning: A Theory of Acton Perspective*. Addison-Wesley.

Ashcroft, L. S. (1997). Crisis management – public relations, *12*(5), 325-332.

Asociación Mexicana de la Industria de Tecnologías de Información A.C., Instituto Mexicano para la Competitividad A.C., & Select Estrategia A.C. (2013). *Mapa de ruta 2025 para transformar a México a través de las Tecnologías de la Información y Comunicaciones*. México, D.F. Recuperado a partir de http://imco.org.mx/wp-content/uploads/2013/5/mapaderuta2025_sec.pdf

Bozeman, B. (2011). The 2010 BP Gulf of Mexico oil spill: Implications for theory of organizational disaster. *Technology in Society*, *33*(3-4), 244-252. doi:10.1016/j.techsoc.2011.09.006

Bravo, L., García, F., Hernández, M. L., López, C. E., Furlong, M. M., Isario, L., & Galván, N. L. (2008). Análisis de las Tecnologías de la Información y de la Comunicación en México. Recuperado a partir de http://www.paginaspersonales.unam.mx/files/150/TIC_en_Mexico.pdf

Carmeli, A., & Schaubroeck, J. (2008). Organisational Crisis-Preparedness: The Importance of Learning from Failures. En *Long Range Planning* (Vol. 41, pp. 177-196). doi:10.1016/j.lrp.2008.01.001

Chapman, J. (2005). Predicting technological disasters: mission impossible? *Disaster Prevention and Management*, *14*(3), 343-352. doi:10.1108/09653560510605009

de Rosnay, J. (1979). *Macroscope*. Recuperado a partir de http://www.appreciatingsystems.com/wp-content/uploads/2011/05/The-Macroscope.pdf

Edmonson, A., & Moingeon, B. (1999). Learning, Trust and Organizational Change: Contrasting Models of Intervention in Organizational Behaviour. En Sage (Ed.), *Organization Learning and the Learning Organization.* (pp. 157-175). London.

Emery, F., & Trist, E. (1965). The causal texture of organizational environments. *Human relations*, (1965), 7-20. Recuperado a partir de http://www.pbookshop.com/media/filetype/2/22/22a/20110412180228.pdf

Foddy, W., & Mantle, J. (1994). Constructing Questions for Interviews and Questionnaires – Theory and practice in social research. *Physiotherapy*. doi:10.1016/S0031-9406(10)61110-8

Forrester, J. (1968). Principles of systems: text and workbook. Recuperado a partir de http://www.sidalc.net/cgi-bin/wxis.exe/?IsisScript=LIBROS.xis&method=post&formato=2&cantidad=1&expresion=mfn=003840

García, H. (2015a). Evaluación de un modelo de planeación para la prevención de crisis socio-técnicas en TIC. Recuperado 24 de junio de 2015, a partir de https://docs.google.com/forms/d/1omQGn0JvjVrNuhR5GbpiLcG3HH8eTNwP2YHXAmhg0fE/viewform

García, H. (2015b). Exposición - YouTube. *Youtube*. Recuperado 24 de junio de 2015, a partir de https://www.youtube.com/watch?v=bI3_TYUwi7g

Gardner, R. M., & GRID Consortium. (2007). A Survey of ICT Vulnerabilities of Power Systems and Relevant Defense Methodologies. En *2007 IEEE Power Engineering Society General Meeting* (pp. 1-8). IEEE. doi:10.1109/PES.2007.385713

Gelman, O., & Macías, S. (1983). Metodología para la elaboración de planes de emergencia, 27.

