PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE AMBATO

SERÉIS MIS TESTIGOS

DEPARTAMENTO DE INVESTIGACION, POSTGRADOS Y AUTOEVALUACION

TEMA:

"GESTION DE RIESGOS INFORMATICOS EN LA INDUSTRIA DE CARROCERIAS METALICAS EN LA PROVINCIA DEL TUNGURAHUA"

Tesis de grado previo a la obtención del título de Maestría en Gerencia Informática con mención en Redes y Desarrollo de Software.

AUTOR

GERMAN MARCELO SALAZAR MOSQUERA

DIRECTOR

Ing. Msc. Patricio Medina.

Ambato – Ecuador

Enero, 2009

Pontificia Universidad Católica del Ecuador

Sede Ambato

HOJA DE APROBACION

DEPARTAMENTO DE INVESTIGACION, POSTGRADOS Y AUTOEVALUACION

TEMA:

"GESTION DE RIESGOS INFORMATICOS EN LA INDUSTRIA DE CARROCERIAS METALICAS EN LA PROVINCIA DEL TUNGURAHUA"

AUTOR

GERMAN MARCELO SALAZAR MOSQUERA

Patricio Medina, Ing. Msc
DIRECTOR DE TESIS
F:_____

Galo López Ing. Msc.
CALIFICADOR
F:_____

Janio Jadán Ing. Msc
CALIFICADOR
F:_____

Telmo Viteri, Ing. Msc
DIRECTOR DIPA
F:_____

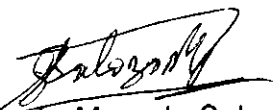
Pablo Poveda Mora, Dr.
SECRETARIO GENERAL PUCESA
F:_____

SECRETARIA GENERAL
PROCURADURIA

DECLARACION DE AUTENTICIDAD Y RESPONSABILIDAD

Yo, Germán Marcelo Salazar Mosquera portador de la cédula de ciudadanía No. 060180262-2 declaro que los resultados obtenidos en la investigación que presento como informe final, previo para la obtención del título de Magister en Gerencia Informática con mención en Redes y Desarrollo de Software, son absolutamente originales, auténticos y personales.

En tal virtud declaro que el contenido, las conclusiones y los efectos legales y académicos que se desprenden del trabajo propuesto de investigación y luego de redacción de este documentos son y serán de mi sola y exclusiva responsabilidad legal y académica.



Dr. Germán Marcelo Salazar Mosquera
C.I. 060180262-2

AGRADECIMIENTO

Agradezco a las personas e instituciones que me brindaron su apoyo incondicional durante la preparación y producción de la Tesis. En especial a la Pontificia Universidad Católica del Ecuador Sede Ambato por haber promovido este extraordinario programa de posgrado, en donde se despertó mi interés por profundizar sobre el estudio de la gestión de riesgos informáticos, convirtiéndole en el tema principal de la tesis.

En el campo profesional merece mención especial, los clientes relacionados con mis actividades de consultoría, como VIHAL, INARECROM, CARROCERIAS ALTAMIRANO, entre otros, empresas estas que me permitieron la aplicación de todos o algunos de los aspectos tratados en esta tesis.

A Patricio Medina, un extraordinario profesional de la informática, con dedicación y entusiasmo, efectuó la revisión técnica durante el desarrollo de la investigación y contribuyó con innumerables ideas para el mejoramiento y éxito de la misma.

Mis alumnos de Pregrado permanentemente fueron inspiradores de los temas y contenidos de la presente tesis y, en especial la forma de presentarlos, y me dejaron con la inquietud. "¿Como harás para ser guía si desconoces el camino?".

DEDICATORIA

Como un maravilloso recuerdo a mis Padres:

Señor Don Rafael Gerardo Salazar Quispe (QEPD)

Doña Dolores Natividad Mosquera Goyes (QEPD)

Ejemplos y Baluartes de entusiasmo y dignidad

A los Estudiantes de las Ciencias de la información,

Futuros líderes de la administración de riesgos tecnológicos.

RESUMEN

La gestión de riesgos informáticos como herramienta para que las organizaciones obtengan productos y servicios con una eficiencia y eficacia relevante que les permita el acceso al mundo competitivo de hoy, constituye un tema de gran actualidad; sin embargo aunque la experiencia internacional refleja ejemplos de empresas de avanzada en este campo y en la práctica empresarial ecuatoriana existen algunos resultados de su aplicación, aún se evidencian insuficiencias en lograr la coherencia en la derivación de de los herramientas utilizadas dentro de los sistemas de control y seguridad de los sistemas informáticos de todos los niveles de decisión desde la alta dirección hasta el sistema físico y la integración de este con el control del talento humano, que permita la proyección de acciones oportunas para la mejora continua de las organizaciones, lo que constituye un problema científico a resolver que requiere de investigaciones que deben ir desde lo conceptual hasta lo práctico, definiéndose como objetivo de este trabajo: Concebir un conjunto de procedimientos para el desarrollo del sistema de control y seguridad informática, a partir de considerar la integración y cohesión que debe existir entre los niveles de dirección, para potenciar la mejora continua de las organizaciones.

ABSTRACT

The computing risks management used like a tool to let organizations get products and services with a relevant efficiency and effectiveness that gives them access to today's competitive world, is considered a current affair; however, although the international experience reflexes examples of leader enterprises in this field, and in the practice of the ecuatorian enterprises there are some results of its application.The lack of coherence in the derivation of the tools used to the control and security in the informatics systems in all decision levels, is evident from de executive until the physical system and the integration of this system with the control of human talent that allows the projection of opportune actions for the sustained improvement of the organizations. This constitutes a scientific problem to solve that requires investigation that should start with theory and end up with practice. Then, the objective of research is to conceive a group of procedures for the development of the control and security systems beginning with the consideration and cohesion that should exist among the management levels, to enhance the sustained improvement of the organizations.

TABLA DE CONTENIDOS

PORTADA.....i
HOJA DE APROBACION.....ii
DECLARACION DE AUTENTICIDAD Y RESPONSABILIDAD.....iii
AGRADECIMIENTO.....iv
DEDICATORIA.....v
RESUMEN.....vi
ABSTRACT.....vii
TABLA DE CONTENIDOS.....viii
TABLA DE GRAFICOS.....viii
FIGURAS.....xiii
CUADROS.....xiv
Introducción.....1

CAPITULO I

PLANTEAMIENTO DEL PROBLEMA

1.1. Antecedentes.....5
1.2. Definición del problema.....6
1.2.1. Formulación del problema.....7
1.2.2. Análisis crítico.....7
1.2.3. Prognosis.....9
1.2.4. Delimitación del problema.....9
1.3. Hipótesis.....10

1.3.1. Variable dependiente 10

1.3.2. Variable independiente 10

1.4. Objetivos.....10

1.4.1. Objetivo general 10

1.4.2. Objetivos específicos.....11

1.5. Metodología.....11

1.5.1. Fuentes de información.....11

1.5.2. Diseño de la investigación.....12

1.5.3. Modalidad básica de la investigación.....12

1.5.4. Tipo de estudio 13

CAPITULO II

ANÁLISIS DE LA SITUACION ACTUAL DE LA GESTION DE RIESGOS INFORMATICOS EN LA INDUSTRIA DE CARROCERIAS METALICAS EN LA PROVINCIA DEL TUNGURAHUA

2.1. Antecedentes de la investigación.....14

2.2. Concepto de Riesgo.....17

2.2.1. Definición de riesgo tecnológico.....19

2.2.2. Orígenes de los riesgos de carácter tecnológico.....21

2.3. Adopción de decisiones en presencia de riesgos.....23

2.4. Caracterización de riesgos tecnológicos.....31

2.5. Actividades de gestión de riesgos.....33

2.5.1. Evaluación de los riesgos.....34

2.5.2. Control de los riesgos.....34

2.6. Técnicas de evaluación de riesgos.....36

2.6.1. Conceptos generales.....36

2.6.2 Análisis de riesgos.....37

2.6.3. Cálculo de las exposiciones de riesgos.....39

2.6.4. Ejemplo de modelo de cálculo de riesgos.....40

2.6.5. Ejemplo de perfiles típicos de riesgos 42

2.6.6. Técnicas para el análisis de riesgos identificadas 43

2.6.7. Ejemplos de gestión de riesgos en la tecnología 47

2.7. Técnicas de control de riesgos.....56

2.7.1. Actividades de control de riesgos.....56

2.7.2. Elaboración de un plan de contingencia.....57

2.7.3. Monitoreo de los riesgos.....63

2.8. Estrategias para minimizar el riesgo 64

CAPITULO III

DISEÑO DE LA PROPUESTA TECNICA PARA GESTIONAR LOS RIESGOS INFORMÁTICOS EN LA INDUSTRIA DE CARROCERÍAS METÁLICAS EN LA PROVINCIA DEL TUNGURAHUA

3.1. Introducción....69

3.2. Componentes del plan de contingencias....78

3.2.1. Planificación....79

3.2.2. Identificación de riesgos....84

3.2.3. Identificación de soluciones....91

3.2.4. Estrategias....108

3.2.5. Documentación del proceso....115

3.2.6. Realización de pruebas y validación....116

3.2.7. Implementación....128

3.2.8. Monitoreo....136

3.2.9. Pasos para desarrollar el plan de contingencia de los sistemas de información....137

3.2.10. Criterios sobre sistemas de información en Internet....162

3.3. Auditoria, seguridad y control de los ambientes....163

3.3.1. Auditoría informática como elemento de control interno....165

3.3.2. Metodologías de control interno y auditoría informática....179

3.4. Análisis de vulnerabilidades y amenazas....196

3.4.1. Vulnerabilidades y amenazas....196

3.4.2. Elementos empleados en las amenazas cibernéticas....205

3.4.3. Infraestructura crítica.....221

3.4.4. Delitos informáticos.....225

3.4.5. Propuesta especifica para el sector carrocero de la provincia del Tungurahua.....229

3.5. Alcance de la propuesta.....231

3.6. Factibilidad de la propuesta.....233

3.6.1. Fortalecimiento de la gestión administrativa y financiera.....233

3.6.2. Perfeccionamiento del personal.....234

3.6.3. Adquisiciones.....234

3.6.4. Gestión de riesgos.....234

CAPITULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones.....238

4.2 Recomendaciones.....239

Bibliografia.....241

Glosario.....244

TABLA DE GRAFICOS

FIGURAS

Figura 1.1 Árbol del problema.....8

Figura 2.1 Fuente de riesgos.....23

Figura 2.2. Proceso de toma de decisiones.....25

Figura 2.3. Matriz de efectos.....26

Figura 2.4. Ejemplo de matriz de efectos.....27

Figura 2.5. Relación entre probabilidades e impactos.....32

Figura 2.6. Modelo cíclico de gestión de riesgos.....36

Figura 2.7. Perfil temporal de un riesgo.....40

Figura 2.8. Tipos de perfiles de riesgos.....42

Figura 2.9. Causas de riesgos.....44

Figura 2.10. Diagramas de Ishikawa.....46

Figura 2.11. Ejemplo de diagrama de Ishikawa.....51

Figura 2.12. Ejemplo de perfil de riesgo: la tecnología no es escalable.....53

Figura 2.13. Cálculo de la exposición a un riesgo.....54

Figura 2.14. Efecto de la inclusión de contingencias.....58

Figura 2.15. Efecto del plan de contingencia sobre la planificación.....60

Figura 2.16. Ejemplo de actividades.....61

CUADROS

CUADRO 3.1. Matriz de planificación de contingencia y ejemplos.....92

CUADRO 3.2 Operaciones críticas del sistema de información.....139

CUADRO 3.3: Procesos estratégicos del negocio.....140

CUADRO 3.4: Análisis sobre un proceso del negocio.....141

CUADRO 3.5: Lista de recursos utilizados.....142

CUADRO 3.6: Lista de periodos aceptables de interrupción.....143

CUADRO 3.7: Lista de problemas probables a ocurrir.....144

CUADRO 3.8. Procesos del área analizada (e).....146

CUADRO 3.9. Formato de costos de cada proceso.....147

CUADRO 3.10 Lista de recursos críticos utilizados.....148

CUADRO 3.11. Tabla de probabilidad de fallas de recursos.....149

CUADRO 3.12. Lista de problemas probables a ocurrir.....150

CUADRO 3.13. Tabla matriz de prioridades de atención de riesgos.....151

CUADRO 3.14. Detalles de medidas preventivas del área analizada.....152

CUADRO 3.15 Matriz de análisis de riesgo.....153

CUADRO 3.16. Lista de medidas preventivas.....154

CUADRO 3.17 Matriz de análisis de riesgos.....155

CUADRO 3.18. Funciones de los grupos de trabajo del sistema administrativo de los sistemas de información.....156

CUADRO 3.19. Lista de acciones ante fallas de recursos.....157

CUADRO 3.20. Formato de lista telefónica del personal esencial en caso de problemas relacionados con el sistema administrativo.....159

CUADRO 3.21. Formato de lista telefonica de los proveedores de servicios 159

CUADRO 3.22. Formato tabla de análisis de riesgos.....160

INTRODUCCION.

En la actualidad las organizaciones se enfrentan a un entorno caracterizado por un elevado grado de incertidumbre y dinamismo, lo que hace necesario el desarrollo de estructuras flexibles y ágiles que den respuesta de manera eficaz y eficiente a las condiciones cambiantes del mercado. Precisamente, esta agilidad se puede desarrollar a través de la formación de alianzas, de manera que las organizaciones pueden optar por centrar sus esfuerzos en el desarrollo y cuidado de sus capacidades distintivas, a la vez que externalizan aquellas actividades y procesos que no resultan clave para su competitividad global. Las estrategias modernas de administrar los negocios descansan fundamentalmente en la tecnología, la cual está expuesta a riesgos, vinculados con los cambios permanentes en el entorno.

En este contexto, son varios los aspectos a debate recogidos en la literatura enmarcada en el tópico de la gestión de riesgos tecnológicos.

Las empresas ecuatorianas, independientemente de su tamaño o del sector en que se desempeñan, se están incorporando a la dinámica del uso de la tecnología. La tecnología es un recurso estratégico, por lo cual las decisiones relacionadas con inversiones en este campo son tomadas al más alto nivel de la organización. El impacto que la actitud de los directivos hacia la tecnología tiene sobre su adquisición, los empresarios ecuatorianos tienen distintos perfiles, destacando el

perfil del administrador que la alienta la inversión en tecnología siempre que haya un beneficio económico tangible, delegando cualquier decisión tecnológica a los expertos en ese campo una vez que el directivo ha autorizado la adquisición. Otro perfil identificado es el del directivo que sólo tiende a invertir pensando en objetivos específicos, como mejorar niveles de producción o hacer más eficiente un proceso, sin reconocer el potencial estratégico de la tecnología. Son muy pocos los directivos que impulsan y se comprometen a integrar la tecnología a la estrategia empresarial como parte importante para la competitividad. Los directivos con este perfil establecen medidas de rentabilidad a largo plazo y hacen un seguimiento continuo de resultados.

Las empresas y las universidades parecen estar de acuerdo en que la tecnología debe ser administrada. La razón es que se ha identificado la necesidad de fortalecer las habilidades de los administradores para vincular los recursos tecnológicos con el ambiente y la estrategia de negocios de las empresas, y para que los directivos comprendan la importancia que tiene la tecnología como instrumento de la competitividad en un contexto de economía global y cambios constantes.

La administración de la tecnología es la interface entre la ingeniería y los negocios. Al interior de las organizaciones la tecnología tiene una trayectoria dual: la estratégica y la operacional.

Desde el punto de vista de los negocios, la tecnología tiene una función principal dentro de las estrategias corporativas para consolidar la competitividad, mientras que

la perspectiva operacional implica la instrumentación y funcionamiento de la tecnología como medio para alcanzar los objetivos de la organización.

Dentro de las empresas, el proceso de administración de la tecnología que inicia en la etapa de planeación tecnológica y continúa con la etapa de transferencia de tecnología concentra en la etapa de administración del cambio tecnológico las acciones requeridas para absorber los impactos que tiene la tecnología a nivel de estructura, nivel funcional y nivel individual y en su ambiente de trabajo denominado cultura organizacional. Esta etapa implica un alto porcentaje de riesgo que debe gestionarse para minimizar el impacto.

Las pequeñas y medianas empresas del sector carrocero de la provincia del Tungurahua, por exigencias del mercado, tienen la exigencia de obtener la certificación de calidad ISO 9000, la mayoría necesita la adopción de la tecnología para cumplir los requisitos indispensables para la obtención de la certificación, además la proyección de ingresar a mercados internacionales, no será posible sin la administración de la tecnología, sin embargo existen los riesgos, la identificación, medición y administración de los riesgos informáticos que permita reducir el impacto en las organizaciones, constituye uno de los principales problemas a resolver por parte de los empresarios y los encargados del área informática en la industria carrocera de la provincia del Tungurahua.

Para enfrentar los retos tecnológicos de la industria carrocera luego de un análisis de las amenazas y vulnerabilidades, se proponen alternativas para minimizar el impacto de los riesgos.

CAPITULO I

PLANTEAMIENTO DEL PROYECTO

1.1. ANTECEDENTES

Todos los responsables de actividades de gran complejidad, desde la más remota antigüedad, eran conscientes de que las actividades programadas podrían sufrir retrasos o requerir mayores costos de los estimados o, incluso, que no fuese posible su realización debido a múltiples causas que lo impidieran. Algunas de esas causas eran previsibles, y los responsables podían anticipar algunas actuaciones, mientras que para otras a pesar del esfuerzo no era factible predecir.

Desde una perspectiva histórica, durante la mayor parte de la historia de la humanidad, pudo considerarse que el contexto en el que la actividad humana se realiza era estable tecnológicamente, por qué la evolución no tecnológica no afectaba a los proyectos informáticos al no existir cambios significativos durante la vida útil del mismo, porque las necesidades de los seres humanas eran satisfechas por los recursos naturales y los procesos que se implementaron a partir de la revolución industrial .

En la actualidad únicamente en proyectos tecnológicos cuya duración es menor a un año puede considerarse que se desarrolla en un entorno estable y conocido. Para

proyectos de mayor duración, se debe considerar que la tecnología puede modificarse sustancialmente durante su desarrollo. Como consecuencia de ello pueden ocurrir eventos que alteren sustancialmente el desarrollo del proyecto. El éxito de la gestión de la tecnología está condicionado por multitud de elementos de riesgo cuyo control debe abordarse de forma integrada con el resto de actividades.

De hecho, la mayor parte de los proyectos de ingeniería complejos dependen de una correcta identificación e incorporación de las tecnologías apropiadas para su desarrollo que deberán gestionarse como parte de éste. Estas tecnologías no son suficientemente conocidas o maduras, por lo que su utilización no siempre genera los beneficios esperados.

Desde este punto de vista, las actividades tecnológicas de una organización se planifican con una serie de suposiciones que pueden verse alteradas por acontecimientos indeseables (riesgos) cuya aparición real modifica o impide el éxito de los proyectos de gestión tecnológica.

1.2. Definición del problema

La importancia estratégica y operativa de las tecnologías de la información en los negocios ya no es cuestionada. A medida que avanza el siglo XXI, muchas empresas de todo el mundo están concentradas en transformarse en dinámicos negocios globales, por medio de importantes inversiones en tecnología. Por lo tanto, existe la necesidad real de que los gerentes se preparen para administrar ésta función

organizacional vital, la administración está sujeta a riesgos que deben ser gestionados para minimizar los impactos y en lo posible convertirlos en oportunidades de mejora.

1.2.1. Formulación del problema

¿Es la subutilización de los recursos informáticos, provocada por la exposición al riesgo ante la inexistencia de un plan de contingencias lo que conlleva a la disminución de los beneficios tangibles de los proyectos de desarrollo informático en la industria carrocera de la provincia del Tungurahua?

¿Cómo incrementar el éxito de los proyectos de desarrollo tecnológico mediante la adecuada gestión de riesgos en la industria carrocera de la provincia del Tungurahua?

¿Cuáles son los riesgos a lo que están expuestos los proyectos de desarrollo tecnológico?

¿Cómo medir el riesgo?

¿Cómo diseñar e implementar un plan de contingencia?

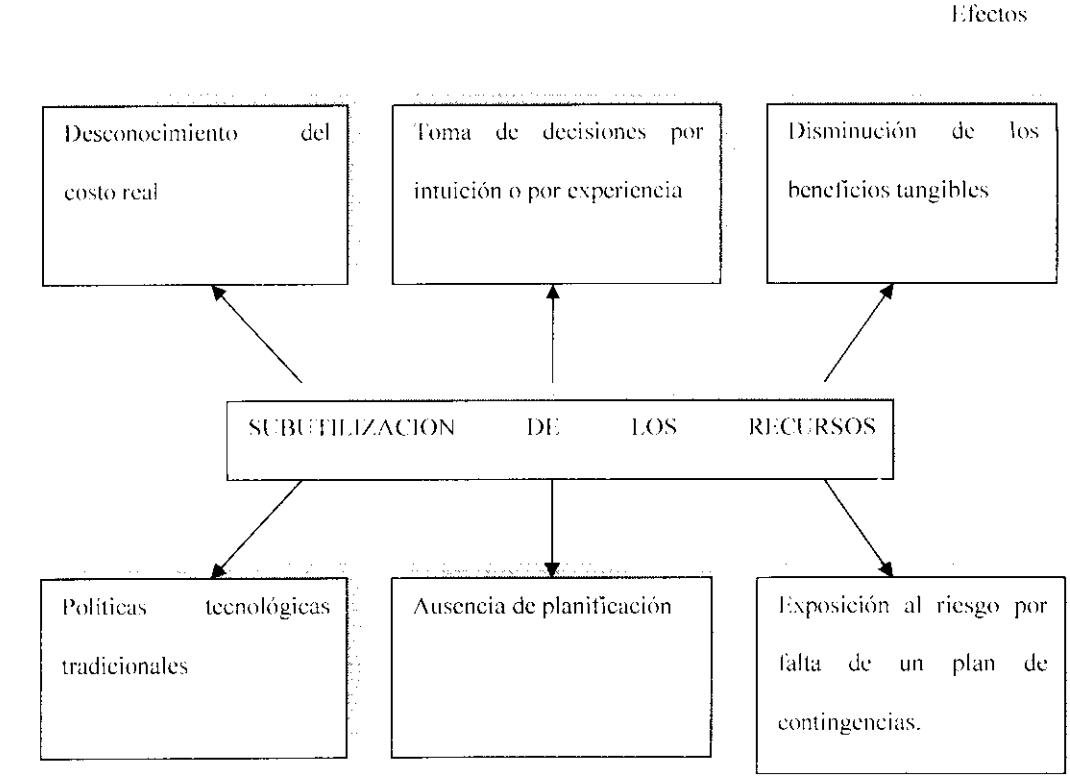
1.2.2. Análisis crítico

La definición de la estrategia informática requiere de hacer un reconocimiento respecto a las tendencias tecnológicas presentes a fin de tomar ventaja de las tecnologías ya disponibles en el mercado o para elegir aquellos proyectos tecnológicos que conviene apoyar internamente, ésta acción se toma ya sea con el

propósito de satisfacer las necesidades propias o para capitalizar la inversión del proyecto, ya que no prevé que hay competencia inmediata de otras empresas. Para minimizar los riesgos es conveniente la construcción de pronósticos tecnológicos formales, lo cuales apoyan a la empresa en la decisión respecto a la asignación de recursos. Los riesgos tecnológicos deben convertirse en oportunidades.

Figura 1.1

Árbol del problema



Elaborado por: GMSM

Fecha: Julio 15 de 2008.

1.2.3. Prognosis

Si el sector carrocero de la provincia del Tungurahua no implementa un sistema de gestión de riegos informáticos que permita aprovechar en forma eficiente los recursos tecnológicos, no tendrá la información relevante para la toma de decisiones y no se identificarán las áreas críticas en donde se deben implementar programas de mejoramiento continuo, siendo una limitación para obtener la certificación ISO 9000.

1.2.4. Delimitación del problema

1.2.4.1. Delimitación de campo

Campo: Administración

Área: Administración de la tecnología

Aspecto: Gestión de riesgos informáticos.

1.2.4.2. Delimitación espacial

La investigación se va a desarrollar en el sector carrocero de la provincia del Tungurahua.

1.2.4.3. Delimitación temporal

El tiempo de duración está estipulado desde el 1 de julio al 30 de diciembre del 2008.

1.3. Hipótesis

La exposición al riesgo por falta de un plan de contingencias, disminuye los beneficios tangibles de los proyectos de desarrollo informático en el sector carrocero de la provincia del Tungurahua.

1.3.1. Variable dependiente:

Beneficios tangibles de los proyectos de desarrollo informático.

1.3.2. Variable independiente:

La exposición al riesgo por falta de un plan de contingencias

1.4. Objetivos

1.4.1. Objetivo general

Analizar la relación que presenta la exposición al riesgo por falta de un plan de contingencias, con la disminución de los beneficios tangibles de los proyectos de desarrollo informático localizados en el sector carrocero de la provincia del Tungurahua.

1.4.2. Objetivos específicos

- Identificar los riesgos a los que están expuestos los proyectos de desarrollo tecnológico en el sector carrocero de la provincia del Tungurahua.

- Determinar los modelos idóneos para medir el riesgo.

- Proponer la implementación de un plan de contingencias que permita gestionar los riesgos informáticos.

1.5. Metodología

1.5.1. Fuentes de Información

Para la realización de la siguiente investigación se tomó información en base a fuentes primarias y secundarias.

En cuanto a las fuentes primarias se obtendrá información directa en los talleres de construcción de carrocerías metálicas en la provincia del Tungurahua, a través del gremio respectivo, los empresarios y empleados quienes aportarán en gran parte, para tener un enfoque claro de la situación actual de la misma. Para lo cual se han utilizado diversas técnicas de la investigación científica como son: entrevistas, encuestas, observación directa y grupos focales, mediante la investigación descriptiva la misma que proporcionará un resumen de aspectos del medio. Previo a

la elaboración del informe final se utilizarán herramientas tecnológicas y fichas técnicas, para levantar y tabular la información.

En cuanto a fuentes secundarias la información se recolectará de Libros, revistas, folletos, tesis de grado, blogs electrónicos estudios especializados realizados con anterioridad.

1.5.2. Diseño de la investigación

El enfoque de la investigación viene dada cuantitativa, porque en todo el análisis se medirá a través de indicadores: el impacto de los riesgos tecnológicos y se determinará la factibilidad de implementar planes de contingencia.

1.5.3. Modalidad básica de la investigación

Se realizará una investigación de campo, mediante el análisis de los riesgos tecnológicos existentes en la industria carrocera de la provincia del Tungurahua.

También se aplicará la investigación bibliográfica – documental, la misma que se permitirá recolectar y analizar información.

Mediante una investigación experimental, se procederá a seleccionar las variables dependiente e independiente; permitiendo verificar la relación causa – efecto.

1.5.4. Tipo de estudio

1.5.4.1. Exploratorio

Para la presente investigación inicialmente se realizará un análisis de la situación actual de la gestión de riesgos tecnológicos en el sector carrocero de la provincia del Tungurahua; determinando posibles problemas que atraviesan la misma; y cómo perjudican al sector industrial, en medio de un entorno competitivo.

1.5.4.2. Descriptivo

En el sector carrocero se puede observar a priori la necesidad de mejorar la eficiencia de los proyectos de desarrollo tecnológico, para ello es necesario describir los procedimientos, políticas y lineamientos que debe contener un plan de contingencias.

CAPITULO II

ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA GESTIÓN DE RIESGOS INFORMÁTICOS EN LA INDUSTRIA DE CARROCERÍAS METÁLICAS EN LA PROVINCIA DEL TUNGURAHUA

2.1. ANTECEDENTES DE LA INVESTIGACIÓN

Para entendernos como humanos, debemos pensar y actuar como humanos. Esto quiere decir que, en primer lugar, tenemos que ser capaces de jerarquizar y discriminar lo que nos hace tal como somos, teniendo en cuenta que lo que escojamos supeditará fuertemente la definición misma de la condición humana. En segundo lugar, se debe someter a juicio las actitudes idealistas que nos separan del mundo real y nos transportan al mundo impreciso de aquello que no es racionalmente aprehensible. En tercer lugar, nos tenemos que sacar de encima el caduco humanismo idealista de inspiración irracional, que tuvo valor operativo siglos atrás pero que ahora constituye una carga pesada.

Para acabar, hace falta que todos construyamos una forma de entender el mundo que sea adecuada a la gran capacidad que tenemos de transformar el entorno y

transformarnos a nosotros mismos, capacidad que hemos adquirido gracias al conocimiento teórico y práctico en el proceso evolutivo.

Es necesario manifestar claramente nuestro posicionamiento, en el sentido de abogar por la postura de los países desarrollados alterando el esquema actual de crecimiento económico por el progreso del hombre; eso es, contemplar al talento humano como protagonista de la actividad económica y social y no posponer al individuo de sus obras, sabiendo que la labor realizada es consecuencia de que su autor, el hombre, se sienta persona.

Inspirado en esta filosofía el autor emprendió una intensa revisión bibliográfica tanto en medios tradicionales como en medios electrónicos encontrando una gran cantidad de textos y documentos técnicos relacionados con el tema, que se encuentran citados en las secciones respectivas del presente trabajo.

En esta sección incluiremos algunos aspectos que han sido mencionados en otros ensayos o tesis y que servirán para orientar el desarrollo de la presente investigación, entre ellas tenemos las siguientes:

"En las últimas décadas las empresas han incorporado nuevas tecnologías de información como componente eje de sus sistemas de información, hasta el punto de acabar equiparándolo con el sistema o red informática de la empresa. Pese a que su implantación ha sido progresiva, en contadas ocasiones ha sido llevada a cabo en

forma correcta, ya que la confusión existente entre información e informática ha conllevado muchos errores.

La importancia que se le ha otorgado a la tecnología la ha acabado convirtiendo en el objetivo a alcanzar por la organización y con este razonamiento se ha llegado al convencimiento de que la tecnología de forma aislada puede mejorar el funcionamiento de ésta, el control de sus procesos y la gestión de sus recursos. De este modo, la empresa mejor dotada tecnológicamente debería ser la que alcanzará resultados más óptimos, pues su gestión debería ser mejor. La tecnología se presente como un evidente factor de éxito" (Serrano González, Susana; Zapata Luch, Mónica. "Auditoría de la información, punto de partida de la gestión del conocimiento": 2003.

"¿Se conoce el impacto de las decisiones que tomamos en términos tangibles e intangibles?

Ello nos conlleva a plantear la necesidad de conocer la manera de los tangibles e intangibles generan valor en una empresa. Para lograrlo se deben entender los intercambios de información y otros intangibles dentro y fuera de la organización.".(Marsal: 2003).

"A medida que las organizaciones adquieren mayor tamaño, y una mayor sensibilidad por el control interno, en la búsqueda de eficiencia de sus procesos, la necesidad de formalizar la función de auditoría informática se hace más patente.

A la hora de formalizar dicha función, las organizaciones deben tener muy presentes los objetivos que se plantean con ella, sus necesidades en cuanto a recursos y las diferentes estrategias que se pueden adoptar para ello, sin olvidar la posibilidad de externalizar total o parcialmente la función."(Pons: 2007).

"El buen gobierno (gobernanza) empresarial tiene y persigue, entre otras manifestaciones, la emisión de información contable relevante y fiable, que son las características que contribuyen a hacerla útil para los interesados en su contenido, y a la vez permiten elevar la eficiencia de los mercados en los que opera la empresa" (Gonzalo: 1995)

"Renunciar a competir es renunciar al futuro inmediato; son tiempos de competir y la ventaja la tendrán las empresas que aprendan más rápido a ser eficaces, hoy se dividen en dos, las rápidas y las lentas en reaccionar a los cambios mundiales; estamos en una carrera de supervivencia en que la calidad es el único camino para no desaparecer, la competencia arrecia día tras día con más fuerza, pero no debemos temer a la competencia sino más bien a nuestra propia incompetencia."(Muñoz: 2005).

2.2. Concepto de riesgo

Todas las actuaciones relacionadas con la tecnología de una organización deben planificarse a lo largo del tiempo. En momentos cruciales toman la forma de un plan tecnológico, lo que implica la identificación y secuenciamiento de las actividades, la

asignación de recursos humanos, el empleo de recursos materiales, las necesarias asignaciones económicas y los métodos de control del progreso de las actividades. La planificación se realiza suponiendo que todo va a suceder de acuerdo con lo que se ha pensado y valorado.

No obstante, durante la puesta en marcha de cualquier actuación relacionada con la tecnología pueden surgir acontecimientos indeseables en la planificación inicial de actividades.

Cualquier modificación de las previsiones efectuadas afecta fuertemente a la planificación (plazo y costo de las tareas identificadas) y la obtención de los resultados deseados con el nivel de calidad exigido. Las modificaciones de la planificación inicial son siempre complicadas: requieren tiempo y dinero y obligan a dedicar recursos humanos calificados para ello.

Consciente de ello, la dirección de la gestión de la tecnología de la empresa debe tener previstas actuaciones en el caso de que los riesgos que se hayan identificado se presenten realmente. El simple conocimiento de los riesgos de una actividad ya supone una ventaja al facilitar un estado de alerta sobre ellos que disminuye sus consecuencias indeseables en caso de producirse.

Como ejemplo, un rompevelocidades en una carretera presenta un peligro mucho mayor para un conductor que no conozca su existencia que para quien viaja frecuentemente por esa carretera. Este conoce su existencia por lo que puede

disminuir su velocidad y frenar a tiempo. Incluso, aunque no conozca exactamente dónde se encuentra pero sí que existe en algún lugar de la carretera, puede tomar algún tipo de precauciones.

Estas actuaciones se concretan en la elaboración de planes de contingencia incorporados en los planes tecnológicos o ligados a determinados procesos de uso de la tecnología. El objetivo de estos planes es reducir el efecto indeseado de los riesgos mediante la puesta en marcha de un conjunto de actuaciones previamente identificadas. Seguidamente se analizará el concepto de riesgo y las actividades de gestión de éste.

2.2.1. Definición de riesgo tecnológico

Como el riesgo constituye una falta de conocimiento sobre futuros acontecimientos, se puede definir como el efecto acumulativo que estos acontecimientos adversos podrían tener sobre los objetivos de la actividad planificada. También puede hablarse de riesgo cuando la consecuencia sea positiva para la marcha de la organización. Algunos autores llaman a este caso oportunidad, pero este enfoque no será considerado en esta investigación. Entre las principales definiciones de riesgo se pueden resaltar las siguientes:

La gestión de riesgos, en el contexto de un proyecto, es el arte y ciencia de identificar, analizar y responder a los factores de riesgo a lo largo de la vida del proyecto y en el mejor cumplimiento de sus objetivos" (Duncan: 1996).

Para el investigador, un riesgo tecnológico se conceptúa como la posibilidad de que existan consecuencias indeseables o inconvenientes de un acontecimiento relacionado con el acceso o uso de la tecnología y cuya aparición no se puede determinar a priori.

Para que un riesgo pueda considerarse gestionable y, por tanto, susceptible de ser incluido dentro de los procesos de gestión de la tecnología en una organización, es necesaria la existencia simultánea de los siguientes tres componentes:

Pérdidas asociadas con el riesgo identificado. Ello se refiere a la existencia de efectos negativos resultantes de que el riesgo se concrete durante el desarrollo de la actuación contemplada. Generalmente estas pérdidas se pueden hacer corresponder con una valoración económica, pero hay casos en los que eso no se produce así, como ante pérdidas de vidas humanas o desastres medioambientales (en nuestro caso, derivados del uso incorrecto o desproporcionado de la tecnología).

Incertidumbre asociada. Probabilidad, pero no certidumbre, de que el riesgo identificado tenga lugar (ocurra efectivamente) y el momento temporal en el que eso pueda suceder. Téngase en cuenta que esta condición implica que al riesgo debe poder asociársele una probabilidad de ocurrencia a lo largo del tiempo.

Elección entre alternativas. Posibles actuaciones que mitiguen los efectos del acontecimiento indeseable. Si no existe elección por parte del gestor no existe riesgo

gestionable, aunque sí puedan existir pérdidas. Estas alternativas permiten al gestor actuar para reducir su aparición, las pérdidas ocasionadas o ambas.

No todos los riesgos que ocasionan fuertes pérdidas son gestionables en el sentido indicado. Es, precisamente, la conjunción simultánea de los tres componentes mencionados lo que permite su gestión.

2.2.2. Orígenes de los riesgos de carácter tecnológico

Los riesgos asociados a la tecnología desde su concepción, desarrollo y utilización en determinadas comunidades de usuarios no sólo afectan a las organizaciones que la conciben durante el tiempo de su desarrollo. Los riesgos en un proyecto pueden tener orígenes diversos, y entre las fuentes más típicas se encuentran las siguientes:

Derivadas del propio proceso de adquisición o transferencia de tecnología. Son causas internas derivadas de una planificación defectuosa o el desarrollo extemporáneo de las competencias de los recursos humanos implicados.

Derivadas de dificultades en la organización receptora. Son causas derivadas de la organización en la que la tecnología se va a utilizar y que afectan a su desarrollo o implantación.

Derivadas de la tecnología empleada en su desarrollo, como la inestabilidad de la tecnología empleada o la aparición de otras tecnologías alternativas que la hagan inútil o prematuramente obsoleta.

Derivadas del contexto externo a la organización. Como ejemplo, causas socioeconómicas o políticas que impidan el acceso a la tecnología o su mantenimiento posterior.

Derivadas del mercado y de la evolución de éste durante el desarrollo d las actuaciones tecnológicas consideradas. Como ejemplo, causas económicas y de penetración tecnológica muy diferentes de las previstas por acontecimientos no ligados a la tecnología en sí misma: una crisis económica global.

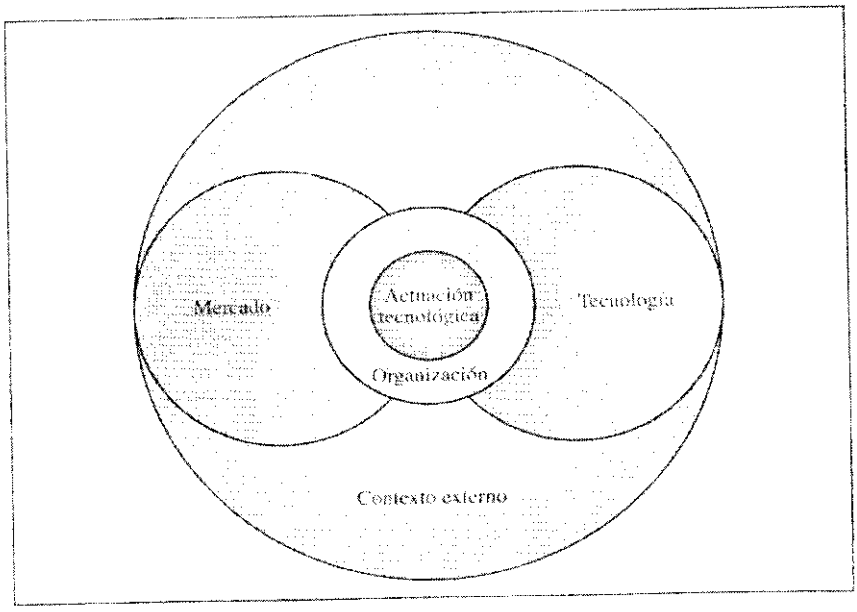
Muchas veces estas fuentes de riesgos están relacionadas entre sí, como también lo están los riesgos concretos de un proyecto, por lo que su separación y análisis diferenciado será uno de los problemas y limitaciones a resolver por los gestores.

Por simplicidad se va a suponer que todos los riesgos son independientes, aunque en la práctica existen siempre riesgos cuya probabilidad de aparición o cuyos efectos pueden incrementarse debido a la aparición efectiva de otros.

La figura 2.1 representa esquemáticamente la interacción entre todas las fuentes de riesgos indicadas. Con ello se ha querido representar que la existencia de fuentes de riesgos múltiples no va a permitir un enfoque analítico de separación de causas. Los

riesgos derivados del contexto externo, por ejemplo, también influyen en el mercado, tecnología y organización, potenciando el efecto de todos ellos.

Figura 2.1 Fuentes de riesgos



ELABORADO POR: GSM

FECHA: 15/08/2008

2.3. Adopción de decisiones en presencia de riesgos.

Durante la actividad de una organización (por ejemplo, en la puesta en marcha de un plan tecnológico) se toman decisiones tecnológicas continuamente, tanto por el responsable como por el resto del equipo en función de sus responsabilidades respectivas. La toma de decisiones está, sin embargo, condicionada por la existencia

de riesgos cuyos efectos y probabilidades pueden incrementarse por estas mismas decisiones. Cualquier decisión puede realizarse en tres condiciones diferentes:

Con certidumbre. Se dispone de toda la información necesaria para predecir el resultado de la decisión.

Con incertidumbre. No se dispone de la información necesaria para tomar una decisión. Únicamente se puede emplear la experiencia previa y la intuición.

En presencia de riesgos. Sólo se dispone de información parcial, aunque los efectos de los acontecimientos pueden predecirse y su impacto se puede estimar con razonable grado de aproximación:

La figura 2.2 representa esquemáticamente el proceso de toma de decisiones relativo a la tecnología. Ante un problema identificado relativo a la aparición de un riesgo previamente detectado, el gestor considera la situación actual de la organización y, teniendo en cuenta su experiencia en el tratamiento de situaciones parecidas, selecciona una posible alternativa entre las previamente analizadas y predefinidas.

La selección de la alternativa más adecuada no siempre es sencilla de determinar, puesto que ello depende de múltiples factores contradictorios que será necesario priorizar en función de la maximización de algunos parámetros.

El efecto de determinadas opciones puede representarse mediante las denominadas matrices de efectos. La figura 2.3 describe una estructura genérica de matriz de efectos.

Se han representado en filas las posibles opciones en manos del gestor, sus estrategias tecnológicas, y en columnas un conjunto de acontecimientos sobre los que el gestor no tiene control directo pero que influyen directamente en los resultados de sus decisiones (situaciones previsibles).

La selección de una alternativa en el caso de que se produzca uno de esos acontecimientos tiene consecuencias muy diferentes sobre la organización. Supondremos que los acontecimientos están relacionados entre sí y, por tanto, sólo uno de ellos puede realmente producirse.

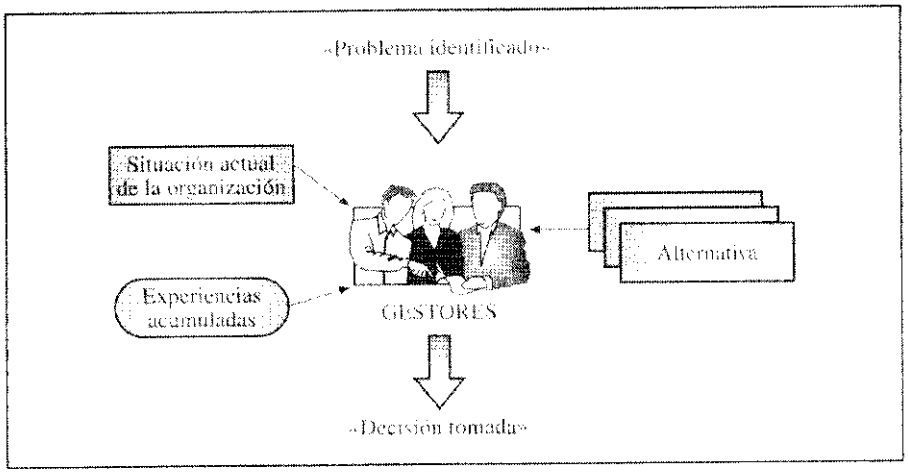


Figura 2.2. Proceso de toma de decisiones.

Elaborado Por: GMSM

Fecha: 16/08/2008

Para construir una matriz de efectos se deben identificar las situaciones sobre las que no se tiene control. Luego se selecciona el conjunto de estrategias que se desea adoptar. Cada una de las estrategias implica adoptar determinados riesgos que serán diferentes en función de las situaciones externas que finalmente se presenten.

En el caso de una decisión con certidumbre, independientemente de la situación que finalmente ocurra, existirá una estrategia dominante que producirá mayores ganancias que cualquier otra.

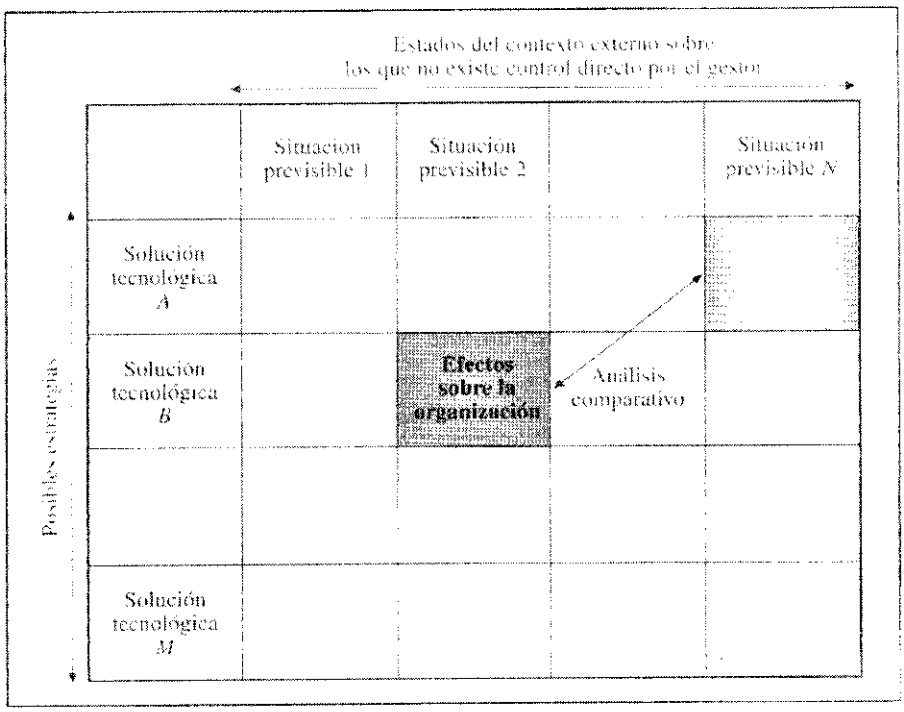


Figura 2.3. Matriz de efectos

Elaborado por: GMSM

Fecha: 17/08/2008

No obstante, en la práctica no hay una estrategia dominante para todas las situaciones, puesto que la decisión se producirá con información parcial. Generalmente, los mayores beneficios se producen cuando los riesgos son más altos y las pérdidas más probables.

Normalmente, cada situación podrá producirse con una determinada probabilidad cuya estimación deberá conocerse de la manera más clara posible, si bien estas estimaciones son difíciles de obtener.

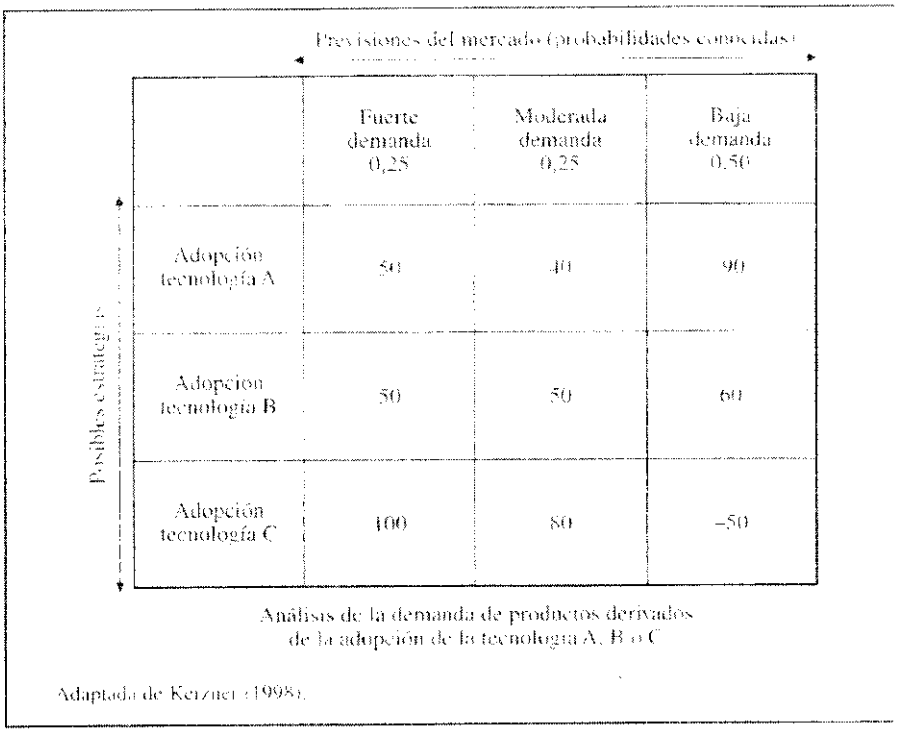


Figura 2.4. Ejemplo de matriz de efectos.

Adaptado Por: GMSM

Fecha: 17/08/2008

La figura 2.4 representa un ejemplo concreto de matriz de efectos para el caso de una inversión de 50 millones de dólares para adoptar una tecnología.

Como puede observarse, el gestor puede seleccionar tres tecnologías posibles que le permitirán desarrollar un nuevo tipo de producto. Su impacto en términos de beneficios sobre la organización depende de la demanda que esta tecnología asociada al producto tenga en el futuro.

En la matriz de la figura 2.4 se han indicado también las probabilidades asociadas a cada una de las posibles respuestas del mercado. Tras un análisis del mercado, los gestores han supuesto tres posibles situaciones (ajenas a su control) relativas a la respuesta que el mercado tendría a la introducción de su producto: baja demanda (con una probabilidad de 50%), demanda moderada (con una probabilidad del 25%) y fuerte demanda (con una probabilidad del 25%).

Desde el punto de vista de la adopción de la tecnología, los gestores conocen que existen tres estrategias posibles: tipo A (muy avanzado tecnológicamente empleando tecnologías emergentes), tipo B (con una tecnología madura pero no adoptada todavía por la empresa) y tipo C (con una tecnología convencional actualmente disponible en la organización). La matriz representada indica la situación previsible que se obtendría con cada estrategia en función de la respuesta del mercado (en términos de pérdidas o beneficios). A partir de ello, es necesario determinar la estrategia concreta que debería seguir la empresa.

Un ejemplo real de esta situación se puede encontrar en el desarrollo de un nuevo computador en el que se desea incorporar un sistema de almacenamiento externo para intercambio de información. Tras un análisis de las tecnologías disponibles, el diseñador duda en incorporar una de tres soluciones tecnológicas posibles: flash memory en formato de memory stick, flash memory en formato PMCIA o CD-RW.

Ninguna de ellas ha penetrado suficientemente en el mercado como para identificarla como la solución ganadora, aunque el grado de madurez de cada una es diferente. En el caso de flash memory, la decisión está más ligada al formato que a la tecnología en sí. Existe, por tanto, un riesgo derivado de una decisión de incorporación en el producto de una tecnología que no necesariamente será la que el mercado adoptará finalmente en el futuro, comprometiendo el éxito del producto.

Los valores esperados (valor medio que el gestor esperaría si realizara este esfuerzo cien veces) serían:

E_1= 50 x 0,25 + 40 x 0,25 + 90 x 0,50= 67,5

E_2 = 50 x 0,25 + 50 x 0,25 + 60 x 0,50=55

E_3= 100 x 0,25 + 80 x 0,25— 50 x 0,50 = 20

El gestor siempre elegiría el desarrollo tipo A, aunque no es la única opción posible. Su tolerancia al riesgo puede hacer que rechace una opción en la que perder la inversión o preferir otra en la que el beneficio sea máximo.

Estos comportamientos se concretan en criterios a adoptar cuando no hay probabilidades (desconocimiento del mercado) ni tampoco hay una estrategia dominante. Los principales criterios se pueden resumir en:

Criterio de Hurwicz. El gestor (optimista) adopta la estrategia que conduce a los máximos beneficios. En el caso expuesto, el desarrollo tipo C. Este comportamiento es típico en las grandes empresas, puesto que podría compensar las pérdidas en otras actuaciones en diferentes sectores.

Criterio de Wald. El gestor (pesimista) desea minimizar las pérdidas máximas. Elegiría el tipo B. Este comportamiento es típico de las pequeñas empresas, cuyo margen de maniobra es limitado.

Criterio de Savage. Intenta minimizar los máximos castigos, es decir, hacer mínimo el máximo costo de oportunidad. Eso se hace para cada columna restando cada elemento de la columna que figura en ella del mayor elemento de la misma. El máximo castigo es el mayor castigo de cada estrategia. (En nuestro caso, 50 para el tipo A, 50 para el tipo B y 140 para el tipo C.). Elegiría el tipo A o el B y rechazaría el C.

Criterio de Laplace. Intenta transformar una situación de incertidumbre en una situación de riesgo (con probabilidades). Para ello, supone que cada estado de la naturaleza tiene una probabilidad de ocurrencia similar. Con ello, elegiría el tipo A.

2.4. Caracterización de riesgos tecnológicos.

No todos los riesgos tienen la misma importancia. De entre todos los factores que permitirían caracterizar un riesgo, dos de ellos, el impacto y la probabilidad de ocurrencia, son los que tienen mayor importancia para el gestor. Debido a ello, la gestión de riesgos debe comenzar con la situación relativa de todos los riesgos identificados en un mapa bidimensional de impactos y probabilidades. Sobre este mapa se pueden tomar decisiones relativas a los riesgos a los que se debe prestar mayor atención.

Obsérvese que la existencia de un riesgo con una probabilidad muy baja puede despreciarse a pesar de que su impacto sea muy alto. En otros casos, la probabilidad muy alta puede verse compensada porque el efecto sea muy pequeño. La importancia relativa depende de la consideración simultánea de ambos factores.

La figura 2.5 representa una situación en la que existen cuatro riesgos claramente diferenciados (R_i, R_j, R_k, R_l). Cada uno de los riesgos tiene una determinada probabilidad de ocurrencia y un impacto previsible dentro de un cierto margen. Estos valores pueden ser en la práctica muy diferentes y, en función de ello, el gestor puede concentrarse en todos o en un número limitado de ellos.

En la realidad, conocer exactamente la probabilidad y el impacto de todos los riesgos posibles es muy difícil. Generalmente, sólo se dispone de estimaciones para ambas variables cuya precisión es también muy diferente en función del riesgo considerado.

En la figura 2.5 se puede observar cómo el margen (la nube de incertidumbre) asociado a cada riesgo puede ser mayor o menor.

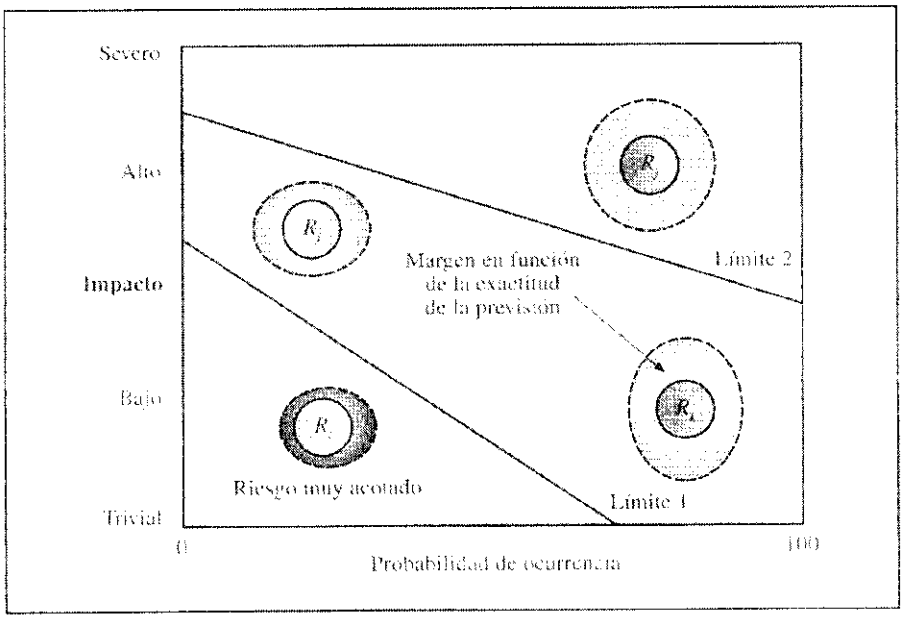


Figura 2.5. Relación entre probabilidades e impactos.

Elaborado por: GMSM

Fecha: 18/08/2008.

Las opciones posibles del gestor se han representado en la figura 2.5 mediante el establecimiento de dos límites distintos. Con el límite 1, el riesgo R_1 no sería considerado. Si se decide incrementar el umbral al límite 2, únicamente el riesgo R_j debería gestionarse.

Si se aplica este caso a la matriz de efectos descrita anteriormente y se considera que tanto los efectos como las probabilidades están en un rango amplio, la decisión que

tiene que tomar el gestor se complica y ya no es tan evidente cuál sería la estrategia más adecuada. En gran medida, dependerá del gestor y de su actitud o tolerancia frente al riesgo.

Siguiendo con el ejemplo de la matriz de efectos, supóngase que las previsiones del mercado no son tan claras. Dicho de otro modo, los estados no controlados no permiten calcular adecuadamente probabilidades. Si se recalculan los valores con máximos y mínimos, posiblemente los valores esperados se situarían en que se solaparían. La consecuencia es una dificultad mucho mayor para la toma de decisiones.

2.5. Actividades de gestión de riesgos.

Las actividades de gestión de riesgos han sido extensamente estudiadas en el caso de proyectos de ingeniería. En algunos como el desarrollo de proyectos software, estas técnicas han permitido la identificación de riegos concretos o incluso el desarrollo de metodologías integradas de gestión de riesgos como RiskMan.

En esta sección se extrapolará este cuerpo de doctrina para la gestión de tecnología en las organizaciones, asumiendo que en éstas se realizarán proyectos y operaciones incluidos en programas tecnológicos que requerirán la adopción de nuevas tecnologías. Los procesos asociados a la gestión de riesgos pueden clasificarse en dos grandes grupos: evaluación y control.

2.5.1. Evaluación de los riesgos

Existen muchos riesgos potenciales, pero un gestor no puede atender a todos y, además, algunos no son lo suficientemente importantes como para compensar a puesta en marcha de procedimientos concretos.