Gelman, O., & Negroe, G. (1982). La planeación como un proceso básico de conducción. *Revista de la Academia Nacional de Ingeniería*, *1*(4), 253-270. Recuperado a partir de

http://biblat.unam.mx/en/revista/revista-de-la-academia-nacional-de-ingenieria/articulo/la-planeacion-como-un-proceso-basico-de-conduccion

Hernantes, J., Rich, E., Laugé, A., Labaka, L., & Sarriegi, J. M. (2013). Learning before the storm: Modeling multiple stakeholder activities in support of crisis management, a practical case. *Technological Forecasting and Social Change*, *80*(9), 1742-1755. doi:10.1016/j.techfore.2013.01.002

Hovden, J., Albrechtsen, E., & Herrera, I. A. (2010). Is there a need for new theories, models and approaches to occupational accident prevention? *Safety Science*, *48*(8), 950-956. doi:10.1016/j.ssci.2009.06.002

Information Technology Infrastructure Library. (2011). ITIL Glossaries | ITIL®. Recuperado a partir de http://www.itil-officialsite.com/InternationalActivities/ITILGlossaries_2.aspx

Instituto Mexicano de Ejecutivos de Finanzas, A. C. (2007). *Tecnologías de Información y Comunicaciones para la Competitividad*. (IMEF, Ed.) (1a ed.). México: IMEF. Recuperado a partir de http://www.elsotano.com/libro-tecnologias-de-informacion-y-comunicaciones-para-la-competitividad-pd-10268877

Instituto Nacional de Estadística y Geografía. (2015). Estadística. Ciencia y Tecnología. Recuperado 18 de junio de 2015, a partir de http://www3.inegi.org.mx/sistemas/temas/default.aspx?s=est&c=19007

International Telecommunication Union. (2013a). About ITU. Recuperado a partir de http://www.itu.int/en/about/Pages/overview.aspx

International Telecommunication Union. (2013b). *Medición de la Sociedad de la Información 2013. Resumen ejecutivo.* Geneva Switzerland: UIT.

International Telecommunication Union. (2014). *Measuring the Information Society Report 2014*. Geneva Switzerland. Recuperado a partir de https://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2013/https://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2014/MIS2014_without_Annex_4.pdf

International Telecommunication Union. (2015). ITU: Committed to connecting the world. Recuperado 29 de octubre de 2015, a partir de http://www.itu.int/en/pages/default.aspx

ISO/IEC-IEEE. (2008). ISO/IEC 12207:2008. En ISO/IEC-IEEE (Ed.), .

Jackson, M. C. (2000). *Systems approaches to management*. (K. Academic/Plenum, Ed.). New York. Recuperado a partir de http://link.springer.com/content/pdf/10.1007/b100327.pdf

Jaques, T. (2007). Issue management and crisis management: An integrated, non-linear, relational construct. *Public Relations Review*, *33*(2), 147-157. doi:10.1016/j.pubrev.2007.02.001

Jaques, T. (2010). Embedding issue management as a strategic element of crisis prevention. *Disaster Prevention and Management*, *19*(4), 469-482. doi:10.1108/09653561011070385

Khidzir, N. Z., Mohamed, A., & Arshad, N. H. (2010). Information security risk factors: Critical threats vulnerabilities in ICT outsourcing. En *2010 International Conference on Information Retrieval & Knowledge Management (CAMP)* (pp. 194-199). IEEE. doi:10.1109/INFRKM.2010.5466918

Khodarahmi, E. (2009). Crisis management. *Disaster Prevention and Management*, *18*(5), 523-528. doi:10.1108/09653560911003714

Kovoor-Misra, S., Zammuto, R. F., & Mitroff, I. I. (2000). Crisis Preparation in Organizations. *Technological Forecasting and Social Change*, *63*(1), 43-62. doi:10.1016/S0040-1625(99)00049-9

Lalonde, C. (2011). Managing crises through organisational development: a conceptual framework. *Disasters*, *35*(2), 443-64. doi:10.1111/j.1467-7717.2010.01223.x

Lee, J., Woeste, J. H., & Heath, R. L. (2007). Getting ready for crises: Strategic excellence. *Public Relations Review*, *33*(3), 334-336. doi:10.1016/j.pubrev.2007.05.014