Posteriormente se analizará que ello es necesario tener alguna magnitud que permita centrar la atención en un conjunto de riesgos que sean los más importantes.

Los procesos de gestión relacionados con la evaluación de riesgos permiten identificar los riesgos que van a controlarse, su análisis y priorización. Las áreas de gestión asociadas son las siguientes:

- Identificación de riesgos.
- Análisis de riesgos.
- Priorización de los riesgos identificados.

2.5.2. Control de los riesgos

Sobre cada uno de los riesgos que se ha decidido controlar es necesario establecer algún tipo de actuación preventiva y comprobar que el riesgo se produce en función de algún tipo de señal, y poner en marcha, en su caso, las medidas previstas, que por lo general se incluyen en el plan de contingencias.

Todos estos procesos se superponen al resto de los procesos de gestión del sistema (que, a su vez, se superponen a los de desarrollo del proyecto). Las áreas de gestión asociadas son:

- Planificación del control de riesgos.
- Resolución de riesgos.
- Monitoreo de la evolución de riesgos.

Cada uno de los tipos mencionados está constituido a su vez por diferentes procesos relacionados con:

- Obtención de información.
- Elaboración de una estrategia de mitigación.
- Toma de decisiones.
- Monitoreo de los efectos.
- Documentación de las lecciones aprendidas.

La figura 2.6 representa gráficamente que los procesos de gestión descritos anteriormente se aplican secuencialmente. El modelo cíclico sugerido por el reloj implica que la organización aprende de su gestión en diversos procesos de gestión de la tecnología, mejorando sus procedimientos de identificación, análisis o mitigación para posteriores procesos de gestión.

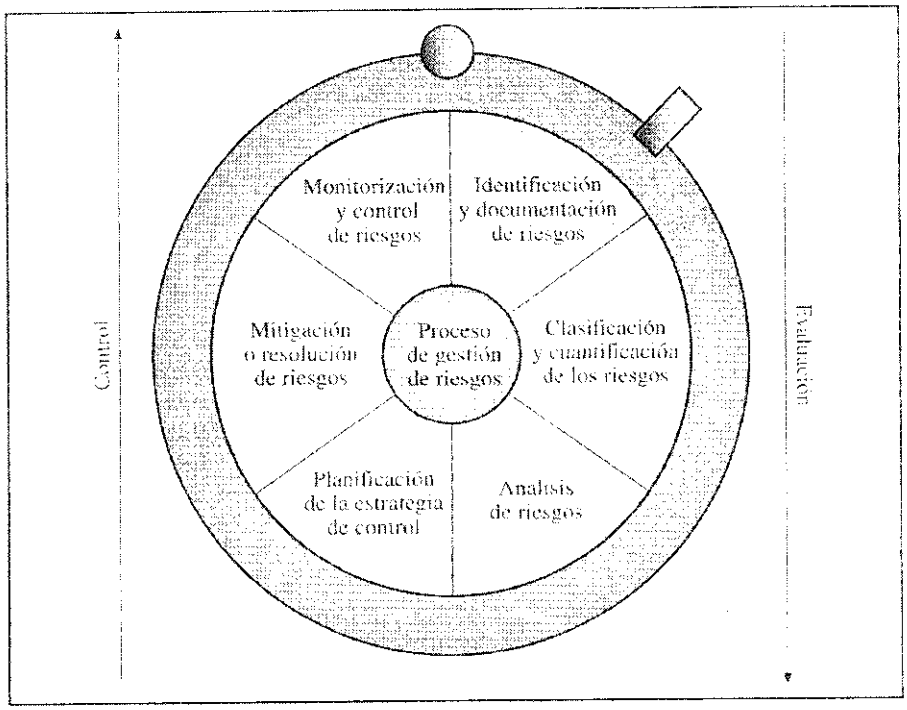


Figura 2.6. Modelo cíclico de gestión de riesgos.

Elaborado por: GMSM

FECHA: 18/08/2008

2.6. Técnicas de evaluación de riesgos.

2.6.1. Conceptos generales

Sólo se pueden adoptar medidas ante riesgos previamente evaluados, razón por la cual la evaluación de los riesgos se realiza antes de la planificación. Identificar riesgos correctamente implica disponer de información suficiente para ello. De esta manera, la primera preocupación del gestor deberá ser la de disponer de fuentes de información fiable y suficiente. Cada actividad, por ejemplo la ejecución plan

tecnológico, posee riesgos propios y diferentes, aunque la experiencia acumulada puede emplearse en la elaboración de planes tecnológicos similares.

Como la evaluación de riesgos tiene aspectos objetivos (basados en datos registrados de proyectos anteriores o del actual) y subjetivos (basados en las experiencias de diversos expertos y de la interpretación de éstas por el gestor), no debe olvidarse que la misma información puede dar origen a una identificación diferente por dos gestores distintos.

Las fuentes de información disponibles son:

- Procedentes de las actividades de cada una de las fases.
- Análisis de la documentación generada en el ciclo de vida.
- Análisis de costos.
- Bases de datos de lecciones aprendidas en ocasiones anteriores.
- Procedentes de técnicas basadas en juicios de expertos:
- Método Delphi, basado en cuestionarios.
- Técnica de grupo nominal, basada en entrevistas.

2.6.2. Análisis de riesgos

Una vez que se han identificado todos los riesgos, es necesario conocer su importancia relativa para poder decidir sobre su priorización.

Es evidente que no todos los riesgos tienen el mismo impacto ni probabilidad. Por ello, se ha buscado un parámetro que resuma esa importancia: la exposición.

La exposición a un riesgo mide el efecto del riesgo en un momento determinado teniendo en cuenta la probabilidad de que se produzca en ese momento. En otras palabras:

Exposición (R_i, t) = Efecto (R_i, t) x Probabilidad (R_i, t)

La medida de exposición al riesgo intenta combinar dos factores: probabilidad de ocurrencia y efecto sobre el proyecto, considerando que responden a variables independientes que pueden estimarse por los gestores del proyecto. El efecto debe entenderse en la ejecución del proyecto de desarrollo o incorporación de una tecnología y no en el uso posterior de la misma.

El mensaje para el gestor es que sólo deben gestionarse aquellos riesgos cuya exposición supere un umbral mínimo dictado por la experiencia (modelos comparativos) y por la capacidad de gestión en la organización.

Volviendo al ejemplo anterior de la aeronave, el riesgo en el proyecto se reduce a que pueda caer un avión sobre el edificio cuando se está construyendo.

Obviamente, también puede caer posteriormente, pero ése no será un riesgo a considerar en el proyecto, sino en la operación posterior (únicamente hay que tener

en cuenta las responsabilidades en la fase de garantías posteriores a la entrega del edificio). Para un comprador, el riesgo persistirá durante toda la vida útil del edificio y eso es lo que tendrá en cuenta una campaña de seguros. Este riesgo no siempre será el mismo. Si años después el corredor aéreo cambia de ubicación o el tamaño de las aeronaves aumenta, la probabilidad de ocurrencia disminuirá y el impacto aumentará, respectivamente.

La fórmula descrita anteriormente debe tener en cuenta que tanto la probabilidad como el efecto sobre el proyecto son variables que dependen del tiempo.

Como ejemplo, supóngase que se identifica un riesgo que puede ocurrir en las primeras fases del ciclo de vida. Después de la terminación de estas fases ya no tiene sentido preocuparse, porque la causa del riesgo ha terminado y la probabilidad de que suceda es nula.

2.6.3. Cálculo de las exposiciones de riesgos

La combinación de los factores de probabilidad y efecto genera para cada riesgo una curva (perfil) con la exposición al riesgo a lo largo del tiempo (figura 2.7). La exposición mide el impacto global del riesgo, si se es capaz de evaluar el efecto y la probabilidad a lo largo del tiempo. Con ello se estará en disposición de estimar los costos debidos a los recursos malgastados en el caso de aparición del riesgo. Como ejemplo, valoración económica de los retrasos introducidos en el desarrollo del proyecto si el riesgo se concreta o pérdidas asociadas con el riesgo en cuestión

(materiales, económicas, recursos humanos, etc.). Todos estos datos permiten generar un perfil del riesgo cuya caracterización precisa es un elemento fundamental para determinar los procedimientos de gestión más adecuados. El perfil indica también cuándo hay que preocuparse por un riesgo concreto.

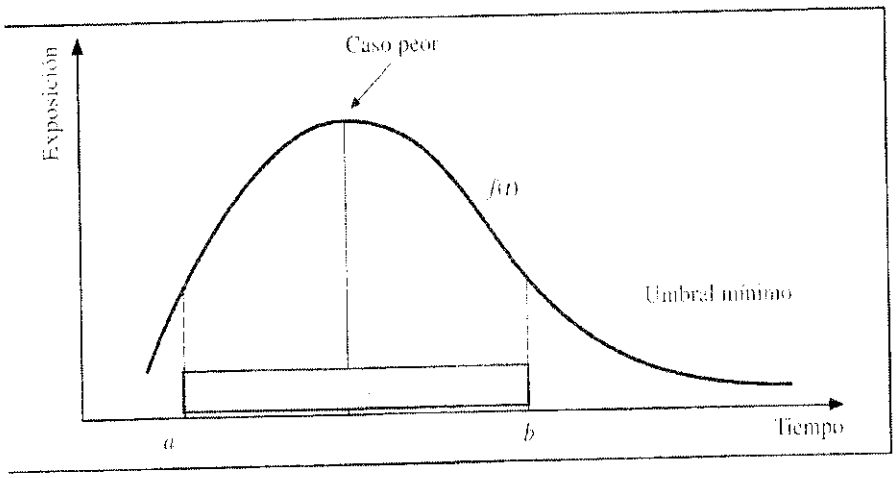


Figura 2.7. Perfil temporal de un riesgo.

Elaborado Por: GMSM

Fecha: 19/08/2008.

2.6.4. Ejemplo de modelo de cálculo de riesgos

El siguiente modelo puede utilizarse para el cálculo de la exposición al riesgo de carácter técnico en el caso de desarrollo de un sistema Hw-Sw. Se pretende estimar la probabilidad de falla del sistema y el efecto que ello daría. En una hipótesis simplificada, en la que no existe variación en el tiempo, la exposición sería:

Exp. (falla técnico) = Pf x Ef

Donde:

Pf (probabilidad de falla).

Ef (efecto o consecuencia del falla).

Por su parte:

Pf = a X P(M - Hw) + b X P(M - Sw) + c X P(C - Hw) + d X P(C - Sw) + e X Pd

Ef = f X Ct + g X Cc + h X Cp

Siendo:

P(M - Hw) = Probabilidad de falla debido a la madurez de la tecnología hardware.

PM - Sw = Probabilidad de falla debido a la madurez de la tecnología software.

P(C - Hw) = Probabilidad de falla debido a la complejidad hardware.

P(C - Sw) = Probabilidad de falla debido a la complejidad software.

Pd = Dependencia cruzada de otros factores.

Ct Consecuencias de falla debido a factores técnicos.

Cc = Consecuencias del falla debido a cambios en los costos

Cp = Consecuencias del falla debido a cambios en la planificación.

a, b, c, d, e, f, g y h son parámetros definidos en función del tipo de proyecto.

La dificultad estriba en conocer los valores de los parámetros para un proyecto de innovación en concreto.

Es difícil obtener para cada riesgo una función matemática f(t) que represente su exposición a lo largo del tiempo. En casos prácticos, lo más que se puede hacer es

identificar valores estimativos de la exposición en puntos concretos relacionados con hitos fundamentales del proyecto. En el caso de la figura 2.7. el riesgo sólo debe preocupar en el intervalo (a, b). No obstante, existen modelos matemáticos más complejos para el cálculo de la importancia relativa de los riesgos que no van a abordarse en este capítulo (Haymes, 1998). Un aspecto fundamental a la hora de realizar estimaciones correctas es la importancia de la experiencia previa que tenga la empresa en el desarrollo de ese tipo de proyectos.

2.6.5. Ejemplos de perfiles típicos de riesgos

Si bien es muy difícil obtener una función matemática continua del perfil del riesgo, sí es más sencillo estimar valores en instantes determinados del proyecto. La figura 11.8 representa una situación en la que se han identificado cuatro riesgos diferentes en Momentos concretos del desarrollo de un Proyecto.

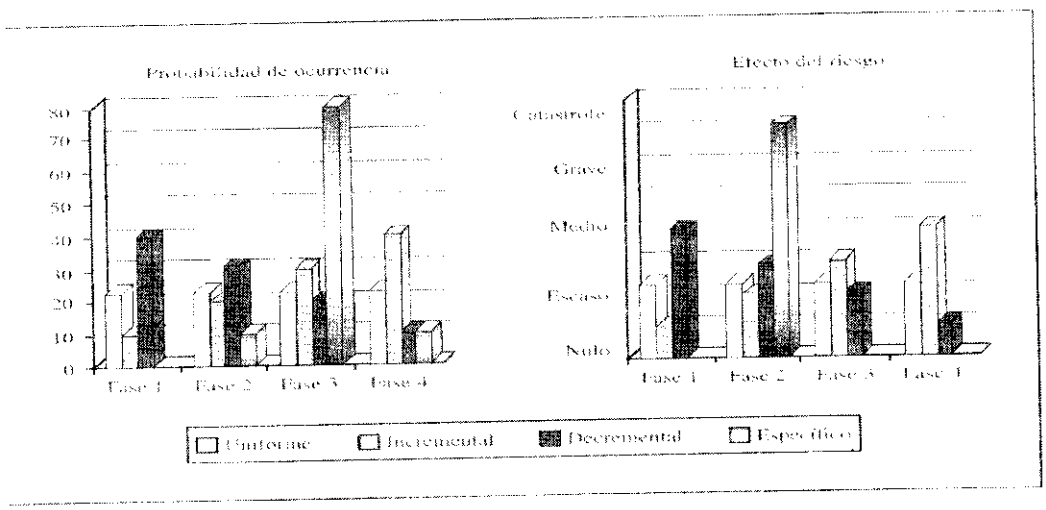


Figura 2.8. Tipos de perfiles de riesgos

Elaborado Por: GMSM.

Fecha: 20/08/2008

Cada uno de los riesgos tiene diversos valores de probabilidad de ocurrencia y efecto a lo largo de las diferentes fases del ciclo de vida. En función de ello, sus exposiciones serán también diferentes:

- El riesgo de carácter uniforme es el que no varía a lo largo de las diferentes fases.
- El riesgo de carácter incremental es aquel cuya exposición va creciendo con el tiempo, es decir, cada vez es más peligroso.
- El riesgo de carácter decremental es aquel en el que su exposición va reduciéndose en el tiempo. Si no ha aparecido en las primeras fases puede ser residual y deja de tener importancia.
- Finalmente, el riesgo de carácter específico es el que tiene importancia decisiva en una fase determinada y mucho menor en las demás.

Obsérvese que para el riesgo específico, los valores más altos de probabilidades y efectos se producen en instantes temporales diferentes, por lo que su producto (exposición) será bajo. Hay que tener presente que la decisión se toma en función de las exposiciones, por lo que los valores de probabilidades y efectos pueden no seguir un perfil decreciente, creciente o uniforme, y sí hacerlo la exposición resultante.

2.6.6. Técnicas para el análisis de riesgos identificadas

La comprensión de las causas de origen a los riesgos constituye la base de su gestión, pero no siempre es posible conocer las causas del origen de un riesgo concreto.

La figura 2.9 representa con más detalle una situación en la que una causa afecta a varios riesgos diferentes, y también se puede ver cómo un riesgo puede estar afectado por varias causas y que los riesgos pueden estar relacionados entre sí.

Existen técnicas concretas que ayudan a la identificación de riesgos. Se caracterizan por ser técnicas basadas en una utilización cualitativa orientada a entender las causas de los riesgos y su importancia relativa en un proyecto, seguido de un cierto análisis cuantitativo a partir de la información suministrada. Las técnicas de mayor utilidad son las siguientes:

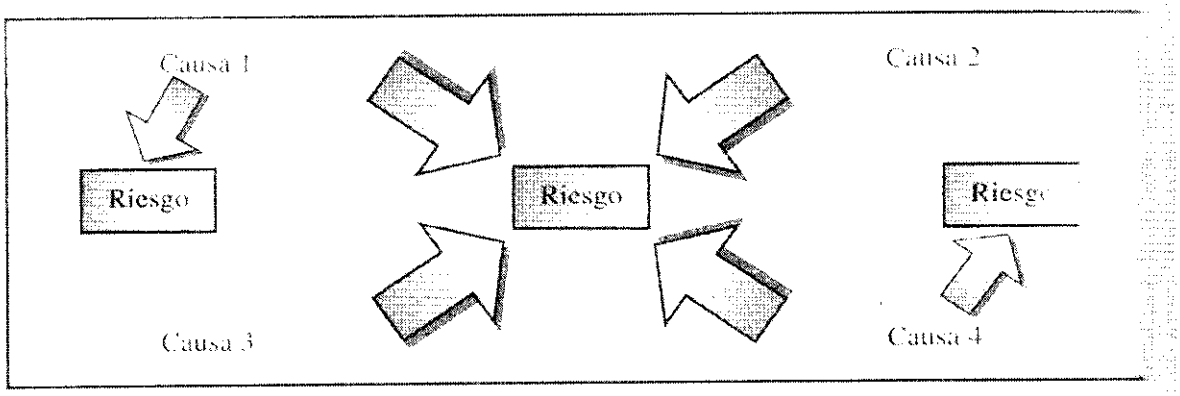


Figura 2.9. Causas de riesgos

Elaborado por: GMSM

Fecha: 21/08/2008

a. Diagramas de Ishikawa

Procedimiento utilizado para la identificación de causas de riesgos, aunque su origen es anterior y empleado en el diseño de productos.

b. Mapas de riesgos

Diagrama de todos los riesgos identificados y su gravedad en caso de producirse.

c. Risk Function Deployment (RFD)

Técnica basada en matrices para examinar las interacciones entre diversas perspectivas de los riesgos.

Constituye una evolución del QFD (Quality Function Deplovment), para tener en cuenta los aspectos de información de riesgos y correlación entre causas.

Las técnicas que se han seleccionado se basan en discusiones en grupo en las que la información depende de la percepción que tienen las diversas partes interesadas en el proyecto.

Parten del supuesto de que la elección adecuada de los miembros del grupo (experiencia y perfiles complementarios) permite disponer de la suficiente información como para facilitar la toma de decisiones posterior.

a. Diagramas de Ishikawa

Fueron ideados a partir de los años sesenta en Japón para organizar los datos recogidos durante lluvias de ideas para conocer las necesidades de los clientes en el

sector automovilístico. La justificación estribaba en la necesidad de incrementar el conocimiento de las necesidades de clientes desconocidos en el mercado japonés o en otros.

La construcción de un diagrama de Ishikawa parte de la existencia de unas causas primarias de las que se desprenden otras muchas. En la figura 2.10 se han identificado como causas primarias las correspondientes a las categorías principales de riesgos. En un caso real sería necesario identificar las causas primarias más importantes en el riesgo considerado. El diagrama continuará hasta que las causas sean lo suficientemente evidentes por sí solas como para que no se estime necesario seguir descubriendo otras causas derivadas.

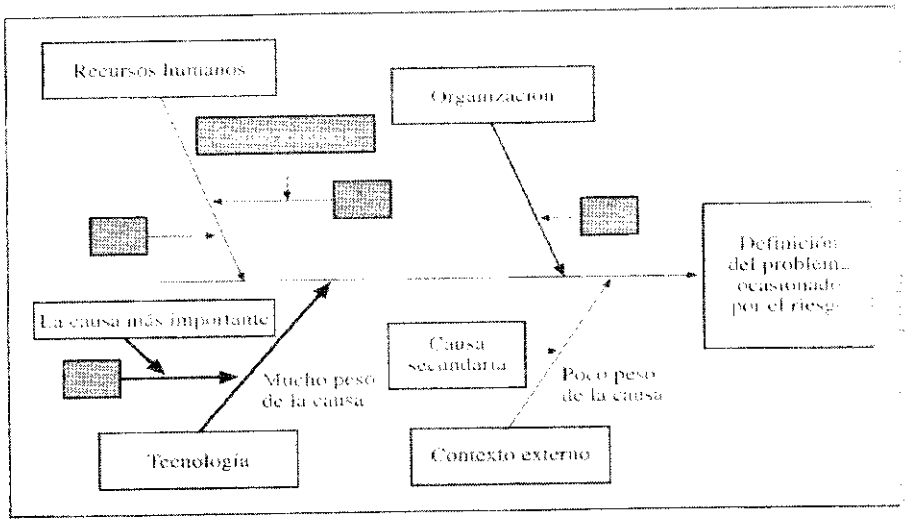


Figura 2.10. Diagramas de Ishikawa.

Elaborado por: GMSM

Fecha: 22/08/2008

2.6.7. Ejemplos de riesgos en la gestión de la tecnología

El número de riesgos potenciales en un proyecto determinado puede ser muy elevado. Únicamente con el objetivo de ofrecer un panorama de posibles riesgos tecnológicos que en la realidad pueden existir, se realiza la siguiente clasificación:

a. Riesgos asociados con la tecnología

Son aquellos cuyas causas principales residen en la tecnología (o tecnologías) empleadas en la organización. Téngase en cuenta que una tecnología puede tener una aplicabilidad limitada en una fase y otras, por el contrario, pueden emplearse en todo el desarrollo. Entre estos riesgos se encuentran:

- Inmadurez de las tecnologías a adoptar:
- Difícil aplicabilidad para los productos.
- Escaso conocimiento de su uso o consecuencias.
- Escalabilidad no probada totalmente.
- Débil soporte de las tecnologías requeridas:
- Escaso apoyo del proveedor de la tecnología.

b. Obsolescencia de la tecnología:

Abandono de la tecnología a incorporar o mejorar su uso durante el desarrollo del plan tecnológico.

c. Riesgos asociados con el contexto organizativo

Son aquellos cuyas causas principales dependen de la forma en la que el proyecto se ha estructurado dentro de una organización. Téngase en cuenta que, generalmente, la organización interna de un proyecto depende, a su vez, de cambios en la estructura de la organización, aunque no estén motivados por el proyecto en sí mismo. Entre estos riesgos se pueden destacar:

- Los procedimientos de gestión existentes previamente no son aplicables en este caso (hay que desarrollar uno nuevo):
- Las técnicas de estimación existentes no son aplicables.
- No existen series históricas.
- Modelo organizativo poco adecuado:
- Escasa relevancia del plan tecnológico dentro de la organización.
- Fuerte dependencia de aspectos externos.
- Dificultad en disponer del personal adecuado.
- Problemas en el acceso a recursos por simultaneidad con otros proyectos.

d. Riesgos asociados con los recursos humanos

Son aquellos cuyas causas principales dependen de la constitución del equipo de trabajo y de los conflictos internos entre sus componentes. Entre estos riesgos se encuentran:

- Inestabilidad en la composición del grupo de transición:
- Pérdida de personas importantes del equipo:
- Por causas imprevistas (ejemplo. accidente).
- Por causas previsibles (ejemplo. promoción).
- Retrasos en la composición del equipo.
- Dificultades en la contratación o asignación de personas.
- Escasa formación o experiencia del equipo de trabajo:
- Falta de personal con experiencia.
- No disponen de formación en alguna de las técnicas.
- Composición del equipo de trabajo:
- Mala asignación de responsabilidades.

c. Riesgos asociados con el contexto externo

Son aquellos riesgos que, aunque no directamente ligados al proyecto, le afectan de forma específica. Pueden proceder de cualquiera de las partes interesadas en el proyecto y de la relación entre ellas. Entre estos riesgos están:

- Riesgos financieros:
- Cambio del valor de la moneda.
- Modificación de los tipos de interés de los créditos.
- Retrasos en la recepción de las subvenciones.
- Riesgos políticos o de seguridad:
- No aceptación del producto o servicio.

- Abandono prematuro del país por falta de seguridad.
- Sabotaje contra las instalaciones.

• Riesgos con el proveedor tecnológico:

- Quiebra de los proveedores.
- Denuncia de la alianza tecnológica.

Un ejemplo de riesgo técnico que puede surgir a la hora de adoptar una nueva tecnología es que esa tecnología no sea válida para el tipo de productos que se desea realizar. Este riesgo surge con tecnologías inmaduras no utilizadas aún industrialmente.

Los principales componentes de este riesgo son:

Efecto: No es posible aplicar la técnica (o sólo en pequeña medida) en dominio de aplicación considerado.
Pérdidas: Gastos en tiempo y dinero (no aplicable a muchos productos).
Elecciones posibles: Trabajar con los proveedores de la tecnología para complementarla y combinar la tecnología propuesta con la convencional.

En definitiva, es un riesgo gestionable, y su análisis puede realizarse sobre la base de la construcción de un diagrama de Ishikawa. Una vez se haya construido el diagrama de Ishikawa con el nivel de detalle que se considere adecuado (seguramente varios niveles de causas en aquellas partes más conflictivas), comienza un proceso de

análisis de la importancia relativa de cada una de ellas con el fin de centrar la atención en las más relevantes.

En la figura 2.11 se ha construido un pequeño diagrama de Ishikawa que responde a las causas principales del riesgo identificado. Posiblemente, sería necesario detallar dos niveles más en el diagrama conjuntamente con el grupo de personas que han colaborado en su generación.

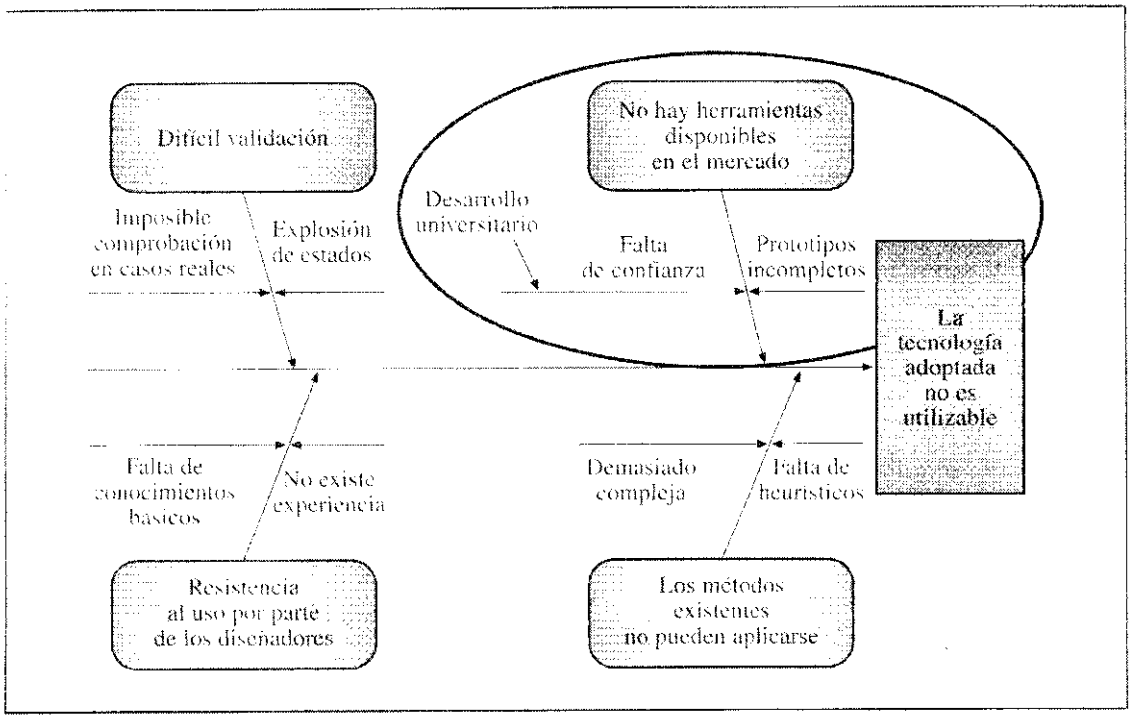


Figura 2.11. Ejemplo de diagrama de Ishikawa.

Elaborado Por: GMSM

Fecha: 23/08/2008

En la figura 2.11 se han señalado como ejemplo aquellas causas relacionadas con la falta de herramientas adecuadas en el mercado. Si ésa es la causa fundamental, los

gestores deberán idear planes de contingencia adecuados que vayan dirigidos a reducir la probabilidad de que esa situación se produzca o a reducir su impacto.
En el ejemplo que se está analizando, una vez se conocen las causas, es necesario preocuparse por los efectos del riesgo sobre el proyecto. El efecto es siempre una variable resumen de diversos factores más o menos relacionados entre sí.

En el proyecto considerado se puede suponer que el interés fundamental reside en aprovechar las ventajas de una nueva tecnología para generar productos que le permitan incrementar la cuota de mercado frente a sus competidores, de lo que se derivarán superiores beneficios. La introducción de un nuevo producto en mercado y su éxito dependen del momento en el que se produce. Un retraso en unos meses puede implicar la aparición de un nuevo producto competidor y una irreparable pérdida de la cuota de mercado prevista o la obsolescencia de la tecnología empleada, lo que hará que el tiempo de permanencia del producto en el mercado muy breve. Esta situación es muy grave en tecnologías que evolucionan muy rápidamente, como ocurre con las tecnologías de la información y de las comunicaciones.

Los factores considerados pueden al final resumirse en una cifra de inversión perdida. No obstante, calcular esta cifra a lo largo del tiempo implica disponer de mucha información, que habitualmente no está disponible, entre la que destaca el análisis de la probabilidad de ocurrencia con la determinación del perfil temporal del riesgo seleccionado.

Determinar los riesgos que existen, su caracterización. Evaluación y priorización es, por tanto, una tarea colectiva en la que deben participar todas las partes interesadas.

La gráfica de la figura 2.12 indica una situación en la que el riesgo de que la tecnología no sea escalable tiene lugar fundamentalmente en la fase de diseño de un proyecto piloto (por simplicidad, se resume el ciclo de vida en tres fases únicamente). También puede afectar ligeramente a la fase de especificación de requisitos, que podría haber adaptado sus resultados suponiendo que posteriormente (en el piloto) se emplea una determinada tecnología; igualmente, los resultados afectan a la difusión de la tecnología en la organización. Si el problema se detecta antes de comenzar la fase de desarrollo de un proyecto piloto de cierta complejidad, sería posible cambiar la tecnología y evitar el problema en la fase de difusión.

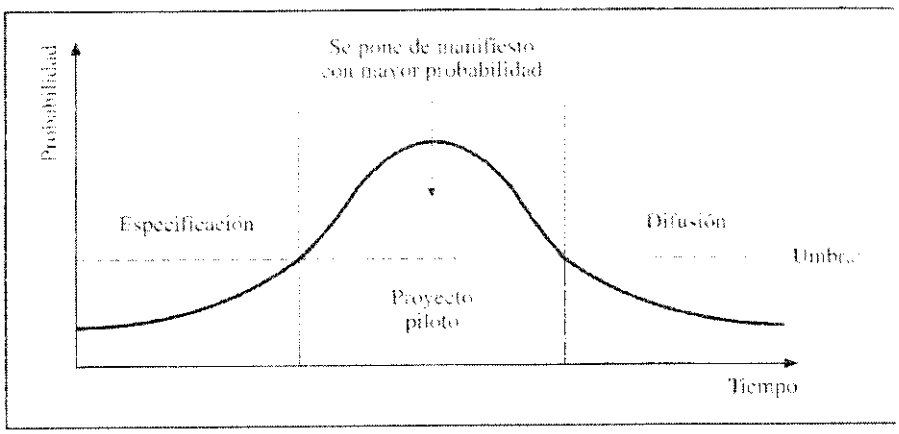


Figura 2.12. Ejemplo de perfil de riesgo: la tecnología no es escalable.

Elaborado por: GMSM

Fecha: 24/08/2008

En la figura 2.13 se representa tanto la exposición como sus factores internos (probabilidad y efecto). Es interesante observar que la exposición puede ser casi uniforme a pesar de que sus componentes pueden tener perfiles muy diferentes. También hay que tener presente la posible relación entre riesgos en el área en la que un riesgo supera un cierto umbral, pues pueden activarse otros riesgos relacionados con el primero.

Si la exposición conjunta es también muy alta, aparece un factor psicológico en el que se percibe un riesgo alto aunque individualmente no lo sea cada uno de los riesgos componentes. Simultáneamente, un buen tratamiento de uno de ellos puede hacer creer que todos han desaparecido, lo que no suele ser verdad. En estas valoraciones influye mucho la tolerancia al riesgo que tienen los gestores implicados.

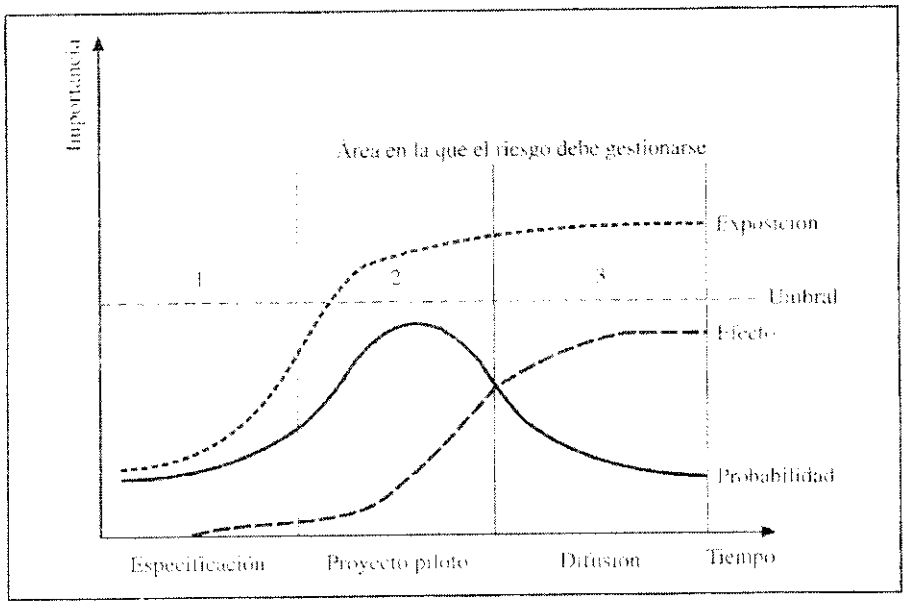


Figura 2.13. Cálculo de la exposición a un riesgo.

Elaborado por: GMSM

Fecha: 25/08/2008

Por su parte, aunque un riesgo se concrete en una fase, sus efectos pueden prolongarse mucho tiempo. Si un riesgo se ha detectado, una vez ocurrido, sólo queda intentar mitigar sus efectos, no prevenirlos.

El conocimiento de los riesgos existentes permite a los diseñadores ajustar las características de sus productos con el fin de reducir los riesgos más importantes:

- No es conveniente adoptar unas determinadas funciones o estrategias en el proyecto que impliquen unos riesgos con exposiciones muy altas.
- Se deben mantener aquellas características fundamentales deseadas por los clientes y asegurar que éstas se pueden llevar a cabo con el mínimo de riesgos técnicos posibles.

Por último, hay que tener muy en cuenta que una estimación excesiva de la exposición a los riesgos inhibe los procesos de innovación y retarda la incorporación de nuevas funciones a los productos, dado que es más difícil obtener las autorizaciones para llevar a cabo el proyecto. En estas circunstancias se debe buscar un equilibrio que no limite el emprendimiento de nuevos proyectos.

Como la percepción subjetiva del riesgo es un elemento importante, el carácter innovador y arriesgado actúa de catalizador de la innovación. Por tanto, hasta que no se conozcan los riesgos gestionables, no es posible establecer los planes de contingencia apropiados.

2.7. Técnicas de control de riesgos.

2.7.1. Actividades de control de riesgos

El proceso de evaluación de riesgos presentado permite planificar procesos concretos de control de aquellos riesgos que se ha decidido gestionar.

El objetivo en esta nueva etapa es determinar la respuesta más adecuada a cada riesgo, para lo cual se identifican las siguientes áreas de gestión:

Planificación. Determinar a lo largo del ciclo de vida del proyecto el momento más adecuado para tratar un riesgo determinado. Generalmente, esta situación implica la modificación de las tareas del proyecto y su secuenciamiento. Utilizando simulaciones se llega a seleccionar las alternativas más razonables.

Resolución. Puesta en marcha de un conjunto de acciones que mitiguen la exposición al riesgo. Debe tenerse presente que estas acciones pueden ser correctoras o previsoras con objeto de reducir su impacto o probabilidad.

Monitorización. Incluye las actuaciones relacionadas con la recogida de información para conocer hasta qué punto los riesgos identificados se van a producir y qué otros riesgos han surgido y será necesario gestionar, además se definen indicadores preliminares.

2.7.2. Elaboración de un plan de contingencia

Los planes de contingencia son los planes de actuación que el gestor introduce en un proyecto para poder enfrentarse a los riesgos, en su elaboración se debe tomar en cuenta la probabilidad de ocurrencia de los distintos escenarios. El término contingencia implica la existencia de un margen en la planificación para tener en cuenta diversos sucesos con una estimación inicial de los recursos necesarios y su presupuesto. Este margen afecta a la inclusión de tiempos adicionales para la ejecución de las tareas o a la disponibilidad de mayores recursos humanos de los que serían necesarios en caso de que todas las actividades se realizasen según los planes o de unas reservas económicas para hacer frente a gastos no previstos.

Debe tenerse en cuenta que si este proceso no va ligado a la existencia de un plan de actuación, la mera existencia de una reserva de fondos no reduce ni el impacto ni la probabilidad de ocurrencia. En realidad, estas contingencias cubren los costos adicionales por imprevistos. En estos mismos proyectos de construcción si existen normas muy rígidas relativas a riesgos laborales con el fin de evitar desgracias personales por accidentes que son sometidas a inspecciones de las administraciones competentes.

Los planes de contingencia agrupan todas las actuaciones necesarias para reducir las exposiciones a los riesgos. En todo caso, los planes de contingencia implican una modificación de la planificación ideal del proyecto.

En la figura 2.14 se observa cómo la introducción de niveles de contingencia razonables permite reducir los niveles de riesgo. Si se incrementa mucho la contingencia, aparecen efectos indeseados sobre otras variables (costo, tiempo o prestaciones), por lo que estas contingencias tienen un límite.

La figura también indica que cuando el riesgo inherente es muy elevado, no va a ser posible simplemente mediante la incorporación de contingencias reducirlo por debajo de un umbral. El posible rango de contingencias posibles no lo reduce suficientemente.

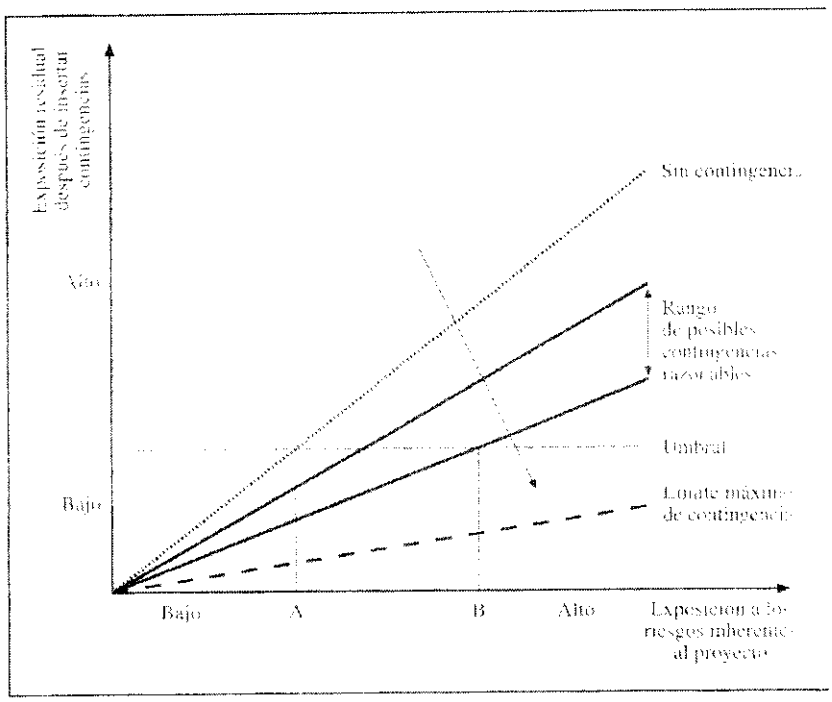


Figura 2.14. Efecto de la inclusión de contingencias.

Elaborado Por: GMSM

Fecha: 26/08/2008

Si el riesgo es poco importante, no sería necesario introducir ningún plan de contingencia. En la práctica, no es posible incrementar ilimitadamente las contingencias para que el riesgo desaparezca, pues ni los recursos económicos, ni el tiempo disponible ni las tecnologías utilizables lo permiten. Se indican a continuación algunos elementos típicos del plan de contingencia:

- Establecimiento de responsabilidades excepcionales en caso de producirse.
- Alternativas técnicas, económicas, logísticas, etc.
- Información técnica, económica o de objetivos tanto dentro como fuera de la empresa frente al riesgo, si se produce.
- Replanificación del plan tecnológico:
- Modificación del diagrama de tiempos.
- Modificación de los costos de las actividades.
- Inclusión de nuevas actividades.
- Indicadores de que el riesgo puede estar produciéndose.

En la figura 2.15 se pueden observar diferentes modificaciones a la planificación realizada de las actividades de un plan tecnológico como resultado en la gestión de riesgos de la puesta en marcha de un plan de contingencia:

Tarea T_1. No se ve afectada por el riesgo.

Tarea T_2. La estimación de tiempos se ve fuertemente afectada. Ello implica no sólo más costos, sino la disponibilidad durante más tiempo del personal asignado.

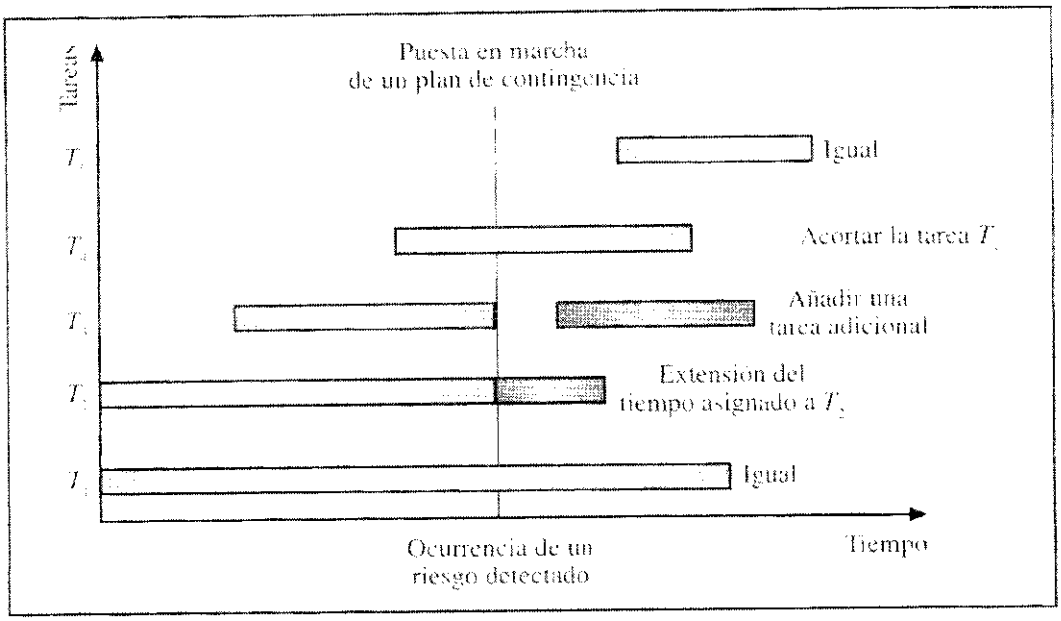


Figura 2.15. Efecto del plan de contingencia sobre la planificación.

Elaborado Por: GMSM

Fecha: 28/08/2008

Tarea T_3. Se mantiene, pero asociado a ello es necesario incorporar una nueva tarea adicional no contemplada anteriormente. Es posible que esta tarea requiera información o resultados de otras tareas.

Tarea T_4. Es posible reducirla debido a alguna oportunidad (factor de riesgo positivo) que ha aparecido o porque algunas de sus actividades ya no tienen sentido.

Tarea T_5. No se ve afectada por el riesgo. Figura 11.15. Efecto del plan de contingencia sobre la planificación.

En la figura 2.16 se representan ejemplos de posibles tareas y actividades modificables en un proyecto. Como ejemplo, en la tarea T-, es necesario incorporar la evaluación de la tecnología de un nuevo proveedor debido a fallos en los proveedores inicialmente considerados. Por su parte, en la tarea T3 se considera necesario iniciar un nuevo proyecto piloto para cubrir determinados aspectos que no pudieron evaluarse previamente por el anterior o que éste no pudo terminarse por causas de riesgo inicialmente consideradas.

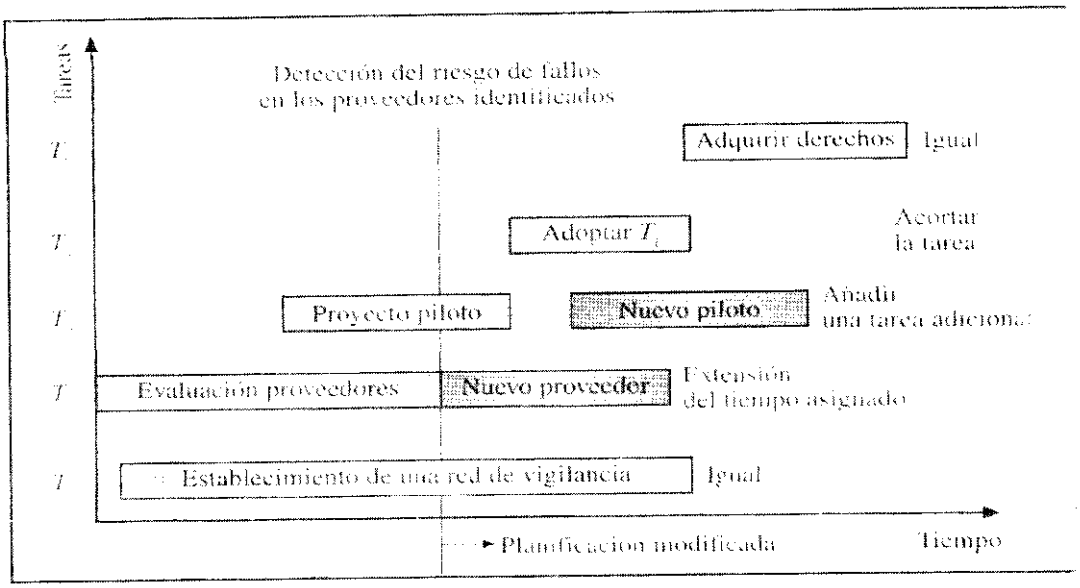


Figura 2.16. Ejemplo de actividades.

Elaborado Por: GMSM

Fecha: 28/08/2008

El plan de contingencia lo que debe establecer es la forma en la que estas modificaciones se pueden tener previstas para que su puesta en marcha sea inmediata. Por ejemplo, el nuevo caso piloto puede estar previamente identificado,

así como las personas que deberían hacerlo. Si es necesario, su puesta en marcha se puede hacer en muy poco tiempo.

La dificultad suele estribar en el reconocimiento de que el riesgo identificado está ocurriendo realmente y en que existe una resistencia de tipo psicológico a aceptar que una determinada planificación debe modificarse inmediatamente. Generalmente se retrasa la toma de decisión esperando que se solucione sólo, y la consecuencia es un incremento de las pérdidas asociadas al riesgo y la imposibilidad de usar los planes de contingencia previstos (pero no puestos en marcha). Como secuencia, no hasta con disponer de planes de contingencia, sino que es necesario ponerlos en marcha en el momento adecuado.

Ejemplo de plan de contingencia:

En los servicios de protección civil las situaciones de puesta en marcha de un plan de contingencia se producen continuamente. Imaginemos una actuación de inundación. La crecida del río puede estimarse por la cantidad lluvia (hay modelos que indican la subida a lo largo del tiempo en el nivel de las aguas en función del caudal que depende de las precipitaciones, etc.). El problema es que la crecida del río se puede monitorizar, pero hay que considerar la incertidumbre en la intensidad futura de las precipitaciones.

El problema para los servicios de protección civil es conocer cuándo deben evacuar a las personas que vivan en zonas protegidas. El plan de contingencia debe tener

establecido cómo realizar la evacuación, alojamientos temporales, medios de transporte, etc., y debe contar con la lógica resistencia de las personas afectadas a abandonar sus hogares. El propio plan de evacuación es un proyecto en sí mismo. La evacuación debe ser complementado con actividades de mitigación en los ámbitos sicológico y económico.

2.7.3. Monitoreo de los riesgos

El esfuerzo realizado en el proceso de evaluación de riesgos para determinar cómo se puede mitigar un riesgo se lleva a cabo en un momento determinado con la información disponible, pero deben tomarse las medidas concretas para monitorizar si cada riesgo evaluado se produce realmente.

Dado que no todos los riesgos tienen exposiciones que superan un umbral determinado durante toda la duración de un proyecto, el número de riesgos activos o potencialmente activos durante la duración del proyecto va cambiando con el tiempo.

La fase de monitorización debe actualizar de forma continua los riesgos que sea necesario tener en cuenta y avisar de este hecho a las unidades gestoras y ejecutoras.

Dentro de esta fase se deben tener en cuenta un amplio conjunto de actuaciones, entre las que destacan:

- Prueba en elementos piloto de los riesgos priorizados.
- Consolidar la experiencia sobre la tecnología en la propia empresa.

- Análisis de los proyectos afectados.
- Extracción de experiencias.
- Posibilidad de extrapolación de los resultados.
- Determinación del porcentaje de proyectos en los que la experiencia es aplicable.
- Planificar acciones específicas durante las diversas fases del proyecto.

Debe, finalmente, tenerse presente que el monitoreo continuo implica comprobar la existencia de unas señales asociadas a cada riesgo que han debido identificarse previamente durante la definición del plan de contingencia.

2.8. Estrategias utilizadas para minimizar el riesgo.

La perspectiva que se ha adoptado en este capítulo para el tratamiento de la gestión de riesgos ha sido la de limitarse a un enfoque de gestión de la tecnología en una organización. Existe, sin embargo, otro enfoque posible más global.

Este enfoque ha sido sistematizado por el sociólogo alemán Beckman (1986), desarrollando el concepto de sociedad del riesgo como característica de la sociedad industrializada en la que existe una probabilidad cada vez mayor de sufrir catástrofes repentinas (Chernobil) o larvadas (destrucción de la capa de ozono) como consecuencia del propio desarrollo tecnológico.

La consideración de que el uso de la tecnología no es neutro ha calado en la sociedad desde la primera revolución industrial.

El conocimiento de las consecuencias que sobre el empleo, los movimientos migratorios o la calidad de vida ha tenido la tecnología ha generado multitud de estudios y recomendaciones. Esta perspectiva ha sido profusamente analizada asociada a la comprensión de los efectos derivados de algunas tecnologías, como es la tecnología ligada a la energía nuclear o a los organismos genéticamente modificados, por citar dos casos que han generado fuertes polémicas en la opinión pública de los países desarrollados.

En función de ello se ha ideado y consolidado, en las sociedades desarrolladas, el denominado principio de precaución, por el que los poderes públicos imponen determinadas restricciones a la actividad de Investigación y desarrollo o al uso de la tecnología cuando pueda acarrear problemas de índole grave o simplemente desconocido en la sociedad.

Históricamente, el principio de precaución fue desarrollado en Alemania con la finalidad de justificar la intervención reguladora para limitar vertidos contaminantes al mar en ausencia de consenso sobre los daños que podrían causar. Posteriormente, fue introducido en la declaración de Bergen (1990), en la que se cita concretamente: Las políticas han de basarse en el principio de precaución. Las medidas ambientales deben anticipar prevenir y atacar las causas de la degradación ambiental. Si existe la amenaza de daños serios e irreversibles, la ausencia de ceniza científica completa no

puede utilizarse como razón para posponer medidas rígidas a prevenir la degradación ambiental.

Aunque inicialmente ligada a problemas medioambientales, la aplicación del principio de precaución también se extiende a diversas tecnologías, incluso mucho después de que el producto esté en el mercado, al conocerse otros factores de riesgo, y también cuando la oposición a la misma crece en intensidad y fuerza. En todo caso, la decisión se toma tras una evaluación de los riesgos y de los beneficios que se derivan de la extensión del uso de la tecnología.

Las decisiones que se han tomado en las últimas décadas en relación con la energía nuclear para primero detener la puesta en marcha de nuevas centrales y posteriormente cerrarlas planificadamente son ejemplos en este sentido.

Los problemas suscitados no se derivan de la necesidad de incrementar los controles necesarios, que, en todo caso, deben ser bienvenidos, sino de la importancia de mantener informada a la opinión pública sobre los riesgos reales derivados de determinadas tecnologías y evitar la extensión de psicosis colectivas sobre riesgos sin base científica para su sustento.

En caso de que se considere necesaria la acción, las medidas basadas en el principio de precaución deberán ser, para mantener un equilibrio:

- Proporcionadas al nivel de protección elegido.
- No discriminatorias en su aplicación.

- Transparentes y coherentes con medidas similares ya adoptadas.
- Basadas en el examen de los posibles beneficios y los costos de la acción o de la falta de acción.
- Sujetas a revisión, a la luz de los nuevos datos científicos.
- Capaces de designar a quién incumbe aportar las pruebas científicas necesarias para una evaluación del riesgo más completa.

Esta situación ha promovido el refuerzo de comités científicos, ya sea en configuraciones permanentes o ad hoc, para el tratamiento de determinados problemas (éticos, de salud pública o riesgo medioambiental) en los que la percepción del riesgo es más elevada. Sus dictámenes han servido para orientar a lo gobiernos en la regulación de la tecnología y permitir o no determinadas actividades.

La evolución constructiva de tecnologías es una manera de responder positivamente a los riesgos del uso de las tecnologías desde tres estrategias complementarias (López y Luján, 2000):

Desarrollo de variaciones alternativas. Se trata de promover tecnologías alternativas no disponibles en el mercado, por ejemplo mediante la financiación de líneas alternativas de investigación y desarrollo o mediante la subvención de la innovación en empresas en la dirección deseada por el gobierno (caso de las tecnologías limpias).

Modificación del ambiente de selección. A través del establecimiento de regulaciones o bien propiciando que compañías de seguros o asociaciones de fabricantes o consumidores establezcan requisitos de protección ambiental.

Creación o utilización de nexos tecnológicos. Entendidos como enlaces institucionales promovidos por los gobiernos para trasladar los requisitos del ambiente de selección a decisiones en las políticas de inversiones de las empresas.

CAPITULO III

DISEÑO DE LA PROPUESTA TÉCNICA PARA GESTIONAR LOS RIESGOS INFORMÁTICOS EN LA INDUSTRIA DE CARROCERÍAS METÁLICAS EN LA PROVINCIA DEL TUNGURAHUA

3.1. INTRODUCCIÓN

Con la llegada del siglo XXI las nuevas tecnologías van integrándose cada vez más en el mundo de la automoción, a todos sus niveles: equipamiento, seguridad, confort, etc., pero también en cuanto a reciclaje, cadena de producción, utilización de herramientas y equipos con base tecnológica, forma de venta y exposición al comprador.

La conciencia ambiental es otro factor que comienza a ser considerado en el momento de escoger los materiales y componentes necesarios para emprender el gran proyecto de renovar el sector automotriz.

La velocidad con la que se producen los progresos en el campo de la automoción ha aumentado durante este siglo considerablemente y todo apunta a que los próximos años continuarán por esta línea.

El crecimiento de la tecnología adaptada al sector automotriz representará un pilar básico en los próximos años en esta industria que refleja claramente los cambios que ha vivido el siglo. Pero todavía quedan muchos retos a los que buscar solución en los próximos años. Estos progresos irán dirigidos principalmente a tres factores:

- Desarrollo de nuevas técnicas de fabricación que reduzcan tiempo y costo del desarrollo de un automóvil.
- Mejora del combustible consumido, y reducción de las emisiones a la atmósfera.
- Búsqueda de un vehículo con características superiores en tanto que se mantienen o mejoran la seguridad, las prestaciones, las emisiones a la atmósfera y el precio.

El gran reto del siglo XXI en la industria carrocera es conseguir que los modelos sean más confortables, ecológicos y seguros en un futuro no muy lejano. Tras más de cien años de progresos, ahora las nuevas tecnologías pueden multiplicar la eficiencia de los vehículos, mejorar su seguridad y comodidad, y bajar su costo de adquisición y mantenimiento, alargando además su vida útil. Los vehículos del mañana deberán hacer frente a nuevas exigencias: mejorar los equipos de seguridad, adaptarse a las cada día más rigurosas normas de circulación y restricciones en materia de contaminación. Se transformarán en vehículos 'inteligentes' a través de la utilización de nuevas técnicas electrónicas que harán que la relación coche-usuario sea más cómoda. Estos avances empiezan a verse reflejados en los vehículos que circulan por nuestras calles y carreteras, sin embargo el proceso de renovación es lento.

Uno de los avances será fabricar vehículos con ayuda electrónica a la conducción, que equipará al vehículo con un 'copiloto' para casos de emergencia. El vehículo sin necesidad de conducirlo frenará o cambiará su trayectoria ante un obstáculo, leyendo y siguiendo las rayas de la carretera, incluso si nos dormimos conduciendo. Por medio del GPS, láser o satélite podremos comunicarnos con otros vehículos, saber datos sobre el tráfico, vías de acceso, itinerarios recomendados, mapas electrónicos. En muchos países se han emprendido grandes proyectos para digitalizar las principales ciudades y la red principal de carreteras. Además, deberá solucionarse el problema de la racionalización del tráfico, vías alternativas al transporte pesado por carretera, la reducción de la siniestralidad o el diseño de sistemas de transporte colectivo alternativos. Los vehículos del siglo XXI circularán sensiblemente más despacio pero con una mayor fluidez, fruto tanto de la preocupación por la seguridad como de la necesidad de contener la contaminación.

La ecología jugará un papel importante debido a la presión social y las duras normas anticontaminación de las diferentes administraciones. Por ello se deberán controlar las emisiones y consumos, mediante la mejora de los motores y combustibles utilizados. De hecho, ya se están consiguiendo resultados espectaculares: un vehículo actual consume la mitad de carburante de lo que se consumía hace 20 años, produciendo el doble de potencia. Uno de los objetivos es no seguir abusando de las limitadas reservas de petróleo existentes, que algunos dicen que se terminarán al ritmo actual a mediados del siglo próximo.