Manion, M., & Evan, W. M. (2002). Technological catastrophes: their causes and prevention. *Technology in Society*, *24*(3), 207-224. doi:10.1016/S0160-791X(02)00005-2

Medikonda, B. S., & Ramaiah, P. S. (2014). Software Safety Analysis to Identify Critical Software Faults in Software-Controlled Safety-Critical Systems (pp. 455-465). doi:10.1007/978-3-319-03095-1_48

Mitroff, I., & Alpaslan, M. (2003). *Preparing for evil*. Recuperado a partir de http://www.visitmyphilippines.com/images/ads/aa7aeca3ce9ab73291f2337e6c4a072b.pdf

Mitroff, I. I. (2004). Think like a sociopath, act like a saint. *Journal of Business Strategy*, *25*(5), 42-53. doi:10.1108/02756660410558933

Mitroff, I. I., & Anagnos, G. (2000). *Managing Crises Before They Happen: What Every Executive Needs to Know About Crisis Management*. AMACOM. Recuperado a partir de http://www.amazon.com/Managing-Crises-Before-They-Happen/dp/0814405630

Morrisey, G. L. (1996). Capítulo 2 ¿Qué cosa? Resultados planeados, ¡claro! En P.-H. Hispanoamericana (Ed.), *Planeación táctica: produciendo resultados en corto plazo.* (1.ª ed., p. 133). Recuperado a partir de http://www.sidalc.net/cgi-bin/wxis.exe/?IsisScript=BAC.xis&method=post&formato=2&cantidad=1&expresion=mfn=040590

Observatorio para la Sociedad de la Información en Latinoamérica y el Caribe. (2004). El estado de las estadísticas sobre Sociedad de la Información en los Institutos Nacionales de Estadística de América Latina y el Caribe. Recuperado a partir de http://www.itu.int/wsis/stocktaking/docs/activities/1102712635/statistics-es.pdf

Panteli, M. (2013). *IMPACT OF ICT RELIABILITY AND SITUATION AWARENESS ON POWER SYSTEM BLACKOUTS*.

Panteli, M., & Kirschen, D. S. (2011). Assessing the effect of failures in the information and communication infrastructure on power system reliability. En *2011 IEEE/PES Power Systems Conference and Exposition* (pp. 1-7). IEEE. doi:10.1109/PSCE.2011.5772565

Pearson, C. M., & Clair, J. A. (1998). Reframing crisis management. *Academy of Management Review*, *23*(1), 17. Recuperado a partir de http://www.jstor.org/stable/259099

Pearson, C. M., Misra, S. K., Clair, J. A., & Mitroff, I. I. (1997). Managing the unthinkable. *Organizational Dynamics*, *26*(2), 51-64. doi:10.1016/S0090-2616(97)90005-X

Pollard, D., & Hotho, S. (2006). Crises, scenarios and the strategic management process. *Management Decision*, *44*(6), 721-736. doi:10.1108/00251740610673297

Presidencia de la República de México. (2013). Objetivos de la Estrategia Digital Nacional | Presidencia de la República. Recuperado a partir de http://www.presidencia.gob.mx/objetivos-de-la-estrategia-digital-nacional/

Pressman, R. S. (2010). *Ingeniería de software. Un enfoque práctico*. (McGraw Hill Interamericana Editores, Ed.) (7.ª ed.). México, D.F.

Quijano, Á. del S. C. (2007). *La aceptación de tecnologías de información y cambio organizacional.* Universidad Nacional Autónoma de México, Facultad de Ingeniería. Recuperado a partir de http://132.248.9.195/pd2008/0625766/Index.html

Rowe, W. D. (1977). *Anatomy of risk*. John Wiley.