En cuanto a la producción y venta de vehículos, la época de la talla única y la uniformidad estética se ha acabado. Existe un producto para cada preferencia. Hasta hace pocos años los catálogos sólo distinguían entre vehículos pequeños, medianos y grandes. La única posibilidad de elección era en los tres o cuatro colores disponibles. Ahora se puede escoger entre una gran variedad de propuestas. En los próximos años se espera la llegada de gran cantidad de modelos. Muchos de ellos consecuencia directa las innovaciones tecnológicas. Es probable que las grandes urbes se vean pobladas de pequeños vehículos de baja polución y de propulsión eléctrica, híbrida o algo parecido.

La quiebra de las pequeñas empresas y su absorción por los grandes grupos hará que en pocos años solamente media docena de grupos industriales controle el mercado mundial de marcas de vehículos. Las fusiones son el pan nuestro de cada día en el sector automotriz. La industria de la automoción avanza hacia la concentración, proceso que desembocará en siglo próximo en la formación de media docena de colosos multinacionales que controlarán este sector.

El elevado número de víctimas mortales por accidente en carretera hace que los constructores pongan todos sus medios para mejorar la seguridad pasiva del vehículo. Las normas de seguridad, intentan minimizar el riesgo de lesiones de los ocupantes en el caso de que el accidente se consume. Se realizan estudios que analizan el comportamiento de los pasajeros en el momento de un choque: consisten en realizar una colisión entre un vehículo ocupado por muñecos y un muro de cemento. Las imágenes captadas durante el accidente son grabadas en cada milésima

de segundo que éste se produce. Estos ensayos confirman los cálculos que se efectúan en la construcción de un vehículo o los modifican.

Para mejorar la protección de los ocupantes, los ingenieros trabajan con especialistas en traumatología, con la finalidad de ver como se producen las lesiones y reducir el riesgo hasta límites aceptables. Estos estudios han permitido a los fabricantes mejorar la rigidez estructural del vehículo, crear zonas de deformación programada y reducir la agresividad de las carrocerías de los vehículos.

El diseño por computador ha permitido la instauración de procedimientos adecuados de industrialización y fabricación destinados a mejorar el confort, la seguridad, el respeto con el medio ambiente, desafíos fundamentales del sector automotriz.

Los responsables de la producción participan cada vez más en todos los procesos de diseño para lograr automotores más fáciles de construir y adaptados a los procedimientos industriales. Realizan estudios de simulación y pruebas con prototipos, construyendo piezas semejantes a la final, para comprobar y solucionar los hipotéticos problemas que se presentarán en la construcción de la misma. En estos momentos, la prioridad en el diseño de cadenas de montaje es la utilización de procesos de pintura al agua, la soldadura por láser, y la utilización de cárteres de aluminio para aligerar peso de los motores. El mecanizado a gran velocidad permite aumentar las cadencias de corte hasta 10 veces más rápido, con una menor deformación de la pieza tratada, y mayor calidad en el acabado final de la superficie.

Para economizar costos lo que hacen los fabricantes es convertir un modelo en base para los demás, aunque su apariencia sea muy distinta; o procedimientos como que las piezas llegan a la fábrica de montaje provenientes de los proveedores justo cuando van a ser montadas sobre el vehículo y disponer únicamente del material necesario para la producción diaria, sin almacenamiento de piezas, para que no suban los costos de producción.

Más del 75 % de los componentes de un vehículo, pueden ser reciclados. La mayoría de los modelos actuales incorpora ya una gran cantidad de piezas potencialmente reutilizables que pueden ser aprovechados para otros fines cuando este llegue a viejo. Éstas van identificadas a tal efecto con un código. Es más, muchos vehículos han comenzado a instalar elementos confeccionados con materiales reciclados. El sistema de reciclaje se realiza de manera muy similar para todos los vehículos. El proceso consiste en un metódico despiece del viejo. En el Ecuador existe un macroproyectos denominado de chatarrización promovido por el Gobierno Nacional. Sin embargo su avance en la ejecución a la fecha de esta investigación ha sido mínimo.

Los nuevos sistemas de «inteligencia artificial» controlarán todas las funciones de seguridad del vehículo. El automóvil del mañana se parecerá al actual en las formas y poco más al convertirse en una máquina provista de tecnología altamente sofisticada. Los Vehículos del futuro serán capaces de detectar que se aproxima su propietario y le permitirá abrirlo sin necesidad de que utilice la llave. En su lugar emplearemos una tarjeta provista de un microchip con código personalizado. El sistema hará posible que una central de seguridad y asistencia pueda determinar,

mediante satélites, en tiempo real, la ubicación del automóvil en caso de ser robado o accidente, o simplemente cuando no nos acordemos donde lo dejamos aparcado. El sistema, aprovechará las posibilidades que le brinda la telefonía móvil, la navegación por satélite y la última tecnología de alarmas para automóviles.

El conductor entablará diálogo con el computador central del automóvil para seleccionar y activar las distintas funciones. El usuario introducirá en el navegador el nombre del punto al que desea ir; de inmediato el sistema propondrá la ruta idónea, así como las posibles alternativas. La elección se efectuará de acuerdo a datos recibidos en tiempo real sobre la densidad de tráfico en las carreteras del itinerario, sus condiciones meteorológicas o el estado de las mismas. El guiado se realiza por medio de indicaciones gráficas en una pantalla del salpicadero por reproducciones de mapas a distintas escalas y con mensajes de voz. El actual volante será sustituido por un mando, que incluso será innecesario para viajar por largas autopistas ya que en este caso será sustituido por un sistema de gestión del tráfico. Ese gran cerebro artificial se encargará de dirigir los vehículos por medio de radares, láser, cámaras de video, sensores magnéticos en el pavimento, etc. Los vehículos respetarán una velocidad y una distancia adecuadas a las circunstancias, con lo que se evitarán congestiones y percances, permitiendo un aprovechamiento óptimo de la calzada. El futuro resulta poco alentador para los amantes de la conducción. El progreso del automatismo irá restando capacidad de decisión al conductor, que terminará por convertirse en un pasajero más, lo qué disminuirá el número de accidentes pero le restará muchos encantos a la conducción.

En todos estos avances están involucrados diversos riesgos relacionados con la tecnología desde la probabilidad de que la tecnología falle, hasta la acción de empresas y personas dedicadas a efectuar fraudes tecnológicos a través de bloquear dispositivos o dejar fuera de operación ciertos programas que permiten administrara los sistemas de inteligencia artificial.

Los riesgos son situaciones que eventualmente al concretarse pudieran evitar o dificultar que alguno o varios de los objetivos se lograran en la forma y con la oportunidad con que fueron planeados. En este sentido, la administración es la responsable de identificar los riesgos e implantar los controles apropiados que permitan su adecuado manejo.

Un aspecto fundamental en la evaluación de los riesgos estriba en que no solo es importante conocerlos sino administrarlos de manera eficiente; esto significa, determinar cuáles eliminar, cuales transferir o reducir y cuales aceptar. Siempre hay que tener presente la relación de costo beneficio, ya que resulta incosteable tratar de obtener una seguridad total o absoluta, es decir cero riesgos.

Las personas que procesan las operaciones y tienen la responsabilidad de cumplir las metas y objetivos, son las que mejor conocen los riesgos que pudieran dificultar el cumplimiento del objetivo correspondiente, por lo que también son los más capacitados para definir sus causas. Adicionalmente, son quienes pueden precisar las mejores acciones para administrar dichos riesgos, puesto que también conocen las condiciones del entorno, los recursos que se podrían asignar al efecto y desde luego,

la oportunidad con que deben aplicar las respectivas acciones de mejora. De manera consecuente se puede acordar que los objetivos y riesgos inherentes sean el punto central en los talleres de carrocerías, lo cual puede ser una estrategia extraordinaria para convencer a los administradores, de la utilidad de establecer la evaluación de los procesos de control.

Existen riesgos que pueden ser comunes a varios tipos de organizaciones, sin embargo, la evolución tecnológica, ha tenido un impacto significativo en la aparición de nuevas posibles contingencias, el profesional en informática contribuye con su experiencia y conocimiento a la definición especifica de los riesgos en la organización a la que sirve.

La provincia del Tungurahua produce el 70% de las carrocerías que circulan por las carreteras ecuatorianas, la mayoría de talleres son artesanales, han incluido mínimos avances tecnológicos en sus procesos, sin embargo el no contar dentro de su personal con especialistas en sistemas, supone un riesgo de disminución de la competitividad.

Los sistemas de producción tienden a automatizarse, para producir más vehículos en menor tiempo, en el caso de que los sistemas fallen el ensamblaje, no sólo puede retrasarse sino incluso ocasionar grandes daños económicos. Los fabricantes de automotores están buscando una cadena de suministro más eficiente para apoyar el desarrollo de nuevos modelos, ciclos de vida más cortos y mayores expectativas de servicios complementarios. Se deben diseñar y gestionar cadenas de suministro

completas para la distribución de entrada (ensamblaje de autos) y mercado posterior (repuestos). Para obtener una óptima flexibilidad y rapidez.

Con este panorama existen expectativas ciertas del crecimiento de la industria carrocera, para cumplir con los requerimientos que contribuyan a la renovación del parque automotor de transporte público, los fabricantes de carrocerías deben implementar ambiciosos programas de innovación tecnológica, sin embargo esto conlleva riesgos, que deben ser gestionados de forma técnica.

3.2. Componentes del plan de contingencias.

Se presenta a continuación un modelo para la elaboración de un plan de contingencia. Contiene los puntos principales que se deben tomar en consideración, las condiciones de los recursos informáticos utilizados en el sector de las carrocerías metálicas.

Debemos tener en cuenta que mucho dependerá de la infraestructura de la empresa y de los servicios que ésta ofrezca para determinar un modelo de desarrollo de plan, no existe un modelo único para todos, lo que se intenta es dar los puntos más importantes a tener en cuenta. Las fases se podrían resumir en las siguientes:

- **Planificación:** preparación y aprobación de esfuerzos y costos.
- **Identificación de riesgos:** funciones y flujos del proceso de la empresa.
- **Identificación de soluciones:** Evaluación de Riesgos de fallas o interrupciones.

- **Estrategias:** Otras opciones, soluciones alternativas, procedimientos manuales.
- **Documentación del proceso:** Creación de un manual del proceso.
- **Realización de pruebas:** selección de casos soluciones que probablemente funcionen.
- **Implementación:** creación de las soluciones requeridas, documentación de los casos.
- **Monitoreo:** Probar nuevas soluciones o validar los casos.

3.2.1. Planificación

a. Diagnóstico

Cada vez que nos encontremos en una actividad que requiere el diseño de una propuesta de solución para un determinado problema, es necesario siempre la revisión exhaustiva de cada uno de los componentes que conforman el sistema, es por esta razón siempre debemos de realizar una etapa de diagnóstico para poder asegurar que las acciones de solución propuestas tengan un fundamento realista.

1) Organización estructural y funcional.

En este aspecto se deben describir y analizar los departamentos en los que se divide la empresa, haciendo referencia de las funciones más importantes que desempeñan cada una de ellos, priorizando tales funciones en relación al sistema productivo de

bienes o servicios que desarrollan. Estas empresas tienen organigramas que se rigen por manuales de organización y funciones.

2) Servicios y/o bienes producidos.

En este punto se hará referencia sobre los bienes y/o servicios que produce la empresa o institución según el orden de importancia por la generación de beneficios. Si la empresa produce más de un bien la prioridad será determinada según el criterio de los directivos.

Además se debe elaborar una base de datos de clientes priorizando de acuerdo a la magnitud de los bienes o servicios que consumen. También se realizará un breve análisis del mercado de consumo de los bienes y servicios producidos, identificando las zonas o sectores de mayor consumo.

3) Servicios y materiales utilizados.

Con relación a los servicios utilizados se debe elaborar un directorio de empresas o instituciones que abastecen de energía, comunicación, transporte, agua, salud y otros servicios resaltando la importancia de ellos en el sistema de producción de la empresa y verificando la seguridad de los servicios sin problemas de afectación por algún tipo de problema. También debe hacerse un directorio de todas las empresas abastecedoras de materias primas o insumos para la producción de información.

4) Inventario de recursos informáticos.

El inventario de recursos informáticos se realizará por departamentos y en forma clasificada:

- **Computadoras:** Intel, AMD, impresoras, scanners, otros.
- **Programas:** De sistemas operativos, procesadores de textos, hojas de cálculo, lenguajes de programación, software de base.
- **Aplicativos informáticos:** Del sistema de contabilidad, de trámite documentario, planillas, almacén, ventas, presupuesto, personal.
- **Equipos empotrados:** De industrias: hornos y envasadoras. De banca y Seguros, cajeros automáticos y bóvedas. De oficinas, centrales telefónicas.

Estos inventarios deberán hacerse a través de formularios sistemáticamente elaborados. El procesamiento de este inventario puede ser de dos tipos:

Proceso Automatizado. Utilizando herramientas informáticas de diferente nivel, grado de detalle y costo, que pueden acelerar el tiempo de la toma del inventario, procesamiento de datos y emisión de resultados.

Proceso Manual. Utilizando formatos de recopilación de información. El conocimiento del inventario de estos recursos nos permitirá hacer una evaluación de los riesgos de la operatividad de los sistemas de información. Estos formatos contienen dos partes:

a) Datos componentes: Donde se registran los datos básicos de ubicación, identificación y características primarias, así como también su importancia, compatibilidad y adaptabilidad.

b) Análisis del proceso de adaptación del componente: Incluye datos de costos, fecha de culminación, medios utilizados y medidas de contingencia.

b. Planificación

La fase de planificación es la etapa donde se define y prepara el esfuerzo de planificación de contingencia/continuidad. Las actividades durante esta fase incluyen:

- Definición explícita del alcance, indicando qué es lo que se queda y lo que se elimina, y efectuando un seguimiento de las ambigüedades. Una declaración típica podría ser, "La continuidad de los negocios no cubre los planes de recuperación de desastres que ya fueron emitidos."
- Definición de las fases del plan de eventos (por ejemplo, los periodos preevento, evento, y post-evento) y los aspectos sobresalientes de cada fase.
- Definición de una estrategia de planificación de la continuidad del negocio de alto nivel.
- Identificación y asignación de los grupos de trabajo iniciales, definición de los roles y responsabilidades.
- Definición de las partes más importantes de un cronograma maestro.

- Identificación de las fuentes de financiamiento y beneficios del negocio; revisión del impacto sobre los negocios.
- Duración del enfoque y comunicación de las metas y objetivos, incluyendo los objetivos de la empresa.
- Definición de estrategias para la integración, consolidación, rendición de informes y arranque.
- Definición de los términos clave (contingencia, continuidad de los negocios, etc.)
- Desarrollo de un plan de alto nivel, incluyendo los recursos asignados.
- Obtención de la aprobación y respaldo de la empresa y del personal gerencial de mayor jerarquía. Provisión de las primeras estimaciones del esfuerzo.
- El plan debe ser ejecutado independientemente de las operaciones y procedimientos operativos normales.
- Las pruebas para el plan serán parte de (o mantenidas en conjunción con) los ejercicios normalmente programados para la recuperación de desastres, las pruebas específicas del plan de contingencia de los sistemas de información y la realización de pruebas a nivel de todos los clientes.
- No habrá un plan de respaldo, y tampoco se dará una reversión ni se podrá frenar el avance del plan de contingencia.
- Si ocurre un desastre, una interrupción, o un desfase de gran magnitud en los negocios de la empresa durante el período del calendario de eventos, se pondrán en práctica los planes de continuidad de los negocios o de contingencia.

- Si la organización ha puesto en moratoria los cambios al sistema, se deben permitir las excepciones a dicha moratoria solamente para los cambios de tipo regulador o para los problemas más importantes que afecten la producción o las operaciones de la empresa, y solamente después de haber obtenido la aprobación del nivel ejecutivo.

3.2.2. Identificación de riesgos

El objetivo de esta fase busca minimizar las fallas generadas por cualquier caso en contra del normal desempeño de los sistemas de información a partir del análisis de los proyectos en desarrollo, los cuales no van a ser implementados a tiempo.

El objetivo principal de la fase de reducción de riesgo, es el de realizar un análisis de impacto económico y legal, determinar el efecto de fallas de los principales sistemas de información y producción de la institución o empresa.

a) Análisis y evaluación de riesgos

Es necesario reconocer y reducir de riesgos potenciales que afecten a los productos y servicios; es por ello que se considera dentro de un plan de contingencia, para favorecer el cumplimiento de los objetivos institucionales.

El análisis y evaluación de riesgos se desarrolla en dos escenarios:

1. Para empresas que desarrollan planes de contingencias su plan de adaptación y no tienen soluciones adecuadas.

Este proceso consta de:

a. Evaluar el impacto de los procesos críticos.

b. Valorar la certificación de los proveedores.

c. Privilegiar proyectos, eliminando aquellos que resultan extemporáneos.

d. Detectar deficiencias ante cambios en los sistemas afectados.

e. Guardar copias de información empresarial mediante convenios de soporte.

2. Empresas que a la fecha no han tomado previsión.

Para aquellas empresas que no están realizando planes de contingencia, el análisis y evaluación de riesgos.

Consta de lo siguiente:

a. Realización un diagnóstico integral del sistema de información.

b. Elaborar una lista de servicios afectados evaluando su importancia, magnitud del impacto, cuantificar con niveles A, B, C u otro.

c. Identificar todos los procesos de los servicios afectados.

d. Analizar sólo los procesos críticos de los servicios.

b) Identificar los procesos críticos

Al igual que las situaciones de falla, las alternativas pueden ser infinitas. Por ende, se deben identificar muchas para ser capaces de seleccionar las mejores opciones de contingencia.

Para empezar comience por los riesgos ya identificados como prioridades máximas porque causarían el mayor impacto negativo en los servicios y en las funciones críticas de su organización.

c) Análisis de las operaciones actuales

El análisis de operación del método actual de trabajo (es decir, cómo y en qué orden su organización obtiene funciones comerciales) puede revelar las oportunidades para reducir, eliminar o simplificar ciertas operaciones o procesos.

Algunas funciones probablemente pueden ser realizadas por terceros sin pérdida de control. Probablemente pueden reducirse algunas operaciones en términos de pasos e interfaces que ellos requieren. Un almacén parcialmente automatizado puede requerir 30 acciones manuales separadas para llenar una orden grande. Si la organización emprende proyectos serios de mejoramiento y técnicamente diseñados puede mejorar su eficiencia en 33 por ciento, con lo cual el mismo proceso requerirá sólo 20 acciones manuales, la eficiencia incrementada puede liberar algunos recursos que pueden usarse en otra parte. Por supuesto, tales acciones van de la mano con la

capacitación. Desde el punto de vista de los sistemas de información, tales consideraciones pueden ser cruciales porque puede haber una necesidad de revertir a las operaciones manuales y en ciertos casos sostener las operaciones existentes.

Si consideramos que "No existe producto y/o servicio sin un proceso. De la misma manera, que no existe proceso sin un producto o servicio". Aunque no todos los procesos generan un producto o servicio útil (creando valor agregado) para la empresa. Por lo que es necesario realizar un análisis de las operaciones y los procesos que involucran.

- Organización. Cualquier grupo, empresa, corporación, planta, oficina de ventas, etc.
- Función. Un grupo dentro de la organización funcional. Funciones características serían ventas y mercadeo, contabilidad, ingeniería de desarrollo, compras y garantía de calidad.
- Proceso. Cualquier actividad o grupo de actividades que emplee un insumo, le agregue valor a éste y suministre un producto a un cliente externo o interno.
- Los procesos utilizan los recursos de una organización para suministrar resultados definitivos.
- Proceso de producción. Cualquier proceso que entre en contacto físico con el hardware o software que se entrega a un cliente externo, hasta aquel punto en el cual el producto se empaca. Esto no incluye los procesos de embarque y distribución.

- Proceso de la empresa. Todos los procesos de servicios y los que respaldan a os de producción (por ejemplo, de pedidos, proceso de cambio en ingeniería, e planilla, diseño del proceso de manufactura). Un proceso de la empresa consiste en un grupo de tareas lógicamente relacionadas que emplean los recursos de la organización para dar resultados definidos en apoyo de los objetivos de la organización.

Al emplear estas definiciones, se puede observar que casi todo lo que hacemos es un proceso y que los procesos de la empresa desempeñan un papel importante en la supervivencia económica de nuestras organizaciones. En todas las organizaciones existen, literalmente, centenares de procesos que se realizan diariamente. Más del 80% de éstos son repetitivos, cosas que hacemos una y otra vez. Estos procesos repetitivos (áreas administrativas, manufactureras e intermedias) pueden y deben controlarse, en gran parte, tal como se vigilan los de manufactura. Se manejan muchos procesos de las instituciones y empresas que son tan complejos como el proceso de manufactura.

d) Uso de la técnica de análisis de procesos

Consideremos para el uso de la técnica de análisis de procesos:

- El ciclo de vida empieza con la descripción de un proceso basado en las metas del proyecto, mientras se utilizan los recursos descritos del proceso.
- El proceso se fija al asignar los recursos.

- El proceso puede instalarse en una máquina o pueden ser procedimientos a seguir por un grupo de personas.
- El proceso es supervisado y medido durante su uso.
- Los datos obtenidos de esta medida se evalúan durante todo el tiempo que se desenvuelva el proceso. Una descripción del proceso existente puede empezar con un informe actual, obtenido de la supervisión y documentación del proceso.

El Proceso de dirección del ciclo de vida contiene la descripción de los componentes del proceso y la producción de los principales insumos de trabajo. La descripción del proceso funcionalmente se descompone en él:

1. Análisis del proceso
2. Plan del proceso
3. Aplicación del proceso.

El análisis del proceso involucra identificación, mientras se analiza el proceso, y los requisitos del proceso. El plan del proceso involucra el modelamiento de la arquitectura y la descomposición funcional del proceso. La aplicación del proceso involucra llevar a cabo el plan del proceso para crear tareas a realizarse y proporcionar la capacitación necesaria para las personas que realicen dichas tareas.

También la aplicación del proceso involucra la preparación del proceso para su actuación en la empresa o institución, el proceso consiste en los detalles específicos del proyecto y fijar los recursos necesarios.

Diagrama del proceso descompuesto

A continuación presentamos una lista de procesos típicos de las empresas definidos por IBM. Esto ayudará a definir los procesos de la empresa.

- Manejo de índices.
- Diseño de sistemas de control.
- Desarrollo de comunicaciones avanzadas.
- Diseño de componentes de cable.
- Prueba de diseño.
- Revisión de diseño y materiales
- Revisión de documentos
- Especificación de diseño a alto nivel
- Coordinación entre divisiones
- Diseño lógico y verificación
- Calificación de componentes
- Identificación de recursos
- Diseño del sistema de energía
- Divulgación del producto
- Confiabilidad y utilidad del sistema
- Requerimiento del sistema
- Diseño interactivo de sistemas para el usuario
- Análisis de la competencia
- Apoyo de los sistemas de diseño

- Desarrollo de la información
- Instrumentos de diseño físico
- Diseño de sistemas
- Gerencia de cambio en ingeniería.

Es el procedimiento por el cual se estudian los procesos dentro de una secuencia (Línea de producción) de producción o provisión de servicios, que a continuación son presentados, teniendo en consideración:

- Las Funciones Institucionales.
- Los procesos derivados.
- Los subprocesos.

3.2.3. Identificación de soluciones

Un proyecto de plan de contingencia no sirve si se queda en plan o papel. Un plan de contingencias debe contemplar todos los procesos institucionales sean estos manuales y/o automatizados, evaluando el volumen de información o materiales afectados, a fin de definir la complejidad de los sistemas.

La magnitud, de un plan de contingencia será proporcional a la complejidad, importancia, costo del servicio al cual está destinado a proteger y su riesgo asociado.

El esquema general del plan de contingencias de los sistemas de información, está constituido por 3 grandes fases:

1. Fase de Reducción de Riesgos
2. Fase de Recuperación de Contingencia
3. Fase de Organización de un Sistema de Alerta contra Fallas

Se debe tener en cuenta al determinar los objetivos, en qué parámetros generales se va a sustentar, para poner en operación el plan de contingencias.

CUADRO 3.1.

Matriz de planificación de contingencia y ejemplos

OPCIONES	OPERACIÓN MANUAL	REEMPLAZO	EXTERNALIZACION DEL SERVICIO
Reparación rápida y de defecto	Recurra al proceso manual sólo en caso de clientes prioritarios.	Tenga disponible software de repuesto que cumpla con los requisitos	Use personal temporalmente para llenar brecha
Reparación parcial	Use hojas de cálculo o base de datos para ofrecer alguna de la funcionalidad original del sistema (fecha de captura).	Use base de datos u otros paquetes para reemplazar la funcionalidad del sistema	Haga que el contratista procese los pagos en sus propias instalaciones
Reparación total	Ofrezca operaciones totalmente funcionales a través del proceso manual, utilizando personal adicional si es necesario	Elimine esfuerzos de reparación e implemente un sistema comercial funcional, rápidamente	Entregue el manejo de la plantilla de pago a una firma comercial especialista

Elaborado Por: GMSM

Fecha: 08/11/2008.

En cualquier caso, sus planes deben identificar dependencias e impactos y, al mismo tiempo, los recursos necesarios para implementar cada alternativa de contingencia. Se deben buscar alternativas "creativas", que logren el efecto de mitigar el impacto en caso de una falla. En la siguiente tabla se muestra la matriz del plan de contingencia y algunos ejemplos.

a. Identificación de Alternativas.

Como indicamos anteriormente, un buen método para identificar alternativas consiste en revisar los planes de administración de emergencia o recuperación de fallas.

Estos son algunos ejemplos de alternativas que pudieran ayudarle al inicio del proceso de preparación.

- Planifique la necesidad de personal adicional para atender los problemas que ocurran.
- Recurra al procesamiento manual (de facturas, órdenes, cheques, etc.) si fallan los sistemas automatizados.
- Planifique el cierre y reinicio progresivo de los dispositivos y sistemas que se consideran en riesgo.
- Instale generadores si no tiene acceso a la red de energía pública.
- Disponga del suministro adicional de combustible para los generadores, en caso de fallas eléctricas prolongadas.
- Disponga de bombas manuales de combustible y úselas si fallan las electrónicas.
- Elaborar un programa de vacaciones que garantice la presencia permanente del personal.
- No haga nada y vea qué pasa – esta estrategia es algunas veces llamada arreglar sobre falla.

b. Identificación de eventos activadores.

Cuando el equipo de planificación seleccione la mejor alternativa de contingencia, debe definir los activadores que provocarán la implementación del plan. Los activadores son aquellos eventos que permitirán decir "OK", es el momento de pasar al plan B". Incluyen las fallas de los sistemas, u otros eventos que hacen evidente la necesidad de implementar el plan de contingencia.

Sin embargo, muchos eventos activadores serán predefinidos como puntos de decisión "pasar/no pasar", el evento que active la decisión de poner en funcionamiento el proceso alternativo puede ser una alerta establecida a una falla anticipada.

La información necesaria para definir los activadores para cada sistema o proceso, provendrá tanto del programa de implementación para los sistemas de información, como de los requerimientos de tiempo desplegados para cada plan de contingencia.

A continuación se muestran algunos ejemplos de los tipos de eventos que pueden servir como activadores en sus planes de contingencia:

- Información de un vendedor respecto a la tardía entrega o no disponibilidad de un componente de software.
- Tardío descubrimiento de serios problemas con una interface.

- Tempranas (no anticipadas) fallas del sistema – corrección/reemplazo no está lista para sustituir.
- Fallas del sistema (datos corruptos en informes o pantallas, transacciones pérdidas, entre otros).
- Fallas de interfaces –intercambios de datos no cumplen los requisitos.
- Fallo de la infraestructura regional (energía, telecomunicaciones, etc.)
- Problemas de implementación (por ejemplo, falta de tiempo o de fondos).
- Aseveraciones falsas o erróneas sobre el cumplimiento, descubiertas demasiado tarde para iniciar las acciones de cumplimiento.

Cabe mencionar que, para desarrollar este proyecto es necesario conocer los lineamientos generales del sistema afectado, es decir el tipo de producción al cual pertenece pudiendo pertenecer al sector de bienes o al sector servicios. Una vez establecido a que rubro de la producción pertenece, identificamos el departamento o área ligada y las funciones que en ella realiza, las áreas principales pueden ser:

- Contabilidad
- Administración
- Finanzas
- Comercialización
- Producción
- Seguridad
- Logística
- Sistemas de información

Se deberán identificar las fallas potenciales que puedan ocurrir para cada sistema, considerando la provisión de datos incorrectos, y fiabilidad del sistema para la institución, y así desarrollar una lista de alternativas priorizadas de fallas.

c. Identificación de Soluciones

El objetivo es reducir el costo de encontrar una solución en la medida de lo posible, a tiempo de documentar todos los riesgos identificados.

Actividades importantes a realizar:

- La asignación de equipos de solución para cada función, área funcional o área de riesgo de la organización.
- La asociación de soluciones con cada riesgo identificado- se recomienda tener un abanico de alternativas de soluciones, por que las soluciones se analizaran y se compararan posteriormente.
- Comparar los riesgos y determinarles pesos respecto a su importancia crítica en término del impacto de los mismos.
- Clasificar los riesgos.
- La elaboración de soluciones de acuerdo con el calendario de eventos.
- La revisión de la factibilidad de las soluciones y las reglas de implementación.
- La identificación de los modos de implementación y restricciones que afectan a las soluciones.

- La definición e identificación de equipos de acción rápida o equipos de intensificación por área funcional o de negocios de mayor importancia.
- Sopesar las soluciones y los riesgos y su importancia crítica en lo que respecta a su eficacia y su costo, siendo la meta la solución más inteligente.

La revisión de soluciones comparándolas con el nivel mínimo aceptable de resultados o servicios.

d. Fallas genéricas funcionales de los sistemas a tener en consideración.

Se han encontrado varias fallas comunes a muchos sistemas de computación. Estos incluyen:

Autentificación. En muchos sistemas, los usuarios no pueden determinar si el hardware y el software con que funcionan son los que se supone que deben ser. Esto hace fácil al intruso reemplazar un programa sin conocimiento del usuario. Un usuario puede inadvertidamente teclear una contraseña en un programa de entrada falso.

Cifrado. La lista maestra de contraseñas debe ser almacenada, cifrada, lo que a menudo no se hace.

Implementación. Un diseño bien pensado de un mecanismo de seguridad puede ser implementado de forma improcedente.

Confianza implícita. Un problema corriente, una rutina supone que otra está funcionando bien cuando, de hecho, debería estar examinando detenidamente los parámetros suministrados por la otra.

Compartimiento implícito. El sistema puede depositar inadvertidamente información importante del sistema, en un espacio de direcciones del usuario.

Comunicación entre procesos. El intruso puede usar un mecanismo de SEND/RECEIVE para probar varias posibilidades. Por ejemplo el intruso puede pedir un recurso del sistema y suministrar una contraseña. La información devuelta puede indicar "contraseña correcta", confirmando la contraseña adivinada por el intruso.

Verificación de la legalidad. El sistema puede no estar realizando una validación suficiente de los parámetros del usuario.

Desconexión de línea. En tiempos compartidos y en redes, cuando la línea se pierde (por cualquier razón), el sistema operativo debe inmediatamente dar de baja del sistema al usuario o colocar al usuario en un estado tal, que sea necesaria la reautorización para que el usuario obtenga de nuevo el control. Algunos sistemas permiten que un proceso "flote" después de una desconexión de línea. Un intruso puede llegar a obtener el control del proceso y usar cualesquier recurso a los que tenga acceso el proceso.

Descuido del operador. Un intruso puede engañar a un operador y hacer que cargue un paquete de disco con un sistema operativo falso.

Paso de parámetros por referencia en función de su valor. Es más seguro pasar los parámetros directamente en registros, que tener los registros apuntando a las localidades que contienen los parámetros. El paso por referencia puede llevar a una

situación en la cual los parámetros, pueden aún encontrarse en el espacio de direcciones del usuario después de una verificación de la legalidad. El usuario podría así suministrar parámetros legítimos, verificarlos, y modificarlos justo, antes de ser utilizados por el sistema.

Contraseñas. Las contraseñas son, a menudo, fáciles de adivinar u obtener mediante ensayos repetidos. Debiendo implementarse con número máximo de intentos infructuosos.

Entrampamiento al intruso. Los sistemas deben contener mecanismos de entrampamiento para atraer al intruso inexperto. Es una buena primera línea de detección, pero muchos sistemas tienen trampas inadecuadas.

Privilegio. En algunos sistemas hay demasiados programas con muchos privilegios. Esto es contrario al principio del menor privilegio.

Confinamiento del programa. Un programa prestado de otro usuario puede actuar como caballo de Troya: puede robar o alterar los archivos del usuario que los prestó.

Residuos. A menudo el intruso puede encontrar una lista de contraseñas con sólo buscar en una papelera. Los residuos se dejan a veces en el almacenamiento después de las operaciones rutinarias del sistema. La información delicada debe ser siempre destruida.

Blindaje. Una corriente en un cable genera un campo magnético alrededor de él; los intrusos pueden de hecho conectarse a una línea de transmisión o a un sistema de computación sin hacer contacto físico. Puede usarse el blindaje eléctrico para prevenir tales "intrusiones invisibles",

Valores de umbral. Están diseñados para desanimar los intentos de entrada, por ejemplo. Después de cierto número de intentos inválidos de entrar al sistema, ese usuario debe ser bloqueado y el administrador del sistema, advertido.

e. Ataques genéricos a sistemas operativos

Ciertos métodos de penetración se han utilizado efectivamente en muchos sistemas.

Asincronismo. Con procesos múltiples que progresan de forma asincrónica, es posible que un proceso modifique los parámetros cuya validez ha sido probada por otro, pero que aún no ha utilizado. Con esto, un proceso puede pasar valores malos a otro, aún cuando el segundo realice una verificación extensa.

Rastreo. Un usuario revisa el sistema de computación, intentando localizar información privilegiada.

Entre líneas. Se usa un terminal especial para conectarse a la línea de comunicación mantenida por un usuario dado de alta en el sistema, que está inactivo en ese momento.

Código clandestino. Se hace un parche en el sistema operativo bajo la pretensión de una depuración. El código contiene trampas que permiten realizar a continuación reentradas no autorizadas al sistema.

Prohibición de acceso. Un usuario escribe un programa para hacer caer al sistema, poner al sistema en un ciclo infinito, o monopolizar recursos del sistema. Lo que se intenta aquí es el negar el acceso o servicio a los usuarios legítimos.

Procesos sincronizados interactivos. Los procesos usan las primitivas de sincronización del sistema para compartir y pasarse información entre sí.

Desconexión de línea. El intruso intenta obtener acceso al trabajo de un usuario después de una desconexión de línea, pero antes de que el sistema reconozca la desconexión.

Disfraz. El intruso asume la identidad de un usuario legítimo, después de haber obtenido la identificación apropiada por medios clandestinos.

Engaño al operador. Un intruso inteligente puede, a menudo, engañar al operador del computador y hacer que realice una acción que comprometa la seguridad del sistema.

Parásito. El intruso utiliza un terminal especial para conectarse a una línea de comunicación. El intruso intercepta los mensajes entre el usuario y el procesador, modifica el mensaje o lo reemplaza por completo. Proporcionando información distorsionada a los usuarios finales.

Caballo de Troya. El intruso coloca un código dentro del sistema que le permita accesos posteriores no autorizados. El caballo de Troya puede dejarse permanentemente en el sistema o puede borrar todo rastro de sí mismo, después de la penetración.

Parámetros inesperados. El intruso suministra valores inesperados a una llamada al supervisor, para aprovechar una debilidad de los mecanismos de verificación de la legalidad del sistema.

A medida que la computación se hace más asequible, los problemas de seguridad aumentan. Las comunicaciones de datos y las redes suponen un gran aumento de la

vulnerabilidad de los sistemas basados en computadores. El hecho de ser favorables al usuario, implica también un incremento de la vulnerabilidad.

Los requisitos de seguridad de un sistema dado, definen lo que para ese sistema significa la seguridad.

- La seguridad externa se ocupa de la protección del sistema de computación contra intrusos y desastres.
- La seguridad de la interface del usuario se encarga de establecer la identidad del usuario antes de permitir el acceso al sistema.
- La seguridad interna se encarga de asegurar una operación confiable y sin problemas del sistema de computación, y de garantizar la integridad de los programas y datos.

La autorización determina qué acceso se permite a qué empresas. La división de responsabilidades da a la gente distintos conjuntos de responsabilidades. Ningún empleado trata con una gran parte de la operación del sistema, de modo que para comprometer la seguridad tienen que estar implicados varios empleados.

La vigilancia trata de la supervisión y auditoría del sistema, y de la autentificación de los usuarios. En la verificación de las amenazas, el sistema operativo controla las operaciones delicadas, en vez de facilitarles el control directo a los usuarios.

Cuando los programas de vigilancia han de tener un acceso mayor que los programas del usuario, para servir las peticiones del usuario, esto se denomina amplificación.

f. Seguridad en redes

1) Las funciones de seguridad de red

En el intento de proteger una red de computadoras, existen varias funciones comunes a las cuales deben dirigirse. La siguiente es una lista de cuatro problemas básicos:

- El anfitrión promiscuo, la red debuggers.
- La autenticación de cliente y servidor.
- La autorización de cliente y servidor
- Contabilidad de cliente y servidor.

a) El anfitrión promiscuo

El anfitrión promiscuo es uno de los principales problemas de seguridad y uno de los problemas más urgentes de cualquier red. Si un intruso es paciente, él puede simplemente mirar que los paquetes fluyen de aquí para allá a través de la red. No toma mucha programación el análisis de la información que fluye sobre la red. Un ejemplo simple es un procedimiento de login remoto. En el procedimiento login, el sistema pedirá y recibirá el nombre y contraseña del usuario a través de la red. Durante la transmisión, ésta información no es codificada o encriptada de cualquier

forma. Una persona paciente simplemente puede esperar, y así recolectar toda la información que necesita para romper cualquier cuenta.

b) Autenticación

El procedimiento de login remoto ilustra el problema de autenticación.

¿Cómo presenta usted credenciales al anfitrión remoto para probar que usted es usted?.

¿Cómo hace usted esto, de forma que no se repita por el mecanismo simple de una jornada registrada?

c) Autorización

Aún cuando usted puede probar que usted es quien dice que es, simplemente, ¿Qué información debería permitir el sistema local acceder desde a través de una red?

Este problema de autorización parecería ser simple en concepto, pero considerar los problemas de control de acceso, cuando todo el sistema tiene su identidad remota de usuario, el problema de autorización sería un problema de seguridad bastante serio, en donde intervienen los conceptos de funciones autorizadas, niveles de autorización, etc.

d) Contabilidad

Finalmente, considerar el problema de contabilidad. Hay que recordar que nosotros debemos asumir que hay otros con un conocimiento mayor de sistemas. ¿Cuánta contabilidad tiene que hacer el sistema para crear una pista de revisión y luego examinar?

2) Componentes de seguridad

Para un intruso que busque acceder a los datos de la red, la línea de ataque más prometedora será una estación de trabajo de la red. Estas se deben proteger con cuidado. Debe habilitarse un sistema que impida que usuarios no autorizados puedan conectarse a la red y copiar información fuera de ella, e incluso imprimirla. Por supuesto, una red deja de ser eficiente si se convierte en una fortaleza inaccesible. El administrador de la red tal vez tenga que clasificar a los usuarios de la red con el objeto de adjudicarles el nivel de seguridad adecuado. A continuación se sugiere un sistema en tres niveles:

Nivel de administración. Aquellos que diseñan, mantienen o ponen en marcha la red. Este debe estar constituido sólo por el administrador o por un pequeño grupo de personal de soporte y administración.

Usuarios fiables. Aquellos usuarios que cumplen las normas y cuyo trabajo se pueda beneficiar de una mayor libertad de acceso a la red.

Usuarios vulnerables. Aquellos que muestran falta de competencia, son excesivamente curiosos o beligerantes, o los que por alguna razón no se puede confiar.

Estos niveles pueden tener un reflejo en el número de barreras que se establecen para el acceso al sistema y el tipo de derechos de acceso que se conceden, para cuando se ha obtenido la conexión, así como el nivel de supervisión y la frecuencia de las comprobaciones.

3) Control de acceso a la red

- Restringir el acceso a las áreas en que están las estaciones de trabajo mediante llaves, tarjetas de identificación, tarjetas inteligentes y sistemas biométricos.
- Restringir la posibilidad de conectar estaciones mediante llaves, tarjetas de identificación, tarjetas inteligentes y sistemas biométricos.
- Identificación para la red con clave de acceso.
- Protección con clave de todas las áreas sensitivas de datos y restricción de acceso a los programas, según su uso.
- Registro de toda la actividad de la estación de trabajo.
- Protección con clave de acceso o bloqueo de todas las operaciones de copia a disquete en las estaciones de trabajo.
- Monitorización de todas las operaciones de copia en disquete en las estaciones de trabajo.

4) Protección del servidor

La parte más importante de la red es el servidor. La concentración de los datos en el servidor, en términos de cantidad e importancia, hace que sea necesario protegerlo de todas las eventualidades. La dependencia en que esté el servidor no debe ser accesible para nadie, excepto para el administrador de la red. No se debe permitir que personas que no han de utilizar el servidor estén cerca de él.

Dada la importancia del servidor y la cantidad de datos que pasan por él, es necesario efectuar copias de seguridad, del servidor. Cabe recordar que las copias de seguridad del servidor de archivos son un elemento especialmente valioso, debiéndose quedar guardados en un lugar cerrado, seguro y con las condiciones ambientales necesarias. Un conjunto de copias de seguridad se debe trasladar regularmente a otro lugar seguro (de preferencia otro local).

5) Redes y tolerancia a fallas.

La tolerancia a fallas es la capacidad de la red de continuar funcionando, en el caso que se produzca un problema importante o una caída catastrófica, sin daño para los datos y sin que el funcionamiento cambie perceptiblemente.

La tolerancia a fallas, se refiere no sólo a la redundancia, sino a la detección de errores. Por lo general, la tolerancia a fallas conduce a un elemento hardware redundante, que entra en funcionamiento de forma automática en el caso que el

componente primario falle. Sin embargo la tolerancia a fallas puede ser algo como duplicar la FAT (tabla de localización de archivos) y las entradas de directorio en áreas distintas de un mismo disco, o una simple verificación de lectura tras escritura, con lo que se asegura que los datos nunca se escriben en un sector dañado del disco. No todas las redes requieren el mismo grado de tolerancia a fallas.

6) Protegiendo la red

Estaciones de trabajo sin acceso a obtener respaldos. Una posible solución para poder impedir la copia de programas y datos fuera de la red en memorias portátiles, y que a través de los mismos ingresan virus y otros programas dañinos a la red, es dotar a los usuarios vulnerables con estaciones de trabajo sin acceso a conectar dichos dispositivos.

3.2.4. Estrategias

Las estrategias de contingencia / continuidad de los negocios están diseñadas para identificar prioridades y determinar en forma razonable las soluciones a ser seleccionadas en primera instancia o los riesgos a ser gestionados en primer lugar.

Hay que decidir si se adoptarán las soluciones a gran escala, como las opciones de recuperación de desastres para un centro de datos o el mantenimiento de archivos de respaldo que permitan proteger información útil.

a. Actividades importantes

- La revisión de procesos, flujos, funciones y opciones de importancia crítica.
- La definición de las opciones de contingencia seleccionadas para cada riesgo identificado.
- La revisión / depuración del cronograma maestro, incluyendo prioridades, fechas importantes en el calendario de eventos y dependencias cruzadas en diversos proyectos o áreas.
- La consolidación de soluciones de acuerdo a las funciones o áreas de negocios más importantes e identificar las estrategias globales.
- La identificación de los impactos de las soluciones y estrategias para ahorrar costos, como puede ser la selección de una solución para cubrir varios riesgos, se deben de considerar varios elementos de costo: como el costo de crear la solución, el costo de implementar la solución, y el costo de mantener vigente dicha solución. Debido a que la continuidad de las operaciones de la organización constituye el enfoque primordial, la estrategia de la empresa rige el análisis de costos.
- La obtención de aprobaciones finales para el financiamiento, antes de que se apruebe la solución.
- La identificación de los beneficios es un elemento clave para asegurar que el costo del proyecto este equilibrado con los retornos reales de la organización.

b. Preparativos para la identificación de soluciones preventivas.

Los puntos que deben ser cubiertos por todas las áreas informáticas y usuarios en general son:

- Respaldar toda la información importante en medio magnético, acordamos que lo que debe respaldarse es INFORMACION y no las aplicaciones.
- Generar discos de arranque para las máquinas dependiendo de su sistema operativo, libres de virus y protegidos contra escritura.
- Mantener una copia de antivirus más reciente en disco para emergencias (dependiendo del fabricante, variarán las instrucciones para generarlo).
- Guardar una copia impresa de la documentación de los sistemas e interfaces, al igual de los planes de contingencia definidos por el resto de las áreas.
- Instalar todos los service packs que el equipo necesite y llevar un registro de los mismos, en caso de formatear el equipo o desinstalar aplicaciones.

c. Medida de precaución y recomendación

- Es recomendable que el centro de cómputo no esté ubicado en las áreas de alto tráfico de personas o con un alto número de invitados.
- Hasta hace algunos años la exposición de los equipos de cómputo a través de grandes ventanales, constituían el orgullo de la organización, considerándose necesario que estuviesen a la vista del público, siendo constantemente

visitados. Esto ha cambiado de modo radical, principalmente por el riesgo de terrorismo y sabotaje.

- Se deben evitar, en lo posible, los grandes ventanales, los cuales además de que permiten la entrada del sol y calor, puede ser un riesgo para la seguridad.
- Otra precaución que se debe tener en la construcción del centro de cómputo, es que no existan materiales que sean altamente inflamables, que despiden humos sumamente tóxicos o bien paredes que no quedan perfectamente selladas y despidan polvo.
- El acceso al centro de cómputo debe estar restringido al personal autorizado. El personal de la institución deberá tener su carné de identificación siempre en un lugar visible.
- Se debe establecer un medio de control de entrada y salida de visitas al centro de cómputo. Si fuera posible, acondicionar un ambiente o área de visitas.
- Se recomienda que al momento de reclutar al personal se les debe hacer además exámenes psicológicos y médico y tener muy en cuenta sus antecedentes de trabajo, ya que un centro de cómputo depende en gran medida, de la integridad, estabilidad y lealtad del personal.
- El acceso a los sistemas compartidos por múltiples usuarios y a los archivos de información contenidos en dichos sistemas, debe estar controlado mediante la verificación de la identidad de los usuarios autorizados.
- Deben establecerse controles para una efectiva disuasión y detección, a tiempo, de los intentos no autorizados de acceder a los sistemas y a los archivos de información que contienen.

- Se recomienda establecer políticas para la creación de contraseñas y establecer periodicidad de cambios de los mismos.
- Establecer políticas de autorizaciones de acceso físico al ambiente y de revisiones periódicas de dichas autorizaciones.
- Establecer políticas de control de entrada y salida del personal, así como de los paquetes u objetos que portan.
- La seguridad de las terminales de un sistema en red podrán ser controlados por medios de anulación del disk drive, cubriéndose de esa manera la seguridad contra robos de la información y el acceso de virus informáticos.
- Los controles de acceso, el acceso en sí y los vigilantes deben estar ubicados de tal manera que no sea fácil el ingreso de una persona extraña. En caso que ingresara algún extraño al centro de cómputo, que no pase desapercibido y que no le sea fácil a dicha persona llevarse un archivo.
- Las cámaras fotográficas y filmadoras no se permitirán en ninguna sala de cómputo, sin permiso por escrito de la dirección, se debe adoptar medidas contra todo tipo de espionaje.
- Asignar a una sola persona la responsabilidad de la protección de los equipos en cada área.
- El modelo de seguridad a implementar, estará basado en el entorno y en la política y estrategias de la instalación.

Estas constituyen algunas de las medidas de precaución y recomendación que deben ser tomadas en consideración por el sector carrocero.

d. Niveles de control:

Existen dos tipos de activos en un centro de cómputo. Los equipos físicos y la información contenida en dichos equipos. Estos activos son susceptibles de sustracción o destrucción del equipo, revelación o alteración no autorizada de la información considerada como clasificada, o interrupción del soporte a los procesos operativos del negocio, congestión de la red con información no deseada, destrucción de los medios de mantenimiento de información de soporte.

El valor de los activos a proteger, está determinado por el nivel de clasificación de la información y por el impacto en el negocio, causado por pérdida o destrucción del equipo o información. Hay que distinguir los activos en nivel clasificado y no clasificado. Para los de nivel no clasificado, no será necesario control. Cualquier control debe basarse únicamente en el valor del equipo y servicios que ellos prestan.

En cambio tratándose de nivel clasificado, deben observarse además todas las medidas de seguridad de la información que estos equipos contengan.

e. Medios de almacenamiento.

Los medios magnéticos que contienen respaldos deben guardarse bajo ciertas condiciones, con la finalidad de garantizar una adecuada conservación de la información almacenada.

Aunque los discos duros vienen de fábrica sellados herméticamente, debe evitarse que los circuitos electrónicos que se encuentran alrededor se llenen de partículas de polvo y suciedad que pudieran ser causa de errores. El computador debe colocarse en un lugar donde no pueda ser golpeado, de preferencia sobre un escritorio resistente y amplio. Se debe evitar que se coloque en zonas donde haya acumulación de calor. Esta es una de las causas más frecuentes de las fallas de los discos duros, sobre todo cuando algunas piezas se dilatan más que otras.

No se debe mover la CPU conteniendo al disco duro cuando esté encendido, porque los cabezales de lectura-escritura pueden dañar al disco. Una de las medidas más importantes en este aspecto, es hacer que la gente tome conciencia de lo importante que es cuidar un microcomputador.

La forma más fácil y común de reducir la fatiga en la visión que resulta de mirar a una pantalla todo el día, es el uso de medidas contra la refección.

Generalmente éstos vienen en forma de una pantalla con un terminado áspero o algún tipo de capa contra brillo con una base de sílice, sobre la superficie de la pantalla del monitor.

Se recomienda sentarse por lo menos a 60 cm. de la pantalla. No sólo esto reducirá su exposición a las emisiones (que se disipan a una razón proporcional al cuadrado de la distancia), sino que puede ayudar a reducir el esfuerzo visual.

También manténgase por lo menos a 1 m. o 1.20 m. (3 o 4 pies) del monitor de su vecino, ya que la mayoría de los monitores producen más emisiones por detrás, que por delante. Finalmente apague su monitor cuando no lo esté usando.

Mantener fuera del teclado grapas y clips pues, de insertarse entre las teclas, puede causar un cruce de función.

Poner debajo del mouse una superficie plana y limpia, de tal manera que no se ensucien los rodillos y mantener el buen funcionamiento de éste.

El manejo de las impresoras, en su mayoría, es a través de los botones, tanto para avanzar como para retroceder el papel.

Caso de mala impresión, luego de imprimir documentos o cuadros generados, apagar por unos segundos la impresora para que se pierda el set dejado.

3.2.5. Documentación del proceso

Todo el proceso de lograr identificar soluciones ante determinados problemas no tendrá su efecto verdadero si es que no se realiza una difusión adecuada de todos los puntos importantes que este implica, y un plan de Contingencia con mayor razón necesita de la elaboración de una documentación que sea eficientemente orientada. Como puntos importantes que debe de incluir esta documentación podremos citar las siguientes:

- Cuadro de descripción de los equipos y las tareas para ubicar las soluciones a las contingencias.
- La documentación de los riesgos, opciones y alternativas de solución por escrito, en detalle y su orden de aplicación.
- La identificación y documentación de listas de contacto de emergencia, la identificación de responsables de las funciones con el fin de garantizar que siempre haya alguien a cargo, y que pueda ser contactada si falla un proceso de importancia.

3.2.6. Realización de pruebas y validación

a. Plan de recuperación de desastres

Es importante definir los procedimientos y planes de acción para el caso de una posible falla, siniestro o desastre en el área Informática, considerando como tal todas las áreas de los usuarios que procesan información por medio de la computadora.

Cuando ocurra una contingencia, es esencial que se conozca al detalle el motivo que la originó y el daño producido, lo que permitirá recuperar en el menor tiempo posible el proceso perdido.

La elaboración de los procedimientos que se determinen como adecuados para un caso de emergencia, deben ser planeados y probados fehacientemente.

Los procedimientos deberán ser de ejecución obligatoria y bajo la responsabilidad de los encargados de la realización de los mismos, debiendo haber procesos de verificación de su cumplimiento. En estos procedimientos estará involucrado todo el personal de la empresa.

Los procedimientos de planes de recuperación de desastres deben de emanar de la máxima autoridad de la empresa, para garantizar su difusión y estricto cumplimiento.

Las actividades a realizar en un plan de recuperación de siniestros se pueden clasificar en tres etapas:

1) Actividades previas al siniestro.
2) Actividades durante el siniestro.
3) Actividades después del siniestro.

1) Actividades previas al siniestro.

Son todas las actividades de planeamiento, preparación, entrenamiento y ejecución de las actividades de resguardo de la información, que nos aseguren un proceso de recuperación con el menor costo posible para las empresas asociadas al proyecto específico. Podemos detallar las siguientes actividades generales:

- Establecimiento del plan de acción.
- Formación de equipos operativos.

- Formación de equipos de evaluación.
- Establecimiento de plan de acción

En esta fase de planeamiento se debe de establecer los procedimientos relativos a:

a) Sistemas de información.

b) Equipos de cómputo.

c) Obtención y almacenamiento de los respaldos de información.

d) Políticas.

a) Sistemas de información. La organización deberá tener una relación de los Sistemas de Información con los que cuenta, tanto los realizados por el centro de cómputo como los hechos por las áreas usuarias. Debiendo identificar toda información sistematizada o no, que sea necesaria para la buena marcha la empresa.

La relación de sistemas de información deberá detallar los siguientes datos:

- Nombre del sistema.
- Lenguaje o paquete con el que fue creado el sistema. Programas que lo conforman.
- El departamento que genera la información base.
- Las unidades o departamentos que usan la información del sistema.
- El volumen de los archivos que trabaja el sistema.

- El volumen de transacciones diarias, semanales y mensuales que maneja el sistema.
- El equipamiento necesario para un manejo óptimo del sistema.
- La(s) fecha(s) en las que la información es necesitada con carácter de urgencia.
- El nivel de importancia estratégica que tiene la información de este sistema para la empresa.
- Equipamiento mínimo necesario para que el sistema pueda seguir funcionando.
- Actividades a realizar para volver a contar con el sistema de información.
- Con toda esta información se deberá de realizar una lista priorizada de los sistemas de información necesarios para que la empresa pueda recuperar su operatividad perdida en el siniestro (contingencia).

b) Equipos de cómputo. Aparte de las normas de seguridad que se verán en los capítulos siguientes, hay que tener en cuenta:

- Inventario actualizado de los equipos de manejo de información, especificando su contenido, su ubicación y nivel de uso empresarial.
- Pólizas de seguros comerciales. Como parte de la protección de los activos empresariales pero haciendo la salvedad en el contrato, que en caso de siniestros, la restitución del computador siniestrado se podrá hacer por otro de mayor potencia, siempre y cuando esté dentro de los montos asegurados.

- Señalización o etiquetado de los computadores de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación. Por ejemplo etiquetar de color rojo a los servidores, color amarillo a las PC's con información estratégica y color verde a las PC's de contenidos normales.
- Tener siempre actualizada una relación de PC's requeridas como mínimo para cada sistema permanente de la empresa, las funciones que realizaría y su posible uso en dos o tres turnos de trabajo, para cubrir las funciones básicas y prioritarias de cada uno de estos sistemas.

c) Obtención y almacenamiento de los respaldos de información. Se deberá establecer los procedimientos para la obtención de copias de seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución de los sistemas o aplicativos de la empresa. Para lo cual se debe contar con:

- Backups del sistema operativo.
- Backups del software base.
- Backups del software aplicativo.
- Backups de los datos.
- Backups del hardware. Se puede implementar bajo dos modalidades:

Modalidad externa. Mediante convenio con otra empresa que tenga equipos similares o mayores y que brinden la seguridad de poder procesar la información, y ser puestos a nuestra disposición, al ocurrir una contingencia y mientras se busca una solución definitiva al siniestro producido. Este tipo de convenios debe tener tanto las

consideraciones de equipamiento como de ambientes y facilidades de trabajo que cada organización se compromete a brindar.

Modalidad interna. Si tenemos más de un local, en ambos debemos tener señalados los equipos, que por sus características técnicas y capacidades, son susceptibles de ser usados como equipos de emergencia del otro local, debiéndose poner por escrito, todas las actividades a realizar y los compromisos asumidos.

En ambos casos se deberá probar y asegurar que los procesos de restauración de información posibiliten el funcionamiento adecuado de los sistemas. En algunos casos puede ser necesario volver a recompilar nuestro software aplicativo bajo plataformas diferentes a la original, por lo que es imprescindible contar con los programas fuentes, al mismo grado de actualización que los programas objeto.

d) Políticas (Normas y procedimientos de backups)

Se debe establecer los procedimientos, normas, y determinación de responsabilidades en la obtención de los backups mencionados anteriormente en el punto c), debiéndose incluir:

- Periodicidad de cada tipo de backup.
- Uso obligatorio de un formulario estándar para el registro y control.
- Correspondencia entre la relación de sistemas e informaciones necesarias para la buena marcha de la empresa, y los backups efectuados.

- Almacenamiento de los backups en condiciones ambientales óptimas, dependiendo del medio magnético empleado.
- Reemplazo de los backups, en forma periódica, antes que el medio magnético de soporte se pueda deteriorar.
- Almacenamiento de los backups en locales diferentes donde reside la información primaria.
- Pruebas periódicas de los backups, verificando su funcionalidad, a través de los sistemas, comparando contra resultados anteriores confiables.

En cada unidad operativa de la empresa, que almacene información y sirva para la operatividad, se deberá designar un responsable de la seguridad por cada unidad.