Saga, V. L., & Zmud, R. W. (1994). Nature and determinants of IT acceptance, routinization, and infusion. En *Diffusion, Transfer and Implementation of Information Technology* (pp. 67-86). Publ by Elsevier Science Publishers B.V. Recuperado a partir de http://www.scopus.com/inward/record.url?eid=2-s2.0-0027989018&partnerID=tZOtx3y1

Sagasti, F. R., & Mitroff, I. I. (1973). Operations research from the viewpoint of general systems theory. *Omega*, *1*(6), 695-709. Recuperado a partir de http://www.sciencedirect.com/science/article/pii/030504837390087X

Sánchez, G. (2003). *Técnicas participativas para la planeación: procesos breves de intervención.* (Fundación ICA, Ed.). México, D.F.: Fundación ICA.

Shaluf, I. M. (2007). An overview on the technological disasters. *Disaster Prevention and Management*, *16*(3), 380-390. doi:10.1108/09653560710758332

Shaluf, I. M., Ahmadun, F., Said, A. M., Mustapha, S., & Sharif, R. (2002). Technological man-made

disaster precondition phase model for major accidents. *Disaster Prevention and Management*, *11*(5), 380-388. doi:10.1108/09653560210453425

Simola, S. (2005). Concepts of Care in Organizational Crisis Prevention. *Journal of Business Ethics*, *62*(4), 341-353. doi:10.1007/s10551-005-3069-9

Smallman, C. (1995). Risk and organizational behaviour : a research model.

Tarn, J. M., Wen, H. J., & Shih, S. C. (2008). A theoretical perspective of man-made system disasters: Social-technical analysis and design. *Disaster Prevention and Management*, *17*(2), 256-280. doi:10.1108/09653560810872550

Tavistock Institute. (1972). Characteristics of Socio-Technical Systems. *Design of Jobs*, *11*, 157-186. Recuperado a partir de http://moderntimesworkplace.com/archives/ericsess/sessvol2/STS_Emery.pdf

Tawfik, M. (2000). *Informe mundial sobre la comunicación y la información*. (M. Tawfik, G. Bartagnon, & Y. Courier, Eds.). Editorial CSIC - CSIC Press. Recuperado a partir de https://books.google.com.mx/books?hl=es&lr=&id=QqD1lSwWqGcC&oi=fnd&pg=PA14&dq=Informe+mundial+sobre+la+comunicaci%C3%B3n+y+la+informaci%C3%B3n&ots=u5FXvllAex&sig=0Qobl2LwFeax8Ao43h582xI_-S8

The World Bank. (2015). Information & Communications Technologies - ICT Glossary Guide. Recuperado a partir de http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/0,,contentMDK:21035032~menuPK:282850~pagePK:210058~piPK:210062~theSitePK:282823~isCURL:Y,00.html#I

Tombs, S., & Smith, D. (1995). Corporate Social Responsibility and Crisis Management: the democratic organisation and crisis prevention. Journal Of Contingencies & Crisis Management.

Turner, B. A. (1976). THE DEVELOPMENT OF DISASTERS-A SEQUENCE MODEL FOR THE ANALYSIS OF THE ORIGINS OF DISASTERS. *The Sociological Review*, *24*(4), 753-774. doi:10.1111/j.1467-954X.1976.tb00583.x

Watkins, M. D., & Bazerman, M. H. (2003). Predictable Surprises: The Disasters You Should Have Seen Coming. *Harvard Business Review*, *81*(3), 72-80. doi:10.5465/AMR.2006.19379633

Wells, G. (1978). *How to Communicate*. New York: McGraw-Hill.

World Economic Forum. (2015). Report Highlights of NRI. Recuperado a partir de http://reports.weforum.org/global-information-technology-report-2015/report-highlights/

World Economic Forum, & INSEAD. (2015). *The Global Information Technology Report 2015*. Geneva Switzerland. Recuperado a partir de http://www3.weforum.org/docs/WEF_GITR2015.pdf

Zuppo, C. M. (2012). Defining ICT in a Boundaryless World : The Development of a Working Hierarchy. *International Journal of Managing Information Technology*, *4*(3), 13-22. doi:10.5121/ijmit.2012.4302