Sus labores serán:

- Ponerse en contacto con los dueños de las aplicaciones y trabajar con ellos.
- Proporcionar soporte técnico para las copias de respaldo de las aplicaciones.
- Planificar y establecer los requerimientos de los sistemas operativos en cuanto a archivos, bibliotecas, utilitarios, etc.
- Supervisar procedimientos de respaldo y restauración.
- Supervisar la carga de archivos de datos de las aplicaciones, y la creación de los respaldos incrementales.
- Coordinar líneas, terminales, módem, otros aditamentos para comunicaciones.
- Establecer procedimientos de seguridad en los sitios de recuperación.
- Organizar la prueba de hardware y software.

- Ejecutar trabajos de recuperación.
- Cargar y probar archivos del sistema operativo y otros sistemas almacenados en el local alternante.
- Realizar procedimientos de control de inventario y seguridad del almacenamiento en el local alternante.
- Establecer y llevar a cabo procedimientos para restaurar el lugar de recuperación.
- Participar en las pruebas y simulacros de siniestros.

Esta función debe ser realizada de preferencia por personal de auditoría, de no ser posible, la realizará el personal del área de informática, debiendo establecerse claramente sus funciones, responsabilidades y objetivos:

- Revisar que las normas y procedimientos con respecto a backups y seguridad de equipos y data se cumpla.
- Supervisar la realización periódica de los backups, por parte de los equipos operativos, comprobando físicamente su realización y adecuado registro
- Revisar la correlación entre sistemas e informaciones necesarios para la buena marcha de la organización, y los backups realizados.
- Informar de los cumplimientos e incumplimientos de las normas, para las acciones de corrección respectivas, o en su caso las actualizaciones a las reglas como consecuencia de la gestión del cambio.

2) Actividades durante el siniestro.

Una vez presentada la contingencia o siniestro, se deberá ejecutar las siguientes actividades, planificadas previamente:

a) Plan de emergencias.

b) Formación de equipos.

c) Entrenamiento.

a) Plan de emergencias

En este plan se establecen las acciones se deben realizar cuando se presente un Siniestro, así como la difusión de las mismas. Es conveniente prever los posibles escenarios de ocurrencia del siniestro:

- Durante el día.
- Durante la noche o madrugada.

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

- Vías de salida o escape.
- Plan de evacuación del personal.
- Plan de puesta a buen recaudo de los activos de la empresa.

- Ubicación y señalización de los elementos contra el siniestro.
- Secuencia de llamadas en caso de siniestro.

b) Formación de equipos

Establecer claramente cada equipo con funciones claramente definidas a ejecutar durante el siniestro. Si bien la premisa básica es la protección de la Integridad del personal, en caso de que el siniestro lo permita, deberá de existir dos equipos de personas que actúen directamente durante el siniestro, un equipo para combatir el siniestro y otro para el salvamento de los recursos Informáticos, de acuerdo a los lineamientos o clasificación de prioridades.

c) Entrenamiento

Establecer un programa de prácticas periódicas de todo el personal en la lucha contra los diferentes tipos de siniestros, de acuerdo a los roles que se le hayan asignado en los planes de evacuación del personal o equipos y protección de la información estratégica, para minimizar costos se puede aprovechar fechas de recarga de extinguidores, charlas de los proveedores, etc. Un aspecto importante es que el personal tome conciencia de que los siniestros pueden realmente ocurrir, y tomen con seriedad y responsabilidad estos entrenamientos, para estos efectos es conveniente que participen los elementos directivos, dando el ejemplo de la importancia que la alta dirección otorga a la seguridad empresarial.

3) Actividad después del siniestro.

Después de ocurrido el siniestro es necesario realizar las actividades que se detallan, las cuales deben estar especificadas en el plan de acción.

a) Evaluación de daños.

b) Priorización de actividades del plan de acción.

c) Ejecución de actividades.

d) Evaluación de resultados.

e) Retroalimentación del plan de acción.

a) Evaluación de daños.

Inmediatamente después que el siniestro ha concluido, se deberá evaluar la magnitud del daño que se ha producido, que sistemas se están afectando, que equipos han quedado no operativos, cuales se pueden recuperar, y en cuanto tiempo, etc. Adicionalmente se deberá lanzar un pre-aviso a la empresa, con la cual tenemos el convenio de respaldo, para ir avanzando en las labores de preparación de entrega de los equipos por dicha empresa.

b) Priorización de actividades del plan de acción

Toda vez que el plan de acción es general y contempla una pérdida total, la evaluación de daños reales y su comparación contra el plan, nos dará la lista de las

actividades que debemos realizar, siempre priorizándola en vista a las actividades estratégicas y urgentes de nuestra empresa.

Es importante evaluar la dedicación del personal a actividades que puedan no haberse afectado, para ver su asignación temporal a las actividades afectadas, en apoyo al personal de los sistemas afectados y soporte técnico.

c) Ejecución de actividades

La ejecución de actividades implica la creación de equipos de trabajo para realizar las actividades previamente planificadas en el plan de acción. Cada uno de estos equipos deberá contar con un coordinador que deberá reportar diariamente el avance de los trabajos de recuperación y, en caso de producirse algún problema, reportarlo de inmediato a la jefatura a cargo del plan de contingencias. Con la finalidad de que al reportar a la alta dirección, se asignen los recursos necesarios que minimicen el imácto del siniestro.

Los trabajos de recuperación tendrán dos etapas, la primera la restauración del servicio usando los recursos de la empresa o local de respaldo, y la segunda etapa es volver a contar con los recursos en las cantidades y lugares propios del sistema de información, debiendo ser ésta última etapa lo suficientemente rápida y eficiente para no perjudicar el buen servicio de nuestro sistema e imagen empresarial, como para no perjudicar la operatividad de la empresa o local de respaldo.

d) Evaluación de resultados

Una vez concluidas las labores de recuperación del (los) sistema(s) que fueron afectados por el siniestro, debemos de evaluar objetivamente, todas las actividades realizadas, que tan bien se hicieron, que tiempo tomaron, que circunstancias modificaron las actividades del plan de acción, como se comportaron los equipos de trabajo, etc. De la evaluación de resultados y del siniestro en si, deberían de salir dos tipos de recomendaciones, una la retroalimentación del plan de contingencias y otra una lista de recomendaciones para minimizar los riesgos y pérdida que ocasionaron el siniestro.

e) Retroalimentación del plan de acción

Con la evaluación de resultados, debemos de optimizar el plan de acción original, mejorando las actividades que tuvieron algún tipo de dificultad y reforzando los elementos que funcionaron adecuadamente. El otro elemento es evaluar cual hubiera sido el costo de no haber tenido la empresa el plan de contingencias llevado a cabo.

3.2.7. Implementación

La fase de implementación se da cuando han ocurrido o están por ocurrir los problemas para este caso se tiene que tener preparado los planes de contingencia para poder aplicarlos. Puede también tratarse esta etapa como una prueba controlada.

a) De las emergencia físicas

CASO A: Error físico de disco duro de un servidor.

Dado el caso crítico de que el disco presenta fallas, tales que no pueden ser reparadas, se deben tomar las acciones siguientes:

1. Ubicar el disco malogrado.
2. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.
3. Deshabilitar la entrada al sistema.
4. Bajar el sistema y apagar el equipo.
5. Retirar el disco malo y reponerlo con otro del mismo tipo.
6. Restaurar el último backup en el disco, seguidamente restaurar las modificaciones efectuadas desde esa fecha a la actualidad.
7. Verificar la integridad de los sistemas contenidos en el disco.
8. Habilitar las entradas al sistema para los usuarios.

CASO B: Error de memoria RAM

En este caso se dan los siguientes síntomas:

- El servidor no responde correctamente, por lentitud de proceso o por no rendir ante el ingreso masivo de usuarios.

- Ante procesos mayores se congela el proceso.
- Arroja errores con mapas de direcciones hexadecimales.
- Es recomendable que el servidor cuente con ECC (error correct checking), por lo tanto si hubiese un error de paridad, el servidor se autocorregirá.

Todo cambio interno a realizarse en el servidor será fuera de horario de trabajo fijado por la compañía, a menos que la dificultad apremie, cambiarlo inmediatamente. Se debe tomar en cuenta que ningún proceso debe quedar cortado, y se deben tomar las acciones siguientes:

1. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.
2. El servidor debe estar apagado, dando un correcto apagado del sistema.
3. Ubicar las memorias malogradas.
4. Retirar las memorias malogradas y reemplazarlas por otras iguales o similares.
5. Retirar la conexión del servidor con el concentrador, ésta se ubica detrás del servidor, ello evitará que al encender el sistema, los usuarios ingresen.
6. Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas.
7. Probar los sistemas que están en red en diferentes estaciones.
8. Finalmente luego de los resultados, habilitar las entradas al sistema para los usuarios.

CASO C: Error de tarjeta(s) controladora(s) de disco

Se debe tomar en cuenta que ningún proceso debe quedar cortado, debiéndose ejecutar las siguientes acciones:

1. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.
2. El servidor debe estar apagado, dando un correcto apagado del sistema.
3. Ubicar la posición de la tarjeta controladora.
4. Retirar la tarjeta con sospecha de deterioro y tener a la mano otra igual o similar.
5. Retirar la conexión del servidor con el concentrador, ésta se ubica detrás del servidor, ello evitará que al encender el sistema, los usuarios ingresen.
6. Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas.
7. Al final de las pruebas, luego de los resultados de una buena lectura de información, habilitar las entradas al sistema para los usuarios.

CASO D: Caso de incendio total

En el momento que se dé aviso por los altavoces de alguna situación de emergencia general, se deberá seguir al pie de la letra los siguientes pasos, los mismos que están

encausados a salvaguardar la seguridad personal, el equipo y los archivos de información que tenemos en dispositivos magnéticos.

- Ante todo, se recomienda conservar la serenidad. Es obvio que en una situación de este tipo, impera el desorden, sin embargo, es muy recomendable tratar de conservar la calma, lo que repercutirá en un adecuado control de nuestras acciones.
- En ese momento cualquiera que sea(n) el (los) proceso(s) que se esté(n) ejecutando en el Computador Principal, se deberá enviar un mensaje (si el tiempo lo permite) de "Salir de Red y Apagar Computador", seguidamente digitar Down en el (los) servidor(es).
- Se apagará (poner en OFF) la caja principal de corriente del departamento de sistemas.
- Tomando en cuenta que se trata de un incendio de mediana o mayor magnitud, se debe tratar en lo posible de trasladar el servidor fuera del local, se abandonará el edificio en forma ordenada, lo más rápido posible, por las salidas destinadas para ello.

CASO E: Caso de inundación

- Para evitar problemas con inundaciones se ha de instalar tarimas de un promedio de 20 cm. de altura para la ubicación de los servidores. De esta manera evitaremos inconvenientes con el agua o residuos orgánicos propios de este tipo de siniestros.

- En lo posible, los tomacorrientes deben ser instalados a un nivel razonable de altura, para evitar que el agua penetre por los orificios y produzca daños en el sistema eléctrico.
- Dado el caso de que se obvió una conexión que está al ras del piso, ésta debe ser modificada su ubicación o en su defecto anular su conexión.
- Para prevenir los corto circuitos, asegurarse de que no existan fuentes de líquidos cerca a las conexiones eléctricas.
- Proveer cubiertas protectoras para cuando el equipo esté apagado.

CASO F: Caso de fallas de fluido eléctrico

Se puede presentar lo siguiente:

1. Si fuera corto circuito, el UPS mantendrá activo los servidores y algunas estaciones, mientras se repare la avería eléctrica o se enciende el generador.
2. Para el caso de apagón se mantendrá la autonomía de corriente que el UPS nos brinda corriente de emergencia, hasta que los usuarios completen sus operaciones, hasta que finalmente se realice el By-pass de corriente con el grupo electrógeno, previo aviso y coordinación.
3. Cuando el fluido eléctrico de la calle se ha restablecido se tomarán los mismos cuidados para el paso de grupo electrógeno a corriente normal (o UPS).

b) De las emergencias lógicas de datos

CASO A: Error lógico de datos

La ocurrencia de errores en los sectores del disco duro del servidor puede deberse a una de las siguientes causas:

- Caída del servidor de archivos por falla de software de red.
- Falla en el suministro de energía eléctrica por mal funcionamiento del UPS.
- Bajar incorrectamente el servidor de archivos.
- Fallas causadas usualmente por un error de chequeo de inconsistencia física.

En caso de producirse alguna de las situaciones descritas anteriormente; se deben realizar las siguientes acciones:

PASO 1: Verificar el suministro de energía eléctrica. En caso de estar conforme, proceder con el encendido del servidor de archivos, una vez mostrado el prompt de Dos, cargar el sistema operativo de red.

PASO 2: Deshabilitar el ingreso de usuarios al sistema.

PASO 3: Descargar todos los volúmenes del servidor, a excepción del volumen raíz. De encontrarse este volumen con problemas, se deberá descargarlo también.

PASO 4: Cargar un utilitario que nos permita verificar en forma global el contenido del(os) disco(s) duro(s) del servidor.

PASO 5: Al término de la operación de reparación se procederá a habilitar entradas a estaciones para manejo de soporte técnico, se procederá a revisar que las bases de datos índices estén correctas, para ello se debe empezar a correr los sistemas y así poder determinar si el usuario puede hacer uso de ellos inmediatamente.

Si se presenta el caso de una o varias bases de datos no reconocidas como tal, se debe recuperar con utilitarios.

CASO B: Caso de virus

Dado el caso crítico de que se presente virus en las computadoras se procederá a lo siguiente:

Para servidor:

- Se contará con antivirus para el sistema que aíslan el virus, llevándolo a un directorio para su futura investigación
- El antivirus muestra el nombre del archivo infectado y quién lo usó.
- Estos archivos serán reemplazados del disco original de instalación.
- Si los archivos infectados son aislados y aún persiste el mensaje de que existe virus en el sistema, lo más probable es que una de las estaciones es la que causó la infección, debiendo retirarla del ingreso al sistema y proceder a su revisión.

Para computadoras fuera de red:

Se revisará las computadoras que no estén en red con antivirus.

De suceder que una computadora se haya infectado con uno o varios virus ya sea en la memoria o a nivel disco duro, se debe proceder a realizar los siguientes pasos:

Utilizar un disco que contenga sistema operativo igual o mayor en versión al instalado en el computador infectado. Reiniciar el computador con dicho disco.
Retirar el disquete con el que arrancó el computador e insertar el disco, antivirus, luego activar el programa de tal forma que revise todos los archivos y no sólo los ejecutables.

De encontrar virus, dar la opción de eliminar el virus. Si es que no puede hacerlo el antivirus, recomendará borrar el archivo, tomar nota de los archivos que se borren. Si éstos son varios pertenecientes al mismo programa, reinstalar al término del escaneado. Finalizado el escaneado, reconstruir el master boot del disco duro.

3.2.8. Monitoreo

La fase de monitoreo nos dará la seguridad de que podamos reaccionar en el tiempo preciso y con la acción correcta. Esta fase es primordialmente de mantenimiento. Cada vez que se da un cambio en la infraestructura, debemos de realizar un mantenimiento correctivo o de adaptación.

Un punto donde se tiene que actuar es por ejemplo cuando se ha identificado un nuevo riesgo o una nueva solución. En este caso, toda la evaluación del riesgo se cambia, y comienza un nuevo ciclo completo, a pesar de que este esfuerzo podría ser menos exigente que el primero, Esto es importante ya que nos alimentamos de las nuevas posibilidades de soluciones ante nuevos casos que se puedan presentar. Estas acciones se deben efectuar sin alterar la normal operación del sistema.

Podríamos enumerar las actividades principales a realizar:

- Desarrollo de un mapa de funciones y factores de riesgo.
- Establecer los procedimientos de mantenimiento para la documentación y la rendición de informes referentes a los riesgos.
- Revisión continua de las aplicaciones.
- Revisión continua del sistema de backup
- Revisión de los sistemas de soporte eléctrico.

3.2.9. Pasos para desarrollar el plan de contingencia de los sistemas de información.

Etapa I: Análisis y selección de las operaciones críticas.

En esta etapa hay que definir cuáles serán nuestras operaciones críticas y tienen que ser definidas en función a los componentes de los sistemas de información los cuales son: datos, aplicaciones, tecnología hardware y software, instalaciones y personal.

Dentro de las cuales podemos identificar las siguientes, las mismas pueden variar de sistema a sistema:

- Reportes impresos de informes del sistema.
- Consultas a las bases de datos vía internet.
- Consultas a las bases de datos vía LAN.
- Sistema de backup y recuperación de datos.
- Sistema de ingreso y modificación en la base de datos de documentos que llegan y salen al exterior.
- Los Servidores de bases de datos y aplicaciones.
- Los servicios de red.
- Los medios de transmisión.
- Las Topologías de red.
- Los métodos de control de acceso.
- Se ha listado los procesos críticos de manera genérica y evaluado su grado de importancia en función a la magnitud del impacto si los procesos pueden detenerse, y luego clasificados en niveles **H** (Alta), **R** (Regular) y **L** (Bajo).

Se tiene que elaborar una tabla denominada operaciones críticas de los sistemas de información, que consta de tres campos:

Operaciones críticas

Objetivo de la operación

Prioridad de la operación.

Cuadro 3.2 Operaciones críticas del sistema de información

Operaciones Críticas	Objetivos de la Operación	Prioridad de la Operación
Reportes Impresos de Informes del Sistema	Informes de los estados financieros de la organización. Informes de plantillas del personal. Informes de producción mensual, anual.	R
Consultas a las Bases de Datos vía Internet	Informes a los clientes. Información a los proveedores. Sistema de ventas vía internet.	L
Consultas a las Bases de Datos vía LAN	Inventarios, Revistas, electrónicas.	R
Sistema de Backup y Recuperación de Data	Procesos de Backups de la información. Establecimiento de las frecuencias de almacenamiento de datos.	H
Sistema de Ingreso y modificación en la Base de Datos de documentos que llegan y salen al exterior.	Proceso de los programas que realizan la entrada y salida de la información. Mantenimiento adecuado de las aplicaciones. Equipamiento necesario para un funcionamiento optimo del sistema.	H

Elaborado Por: GMSM

Fecha: 12/12/2008

Se ha tomado solo estas operaciones como modelo para detallar el desarrollo del plan, pero cabe recordar que debemos de tener muy en cuenta que hay más operaciones que son críticas y que debemos tener cuidado al identificarlas.

Cuadro 3.3: Procesos estratégicos del negocio

OPERACION PRINCIPAL	CONTENIDO DE LA OPERACION	PRIORIDAD D LA OPERACION
VENTAS (A)	Ventas a los clientes	R
ORDENES ACEPTADAS (B)	Aceptar órdenes de los clientes Administración de las ventas a crédito	H
ENVIO Y REPARTO (C)	Administración del inventario Envío de productos Reparto de las ventas a crédito	H
COMPRA (D)	Dando órdenes a los fabricantes Administración de la compra a crédito	H
PRODUCCIÓN (E)	Fabricación	H
ESTADÍSTICAS (F)	Estadísticas mensuales Estadísticas anuales	R
ELABORACION DE INFORMES DE LA ADMINISTRACIÓN (G)	Elaboración de reportes totales de Administración	L

H = Alta R = Regular L = Baja

Elaborado Por: GMSM

Fecha: 13/11/2008

- Para cada una de las operaciones principales, enumerar sus procesos.
- Investigar qué recursos de la empresa (equipamiento, herramientas, sistemas, etc.) son usados, descríbalos y enumérelos.

Cuadro 3.4: Análisis sobre un proceso del negocio

Se utiliza las nomenclaturas para identificar los procedimientos y a que proceso pertenece.

NOMBRE DE LA OPERACIÓN: Aceptación de órdenes.

# DE PROCEDIMIENTO	PROCESOS DE NEGOCIOS	RECURSOS USADOS	# DE SERIE DEL RECURSO	ORDENES ó NOTAS
B – 1	Recepción de órdenes de pedido	Teléfonos fijos	S1	Clientes E y F
		PC´s	S2	Clientes G
		Líneas dedicadas	S3	Clientes H
B – 2	Confirmar la cantidad total límite de órdenes recibidas	Sistema de aceptación de la orden (Software)	S4	
B – 3	Confirmar si se cuenta con el Stock para atender los pedidos	Sistema de aceptación de la orden	S4	
B – 4	Registrar las órdenes	Sistema de aceptación de la orden	S4	
	Enviar las confirmaciones de órdenes Automáticamente	Sistema de aceptación de la orden Faxes	S4 S2	De nosotros para los clientes
B -6	Indicar el envío o remitirlas a sus respectivos centros	Sistema de aceptación de la orden	S4	
		Líneas dedicadas	S3	De los Grupos de Trabajo a los centros de reparto

Elaborado Por: GMSM

Fecha: 14/11/2008

- Enumerar recursos utilizados para los procesos
- Describir ubicaciones de proveedores de servicios por los procesos de cada operación.
- Investigue y describa a los proveedores de servicios.

Cuadro 3.5: Lista de recursos utilizados

N° Serie del Recurso	Recurso	Ubicación	Proveedor del Servicio	Recursos de operaciones utilizados por
S1-1	Pc's	Externo	Proveedor A	B-1
S1-2		Interno	Soporte técnico	B-1
S2-1	Software de administración de compras	Externo	Proveedor A	B-1, B-5, K-1
S2-2		Interno	Soporte técnico	B-1, K-1
S3	Líneas dedicadas	Externo	Teléfono A (Red)	B-1, B-6, K-1
S4-1	Sistema de aceptación de orden (Software base)	Interno	Desarrollo interno (aplicación)	B-2, B-3, B-4, B-5, B-6, S-10, N-1, N-6, N-7, N-11
S4-2		Interno	Electrónica B (Hardware y otros)	B-2, B-3, B-4, B-5, B-6, S-1, S-6, S-10, N-1, N-2, N-3, N-7, N-11
S5	Almacén automatizado	Interno	Maquinaria Q	N-2, N-3
S6	Maquinaria de embolsado	Interno	Maquinaria de precisión R	N-4
S7	Elevadores del almacén	Interno	Industria pesada S	S-9, K-5
S8	Camiones internos	Interno	Motores T	S-7, N-9
S9	Servicio de reparto a domicilio	Externo	Transporte L	N-9
S10	Servidores	Interno	Electrónica B	B-1, B-2, B-3 B-4,N-1
S11	Software Clientes	Interno	Desarrollo Interno	B1- , N-9 , B-2 , B-3

Elaborado Por: GMSM

Fecha: 15/11/2008

- Estudio puntual de fallas
- Considerando el contenido de cada operación, determinar cuanto tiempo una interrupción puede ser tolerada.
- Describir con que frecuencia se utiliza un recurso y que tiempo una parada o interrupción bloquea la operación.

Cuadro 3.6: Lista del periodos aceptables de interrupción

N° Serie del Recurso	Recurso	Recursos de operaciones utilizados por	Frecuencia de uso	Periodo aceptable de Interrupción
S1-1	PC´s (Red)	B-1	Cada día	Medio día
S1-2	PC´s (Red)	B-1	Cada día	Medio día
S2-1	Software (Red)	B-1	Cada día	Medio día
		K-1	Cada día	Medio día
S2-2	Software de administración de Compras	B-1	Cada día	Medio día
		B-5	Cada día	Medio día
		K-1	Cada día	Medio día
S3	Líneas dedicadas	B-1	Cada día	Medio día
		B-6	Cada noche	Un día
		K-1	Cada 3 días	3 días
S4-1	Sistema de aceptación de orden	B-2	Cada día	Medio día
		B-3	Cada día	Medio día
		B-4	Cada día	Medio día
S10	Servidores	B-1	Cada día	3 horas
S11	Software Cliente	B1,B3, B5	Cada día	3 horas

Elaborado por: GMSM

Fecha: 18/11/2008

- Estudie y describe el estado de fabricación de productos que constituyen recursos
- Las soluciones varían según el período asumido de la parada.
- Calcular y describir el período que se pasará hasta la recuperación del elemento afectado, basado en la información confirmada.

Cuadro 3.7: Lista de problemas probables a ocurrir.

N° Serie Recurso	Recurso	Proveedor del Servicio	Resultados confirmados	Juicio de compañías	
			Condiciones de preparación de las medidas preventivas	Posibilidad del problema	Periodo necesario par recuperación
S10	Servidores	Electrónica (Red)	Preparación de las medidas preventivas	Pequeña	3 Horas
S11-1	Software Clientes	Desarrollo (Red)	Preparación de las medidas preventivas	Pequeña	3 horas
S11-2		Electrónica O (Fax)	Equipos listos para los problemas de los sistema de información	Pequeña	3 horas
S3	Líneas dedicadas	Teléfono A (Red)	Preparación de las medidas preventivas	Pequeña	Medio día
S4-1	Sistema de aceptación de orden (Software Base)	Desarrollo interno (aplicación)	Preparación de las medidas preventivas	Media	2 días
S4-2		Electrónica B (Hardware)	Preparación de las medidas preventivas	Pequeña	5 días
S5	Almacén automatizado	Industrial Q	Preparación de las medidas preventivas	Pequeña	2 días
S7	Elevadores del almacén	Industria pesada S	Las partes que pueden tener problemas son reemplazadas y las máquinas examinadas	Pequeña	3 días
S9	Servicio de reparto a domicilio	Transporte L	Preparación de las medidas preventivas	Grande	2 días
S2	Sistema de Administración de la Compra	Desarrollo interno (aplicación)	Preparación de las medidas preventivas	Media	7 días

Elaborado Por: GMSM
Fecha: 19/11/2008

Etapa 2. Identificación de procesos en cada operación

Para cada una de las operaciones críticas en la Etapa 1, se debe enumerar los procesos que tienen.

Los responsables de desarrollar los planes de contingencia deben de coordinar en cooperación con el personal a cargo de las operaciones de los sistemas analizados, los cuáles son conocedores de dichos procesos críticos.

Se debe de investigar qué recursos administrativos son usados en cada proceso, se ha descrito y codificado cada recurso, como:

- sistema eléctrico,
- tarjetas,
- transporte,
- red de datos, PC's.

A su vez también se ha determinado su nivel de riesgo, como críticos y no críticos. La tabla que es presentada a continuación contiene cinco campos:

- Código de los procesos
- Procesos
- Recursos utilizados
- Código del recurso
- Nivel de riesgo

Cuadro 3.8. Procesos del área analizada (e)

Código del Proceso	Procesos	Plan de Contingencia	Código del recurso	Nivel del Riesgo
E- 1	Proceso de los programas que realizan la entrada y salida de la información	Sistema Eléctrico	R1	Crítico
		Red de Datos	R2	Crítico
		Servidores	R3	Crítico
		Sistemas de Gestión	R4	Crítico
		Impresoras	R5	No Crítico
		Humanos	R6	No Crítico
		PC's	R7	Crítico
E - 2	Mantenimiento adecuado de las aplicaciones	Sistema Eléctrico	R1	Crítico
		Red de Datos	R2	Crítico
		Servidores	R3	Crítico
		PC's	R7	Crítico
		Impresoras	R5	No Crítico
		Humanos	R6	No Crítico
		Teléfono	R8	Crítico
		Humanos	R6	No Crítico
		PC's	R7	Crítico
		Servidores	R3	Crítico
		Red de Datos	R2	Crítico
		Teléfono	R8	Crítico

Elaborado Por: GMSM

Fecha: 20-08-2008

Mediante la siguiente tabla de costos, podremos identificar cuales son los procesos que representan mayor costo y posteriormente utilizar esta información para evaluar la prioridad de acciones frente a los procedimientos en nuestra tabla de prioridades.

Cuadro 3.9. Formato de costos de cada proceso

CODIGO DE PROCESO	PROCESOS	COSTOS REPRES. (USD $)
A	Ventas	10,000
B	Aceptación de órdenes	500
C	Envió y reparto	2,500
D	Compras	50,000
E	Producción	80,000
F	Estadísticas	5,000
G	Elaboración de Informes de la administración	1,000

Elaborado Por: GMSM

Fecha: 21/08/2008

Podemos personalizar nuestra tabla de costos según nuestro caso y detallarla según lo más realista posible, ya que de esto dependerá el darle la prioridad necesaria a cierto tipo de procesos los cuales quizás no puedan ser identificados a simple inspección.

Etapa 3. Listar los recursos utilizados por las operaciones

En esta etapa se identifican a los proveedores de los servicios y recursos usados, considerados críticos, para los procesos de cada operación en la etapa 2.

- Se tiene que identificar los recursos asociados al Sistema de Información, basados en los códigos del recurso descritos en la etapa 2.
- Se investiga y describe, si los recursos están dentro del sistema de información o fuera de éste.
- Se investiga y describe a los proveedores de servicios y recursos.
- La importancia de un mismo recurso difiere de operación en operación. Para esto se señala a que operaciones esta relacionado el mismo recurso, esto es necesario para determinar las medidas preventivas para posibles problemas del sistema de información.

Cuadro 3.10 Lista de recursos críticos utilizados

Código recurso	Recursos	Ubicación	Proveedor del servicio	Recursos utilizados por
S1	PC´S (Red)	Interno	Área de soporte	E1,E2,E3
S2	Software de administración de compras	Interno	Área de soporte	E1,E2,E3
S10	Servidores	Interno	Área de soporte	E1,E2,E3
S4	Software de gestión de órdenes	Interno	Área de Desarrollo de Software	E1
S1-2	PC´S	Interno	Área de soporte	E1,E2,E3
S11	Software clientes	Interno	Proveedor	E2,E3
		Externo	Soporte técnico	E2,E3

Elaborado Por: GMSM

Fecha: 22/08/2008

Etapa 4. Especificación de escenarios en los cuales pueden ocurrir los problemas.

- En consideración de la condición de preparar medidas preventivas para cada recurso, se ha evaluado su posibilidad de ocurrencia del problema como (alta, mediana, pequeña).

- Se calculará y describirá el período que se pasará hasta la recuperación en caso de problemas, basados en información confirmada relacionada con los sistemas de información. Mediante el siguiente cuadro podemos elaborar la probabilidad de fallas de cada uno de los recursos identificados.

Cuadro 3.11. Tabla de probabilidad de fallas de recursos

Recursos	Probabilidad de falla			
	Alta	Media	Baja	Ninguna
S1	X	X	X	
S2	X	X	X	
S3	X	X	X	
S4	X	X	X	
S5	X	X	X	
S6	X	X	X	
S7	X	X	X	

Elaborado Por: GMSM.

Fecha: 24-11-2008.

El cuadro 3.11 presenta los siguientes campos:

- Código del recurso
- Recurso
- Proveedor del servicio
- Resultados confirmados
- Análisis de riesgo (probabilidad del problema, período necesario para la recuperación, frecuencia de uso)

Cuadro 3.12. Lista de problemas probables a ocurrir

Código del recurso	Recurso	Proveedor del servicio	Resultados confirmados	Análisis de Riesgo		
			Consideraciones de preparación de las medidas preventivas	Probabilidad del problema	Periodo necesario para la recuperación	Frecuencia de uso
S1	PC´S	Soporte técnico	Preparado	Baja	2 minutos	24 horas
S2	Software de administración de compras	Área de soporte	Finalización en 6 meses	Media/Alta	1 hora	15 horas
S10	Servidores	Área de soporte	Finalización en 6 meses	Media/Alta	1 hora	15 horas
S4	Software de gestión de órdenes	Área de desarrollo	Finalización en 4 meses	Media/Alta	1 hora	15 horas
S11	Software clientes	Proveedor	Finalización en 3 meses	Baja	1 hora	15 horas
		Soporte técnico	Finalización en 3 meses	Baja	1 hora	5 horas

Elaborado Por: GMSM

Fecha: 25/11/2008

Cuadro 3.13. Tabla matriz de prioridades de atención de riesgos

IMPACTO	ALTO	Prioridad 2	Prioridad 1	Prioridad 1
	MEDIO	Prioridad 3	Prioridad 2	Prioridad 1
	BAJO	Prioridad 3	Prioridad 3	Prioridad 2
		BAJA	MEDIA	ALTA
	PROBABILIDAD			

Elaborado Por: GMSM

Fecha: 27/11/2008

En la tabla 3.13 se representa como se debe priorizar los riesgos identificados tomando en cuenta tanto:

- El impacto del riesgo y
- La probabilidad de una falla.

En la siguiente tabla se ha descrito los procedimientos de las medidas preventivas tomadas en detalle, cuando los problemas ocurren.

Las medidas preventivas se dan si se ha probado, investigado y listado los recursos necesarios para llevarlos a cabo, tales como:

- Equipo,
- Manual de fallas y
- Funcionamiento.

Cuadro 3.14. Detalles de medidas preventivas del área analizada

ORDEN	PROCESOS	PROCEDIMIENTO	MEDIDAS ALTERNATIVAS
1	Proceso de los programas que realizan la entrada y salida de la información	Ingreso y recepción de expedientes (cartas, oficios, informes, etc.), envío de los documentos a todas las áreas de la institución, salida de documentos (cartas, oficios, informes, etc.)	Puesta en funcionamiento del grupo electrógeno operaciones manuales puesta en marcha de una red LAN interna.
2	Mantenimiento adecuado de las aplicaciones	Programación de cronograma de mantenimiento, elaboración de órdenes de compra y órdenes de servicios	Puesta en funcionamiento del grupo electrógeno. Comunicación con teléfonos móviles
3	Equipamiento necesario para un funcionamiento óptimo del sistema	Actividades de soporte técnico para casos de fallas Almacén de control de bienes, Programación de requerimientos.	Puesta en funcionamiento del grupo electrógeno Comunicación con teléfonos móviles. Puesta en Marcha de una red LAN interna.

Elaborado Por: GMSM

Fecha: 27/11/2008

El cuadro 3.14 presenta los siguientes campos

- Orden
- Procesos
- Procedimiento
- Recursos necesarios (medidas alternativas)

Como paso OPCIONAL, se pueden mostrar los riesgos en la matriz de análisis de riesgo. Cada riesgo se coloca en el rectángulo.

Cuadro 3.15. Matriz de análisis de riesgo

IMPACTO	ALTO	Software de gestión de compras		
	MEDIO			
	BAJO	PC´S		
		BAJA	MEDIA	ALTA
	PROBABILIDAD			

Elaborado Por: GMSM

Fecha: 27/11/2008

Etapa 5: Determinar y detallar las medidas preventivas

Se han determinado y descrito las medidas preventivas para cada recurso utilizado en el uso y mantenimiento de los sistemas de información, cuando los problemas ocurran, considerando el entorno de problemas que suceden y el período de interrupción aceptable que se estima en la etapa 4.

Si hay más de un conjunto de medidas preventivas para un recurso, se ha determinado cual se empleara, de acuerdo al peso de factor se debe priorizar tomando en consideración sus costos y efectos. Los campos principales considerados en el cuadro 3.16 son los siguientes:

- Código del recurso
- Recurso
- Problema asumido (Análisis de riesgo)
- Medidas preventivas / alternativas

Cuadro 3.16. Lista de medidas preventivas

Código del recurso	Recurso	Problema asumido (Análisis de riesgo)		Medidas preventivas/alternativas	
		Posibilidad de ocurrencia del problema	Periodo de parada aceptable	Ejecutada SI/NO	Contenido
S1	PC´S	Baja	6 horas	NO	Transacciones manuales
S2	Software de administración de compras	Media/Alta	6 horas	SI	Transacciones manuales
S10	Servidores	Media/Alta	6 horas	SI	Red local
S4	Software de gestión de órdenes	Media/Alta	2 horas	SI	Transacciones manuales
S11	Software clientes	Baja	4 horas	NO	Transacciones manuales

Elaborado Por: GMSM

Fecha: 27/11/2008

Cuadro 3.17 Matriz de análisis de riesgos

IMPACTO				
	ALTO	Sistema eléctrico		
	MEDIO			
	BAJO			
		BAJA	MEDIA	ALTA
	PROBABILIDAD			

Elaborado por: GMSM

Fecha: 27/11/2008

Etapa 6. Formación y funciones de los grupos de trabajo

Se debe determinar claramente los pasos y la secuencia lógica para establecer los grupos de trabajo, desde las acciones en la fase inicial, hasta la finalización de las tareas asignadas, las cuales son importantes para el manejo de la crisis de administración de los recursos informáticos.

Los grupos de trabajo permanecerán en operación cuando los problemas ocurran, para tratar de solucionarlos.

Se elaborará un organigrama de la estructura funcional de los grupos de trabajo, en el mismo debe incluirse las responsabilidades.

Un modelo de asignación de funciones del grupo de trabajo relacionado con la gestión de riesgos, se incluye a continuación:

Cuadro 3.18. Funciones de los grupos de trabajo del sistema Administrativo de los sistemas de información.

Dirección	Nombre	Cargo	Funciones
Área de administración		Director técnico	Gerente general
		Especialista	Encargado de la oficina de abastecimientos y servicios auxiliares
		Especialista	Encargado personal de la oficina ejecutiva de personal
Área de desarrollo de software		Director técnico	Dirección técnica de desarrollo de software
		Especialista	Responsable del respaldo de la información de bases de datos y aplicaciones
		Especialista	Responsable de configuración e instalación de los programas o aplicaciones
Dirección técnica de soporte		Director técnico	Dirección técnica de soporte técnico
		Técnico	Responsable de las PC´s y servidores
		Técnico	Responsable del software base
		Especialista	Responsable de correo electrónico
		Técnico	Soporte técnico a usuarios

Elaborado Por: GMSM

Fecha: 27/11/2008

Etapa 7. Desarrollo de los planes de acción

Cuadro 3.19 Lista de acciones ante fallas de recursos

Código del recurso	Recurso	Acción	Como confirmar	Operador	Programa para la acción	Localización para la acción	Ocurrencia del problema
S1	PC´S	Confirmar la ocurrencia de los problemas	El Área de administración comunicará al responsable sobre la ocurrencia del problema	Área de administración	En la mañana	Todas las oficinas	Falla de los PC´S
S2	Software de administración de compras	Confirmar la ocurrencia de los problemas	El administrador de la red supervisará la red e informará cualquier problema	Dirección técnica	En todo el día	Oficinas administrativas	Caída de la red en ciertas áreas
S3	Servidores de gestión	Confirmar la ocurrencia de los problemas	El administrador de la red supervisará la red e informará cualquier problema	Dirección técnica	En todo el día	Oficinas administrativas	Caída de la red en el área de gestión
S10	Sistemas de gestión	Confirmar la ocurrencia de los problemas	El administrador de los servidores supervisará la red e informará cualquier problema	Dirección técnica	En todo el día	Oficinas administrativas	Paralización o fallas en los programas o aplicaciones
S11	Software clientes	Confirmar la ocurrencia de los problemas	Cobertura de los medios	Área de soporte técnico	En todo el día	Lugar de la persona a cargo	Caída de la red en el área de interés

Elaborado Por: GMSM

Fecha: 27/11/2008

Se estableció los días en los cuales los problemas son más probables a ocurrir, incluyendo los sistemas, clientes, proveedores, procesos productivos e infraestructura de la organización. Se señalan los días anunciados, cuando los problemas pueden ocurrir y se mencionan las posibles soluciones con tiempos de ejecución para regresar a la operación normal.

El cuadro 3.19 es un modelo donde debemos señalar exactamente las ocurrencias de fallas y las acciones respectivas aplicadas para cada una de las posibles contingencias. También se deben asignar los responsables de cada proceso.

Etapa 8. Preparación de la lista de personas y organizaciones para comunicarse en caso de emergencia

Se creará un directorio telefónico del personal considerado esencial para la organización en esas fechas críticas, incluyendo el personal encargado de realizar medidas preventivas y los responsables para las acciones de la recuperación y preparación de medios alternativos. A su vez también se creará un listado telefónico de todos los proveedores de servicio del recurso.

Este directorio se usa para realizar comunicaciones rápidas con los proveedores de servicio del recurso, incluso con los fabricantes, vendedores o abastecedores de servicio contraídos, si ocurren los problemas, para hacer que investiguen y que identifiquen las causas de los problemas y que comiencen la recuperación de los sistemas.

Cuadro 3.20 Formato de lista telefónica del personal esencial en caso de problemas relacionados con el sistema administrativo.

FUNCION		Empleado	Primer número de contacto	Segundo número de contacto	Tiempo
Dirección	Cargo				

Elaborado Por: GMSM

Fecha: 27/11/2008

Cuadro 3.21. Formato de lista telefónica de los proveedores de servicios

Código del Recurso	Recurso	Proveedor del servicio	Departamento o cargo	Sección o empleado a cargo	Número Telefónico

Elaborado Por: GMSM

Fecha: 27/11/2008

Cuadro de análisis de riesgos

Como resultado final deberemos elaborar un cuadro donde se muestre los principales componentes del plan de contingencias. En la cual podremos anotar los riesgos en el siguiente formato tabla de análisis de riesgo, la prioridad que tendrán las acciones de

determinada área afectada en función al impacto tanto funcional como de costos, así como también anotaremos su correspondiente estrategia de contingencia.

Cuadro 3.22. Formato tabla de análisis de riesgos

Área afectada	Riesgos identificados	Impacto	Área relacionada	Probabilidad de falla	Área de Acción	Prioridad	Estrategia de contingencia
Todas las oficinas	Pérdida de software de cliente						
Todas las oficinas	Falla del software de administración de compras						
Todas las oficinas	Falla de los servicios de red (servidores)						
Todas las oficinas	Falla de los PC´s						

Elaborado Por: GMSM

Fecha: 27/11/2008

Etapa 9. Pruebas y monitoreo.

En esta etapa hay que desarrollar la estrategia seleccionada, implantándose con todas las acciones previstas, sus procedimientos y generando una documentación del plan.

Hay que tener en claro como pasamos de una situación normal a una alternativa, y de qué forma retornamos a la situación normal. Hay situaciones en que debemos de contemplar la reconstrucción de un proceso determinado, ejemplo: por alguna circunstancia dada se determinó que la facturación se realice en forma manual, restablecido el servicio que nos llevó a esta contingencia debemos tener el plan como recuperar estos datos para completar la información que día a día utilizan las demás áreas.

Antes de realizar las pruebas, los planes deberían ser revisados y juzgados independientemente en lo que respecta a su eficiencia, eficacia, oportunidad y razonabilidad. Las pruebas recomendadas para los planes de recuperación de desastres incluyen una prueba periódica preliminar y un ensayo general, en el que se crea un simulacro de una crisis con el fin de observar la eficacia del plan. Las actividades importantes a realizar son:

- La validación de las estrategias de continuidad de los negocios de una unidad de negocios.
- La validación e implementación de un plan (con las operaciones de la empresa y los representantes de dichas operaciones)
- Realización de pruebas en cada unidad para analizar la eficacia y eficiencia de la solución.
- La preparación y ejecución de pruebas integradas para verificar la eficacia de la solución.

La preparación y ejecución de pruebas casos/eventos, probar las respuestas en caso de situaciones de crisis, en base a un caso en el que los eventos ocurren al azar y se intensifican en forma gradual.

3.2.10. Criterios sobre sistemas de información en internet.

La seguridad es uno de los aspectos más conflictivos del uso de las tecnologías de la información. Es suficiente comprobar cómo la falta de una política de seguridad global está frenando el desarrollo de Internet en áreas tan interesantes y prometedoras, como el comercio electrónico o la interacción con las administraciones públicas.

Los recientes avances en las telecomunicaciones y en la computación en red han proporcionado la aparición de canales rápidos para la propagación de datos a través de sistemas digitales. Las redes abiertas están siendo utilizadas cada vez más como una plataforma para la comunicación en nuestra sociedad, pues permiten rápidos y eficientes intercambios de información con un bajo coste económico asociado y con una fácil accesibilidad.

El desarrollo actual y las perspectivas de futuro de las "superautopistas de datos" y de una infraestructura global de información, es decir, de Internet y de la World Wide Web (WWW), crean toda una variedad de nuevas posibilidades. Sin embargo, la realización efectiva de tales posibilidades están influidas por las inseguridades típicas de las redes abiertas: los mensajes pueden ser interceptados y manipulados, la

validez de los documentos se puede negar, o los datos personales pueden ser recolectados de forma ilícita. Como resultado, el atractivo y ventajas ofrecidas por la comunicación electrónica, tanto en el desarrollo de oportunidades comerciales entre organizaciones privadas como en las interrelaciones entre las organizaciones públicas y los ciudadanos, no pueden ser explotados en su totalidad.

3.3. Auditoria, seguridad y control de los ambientes.

Los escándalos contables de principios de la década han provocado un aumento de los riesgos que implica un análisis de indicadores clave como la sensibilización, tanto de los reguladores como de las organizaciones por el control interno. La existencias de nueva normativa al respecto, las buenas prácticas de gobiernos corporativos, las necesidades de transparencia en la gestión como un activo más de las organizaciones, o la búsqueda de la eficiencia en los procesos internos han actuado durante los últimos años como catalizadores para la mejora de los mecanismos de control interno en las organizaciones.

Entramos así, en una fase de madurez de las organizaciones, en las que la mejora de la eficiencia y el control de sus actividades comienzan a constituirse en necesidades básicas. Dentro de las diferentes actividades que componen la estrategia de control interno de las organizaciones, el control sobre la gestión de los sistemas de información gerencial, día a día adquiere una mayor atención y relevancia. Para ello podemos encontrar, de manera inmediata, algunas razones:

- La creciente dependencia de las organizaciones y sus procesos respecto a sus sistemas de información.

- Derivado de lo anterior, el aumento de la complejidad de los mismos, con entornos heterogéneos y abiertos, a la vez que integrados.

- El éxito de las estrategias de externalización de la gestión de los sistemas de información, con los que la dependencia de los sistemas de información se refuerza con la dependencia de uno o varios proveedores de servicio.

- El uso cada más intensivo de redes de información tanto internas como intranets, y su integración a la gran red mundial conocida como internet.

Prueba de la mayor importancia que el control sobre la gestión de los sistemas de información gana día a día, son el hecho de que, por ejemplo, la normativa europea de autorización de organismos pagadores, define, como uno de sus cuatro grandes criterios de autorización, el del fomento del uso de los sistemas de información como soporte a todos sus procesos y el del establecimiento de un sistema integrado de gestión de la seguridad (SGSI), que no es más que el reflejo del aumento del nivel de control sobre los sistemas de información.

En este escenario, el papel de la auditoría informática se muestra como una nueva herramienta para la mejora del control interno en las organizaciones

3.3.1. Auditoría informática como elemento de control interno

En el momento en el que las organizaciones adquieren conciencia sobre la necesidad de aumentar el nivel de control sobre la gestión de sus sistemas de información, surge la siguiente pregunta natural: ¿pero qué es realmente la auditoría informática y cómo puede ayudarme?

Es natural esta duda desde la perspectiva de que, tradicionalmente, los departamentos de control interno o auditoría interna, están compuestos por perfiles muy cercanos al negocio, principalmente financiero y, en algunos casos, operativo.

A continuación se intenta desglosar algunos de los ámbitos en los que la función de la auditoría informática puede ayudar a la mejora de los sistemas de control interno de las organizaciones, a través de la propia evolución que la labor del auditor informático ha ido experimentando desde sus inicios.

En sus inicios, el auditor informático surge como un apoyo a los tradicionales equipos de auditoría. Su labor de apoyo consistía básicamente en la obtención de información financiera de los sistemas de información en los que residía y tratarla, con herramientas específicas de tratamiento masivo de datos, para facilitar la labor de los equipos de auditoría financiera. Entre las grandes ventajas que el apoyo del auditor informático ofrecía era el da la validación del total de la información disponible, en lugar de los habituales procedimientos de muestreo.

Dicha labor continúa siendo hoy día una de las principales tareas del auditor informático. Así, es fácil encontrar auditores informáticos tratando información para validar información contable compleja de obtener como pueden ser, por ejemplo, en el ámbito financiero, la validación del cálculo de la periodificación de intereses, o en ámbitos productivos el de la amortización de inmovilizados o la valoración de existencias.

En paralelo, el hecho de que, cada vez más, la información contable de las organizaciones fuese tratada automáticamente y casi por completo en sistemas informáticos, condujo a una nueva preocupación.

¿Son íntegros los datos de que dispone el equipo de auditoría? Con esa preocupación, poco a poco, en esa labor de apoyo al auditor financiero, el auditor informático pasa, de meramente tratar los datos contables, a cuestionarse la fiabilidad de los mismos.

Comienza entonces a plantearse nuevos objetivos de control, como son el control de acceso sobre la información, la gestión de autorizaciones, y los mecanismos de registro de actividad sobre dicha información.

En el momento en el que el auditor informático comienza a plantearse objetivos de control sobre quién debe acceder a qué información, qué puede hacer con ella, o a cuestionarse la integridad de la misma, comienza a necesitar y a obtener un conocimiento profundo sobre los procesos de negocio de la compañía. Por otra parte, la integración de dichos procesos en aplicaciones informáticas, provoca que gran

parte de los controles que se aplican sobre los mismos se definan en dichas aplicaciones. A partir de este instante, la labor del auditor informático comienza a confluir con la del auditor financiero y/o de gestión, tanto interna como externa, adquiriendo una doble versión de especialista en la definición de procesos de control interno en los procesos de negocio y en su aplicación o análisis sobre los sistemas de información que los soportan.

Finalmente, en paralelo a la función de apoyo a las auditorías tradicionales como la financiera, administrativa y de gestión, los auditores comenzaron a plantearse nuevas funciones relacionadas con la auditoría informática. Entre los principales impulsores de esas nuevas funciones, podemos encontrar:

- Los organismos reguladores internacionales, que empezaron a generar normativa específica aplicable sobre los sistemas de información de las organizaciones y sus procesos de gestión.
- Los sistemas de comercio electrónico, tanto entre organizaciones (B2B), como orientada a clientes finales (B2C), que han impulsado la mejora de los procesos de comercialización de productos pero a la vez han abierto la puerta a nuevos riesgos derivados de la necesidad de "abrir" los sistemas de información de las organizaciones a terceros.
- El aumento de la complejidad de los sistemas de información y la dependencia de las organizaciones respecto a los mismos, que en ocasiones se muestran opacos para la dirección de las organizaciones y para sus usuarios.

Con ellos, se generó una sensibilización hacia la seguridad de los sistemas de información, entendiendo la misma desde los tres puntos de vista tradicionales:

- Confidencialidad.
- Disponibilidad.
- Integridad.

Los auditores informáticos comenzaron a analizar los riesgos asociados al uso de los sistemas de información y los controles destinados a garantizar sus tres pilares básicos. Así, se incluyen funciones como de análisis de vulnerabilidades, evaluación de planes de continuidad de negocio, y, en general, el análisis de los procesos de gestión.

En definitiva, el papel actual del auditor informático dentro de las organizaciones lo podemos resumir en dos grandes tareas principales:

• Apoyo del auditor interno, en la definición y aplicación de controles sobre los procesos de negocio de las organizaciones, en tanto que gran parte de los mismos se aplican desde sus sistemas de información.

• Auditoría de la gestión de los sistemas de información, con dos objetivos:

- Que los sistemas de información soportan adecuada y eficientemente los procesos de negocio de las organizaciones.
- Que la información tratada por los sistemas de información dispone de un nivel de seguridad adecuado a su valor y a los riesgos asociados a su uso.

Una vez que las organizaciones adquieren conciencia de la necesidad de disponer de una función de auditoría informática y de qué objetivos persigue con ella, surge la siguiente cuestión; ¿cómo lo llevo a la práctica de mi organización? No nos debe generar gran preocupación el encontrarnos con esta cuestión sin tener muy clara la respuesta. A día de hoy, no es atrevido decir que el 90% de las organizaciones en Ecuador se encuentran todavía en este punto, y que sólo un 10% (principalmente entidades financieras y aseguradoras), lo tienen resuelto.

A la hora de formalizar la función de auditoría informática dentro de una organización, existen varias alternativas y, a su vez, diferentes puntos a considerar:

- La complejidad de los sistemas de información de nuestra organización y la dependencia de nuestros procesos internos respecto a los mismos (no sólo en términos de disponibilidad, sino también de confidencialidad e integridad).
- El nivel de especialización necesario para llevar a cabo dicha función.

La complejidad de nuestros sistemas de información nos puede dar una medida del volumen de trabajo potencial que podría realizar la función de auditoría informática en nuestra organización.

Para muchas organizaciones, la complejidad de sus entornos todavía puede no ser tal como para requerir una dedicación "full-time" de personal para el desarrollo de la función de auditoría informática.

Por otra parte, de acuerdo a las funciones típicas del auditor informático, descritas en el punto anterior, el perfil del auditor informático es un perfil muy específico. Si se desglosa un poco las principales habilidades del auditor informático, nos encontramos:

- Buen conocimiento de los procesos de negocio.
- Buenos conocimientos contables.
- Conocimientos informáticos desde varios puntos de vista:

- Programación.
- Administrador de sistemas.
- Administrador de bases de datos.
- Herramientas de auditoría informática.
- Soluciones de seguridad.

En ocasiones, las tendencias naturales a la hora de cubrir las necesidades de auditoría informática son básicamente dos:

- Reaprovechar a algún auditor interno con conocimientos avanzados de informática.
- Incluir un informático dentro del equipo de auditoría interna.

En ambos casos, desde nuestra experiencia podemos contar algunas excepciones dentro de un nutrido número de decepciones, tanto para la organización como para el empleado que se ve responsable de una función a la que no sabe muy bien cómo dotar de contenido.

Desde los dos puntos de vista antes mencionados, una opción razonable, al menos en el arranque de la función de auditoria informática, es la de contar con el soporte de expertos en la materia.

Así, como decíamos anteriormente, podemos encontrar diferentes aproximaciones a la hora de formalizar la función de auditoría informática dentro de las organizaciones:

- Externalizar totalmente la función, mediante acuerdo marcos, en los que, de manera mixta, la organización y expertos en la materia definen los objetivos de control y son los expertos los que desarrollan los trabajos de auditoría.
- Arrancar de manera inicial la función de auditoría informática, dotando a la organización de personal dedicado a ello, con el apoyo de expertos que asesoren a la hora de dotar de contenido a la función y formar al personal interno en el desarrollo de las habilidades necesarias.
- Dotar a la organización de recursos específicos dedicados en exclusiva a la función de auditoría informática.

Cualquiera de las anteriores será válida en función del análisis que cada organización haga de sus necesidades en este sentido. Así, podemos encontrar entidades financieras que han optado con éxito por externalizar totalmente su función de auditoría informática, contando siempre con expertos en cada materia concreta, mediante acuerdos marcos, mientras que otras han optado por dotar de personal interno dicha función y acometerlo totalmente de manera interna.

"La seguridad informática puede ser definida, básicamente, como la preservación de la confidencialidad, la integridad y la disponibilidad de los sistemas de información" (Tipton: 2006). Dependiendo del entorno de la organización, se pueden tener diferentes amenazas que comprometan a los objetivos previamente mencionados. Ante un riesgo concreto, la organización tiene tres alternativas: aceptar el riesgo, hacer algo para disminuir el impacto o transferir el riesgo. A las medidas o salvaguardas que se toman para disminuir un riesgo se les denomina *controles de seguridad.* Los controles de seguridad informática usualmente se clasifican en tres categorías: controles físicos, controles lógicos o técnicos y controles administrativos.

Para que los controles sean efectivos, éstos deben estar integrados en lo que se denomina una *arquitectura de seguridad informática*, la cual debe ser congruente con los objetivos de la organización y las prioridades de las posibles amenazas de acuerdo al impacto que éstas tengan en la organización.

Una fase fundamental en el diseño de la arquitectura de seguridad informática es la etapa de análisis de riesgos, que comprende los siguientes pasos:

Definir los activos informáticos a analizar.

1. Identificar las amenazas que pueden comprometer la seguridad de los activos.
2. Determinar la probabilidad de ocurrencia de las amenazas.
3. Determinar el impacto de las amenaza, para establecer una priorización.
4. Recomendar controles que disminuyan la probabilidad de los riesgos.
5. Documentar el proceso.

Las metodologías de análisis de riesgo difieren esencialmente en la manera de

estimar la probabilidad de ocurrencia de una amenaza y en la forma de determinar el impacto en la organización. Las metodologías más utilizadas son *cualitativas*, en el sentido de que dan una caracterización de "alta/media/baja" a la posibilidad de contingencia más que una probabilidad específica. El estándar ISO/IEC 27001 adopta una metodología de análisis de riesgos cualitativa. El ISO/IEC 27001 es un estándar internacional para los sistemas de gestión de la seguridad informática, que está estrechamente relacionado al estándar de controles recomendados de seguridad informática La dificultad de adoptar una metodología de análisis de riesgo cuantitativa es la complejidad de determinar el impacto de un evento no deseado y, principalmente, la falta de datos suficiente para poder determinar de manera exacta las funciones de distribución de probabilidad para las amenazas más comunes.

Por otro lado, en las metodologías cualitativas, la estimación de probabilidades dependerá de la experiencia de quienes realizan el análisis. Además de estas limitaciones en el enfoque actual de análisis de riesgos, existen otras de mayor alcance que exploraremos en la siguiente sección.

a) Limitantes del análisis de riesgo

En general, a pesar de que se han desarrollado muchas soluciones a los problemas de la seguridad, la apreciación general es que la inseguridad es un problema latente. La perspectiva parece poco optimista, principalmente debido a que los atacantes han pasado de ser aficionados en busca de notoriedad a criminales en busca de lucro.

Posiblemente una de las principales razones por las cuales los problemas de seguridad informática no han sido resueltos es la aparición frecuente de nuevas amenazas. Como un ejemplo de esto es la evolución del malware: los virus altamente nocivos y de amplia difusión han dado lugar a *botnets* furtivos, de difícil detección y dirigidos a objetivos específicos.

Precisamente una de las debilidades de las metodologías de análisis de riesgo es que parten de una visión estática de las amenazas así como de los controles requeridos para disminuir los riesgos. El ciclo de vida establecido para las arquitecturas de seguridad informático suele ser demasiado extenso ante un entorno en cambio constante.

Los cambios en los riesgos que debe considerar una organización tienen dos orígenes:

a) El surgimiento de nuevas amenazas
b) La adopción de nuevas tecnologías que da origen a riesgos no previstos.

Todo sistema de información evoluciona, debido a la integración de hardware y software con características nuevas y más atractivas para los usuarios, así como al desarrollo de nuevas funcionalidades. Estos cambios abren la posibilidad de riesgos imprevistos y también pueden crear vulnerabilidades donde antes no existían.

Algunos estudios han demostrado que existe una brecha entre el uso de tecnología moderna y el entendimiento de las implicaciones para la seguridad inherentes a su

utilización. En su momento, los administradores de sistemas de información que migraron sus organizaciones a entornos altamente interconectados seguían visualizando las amenazas desde un punto de vista pre-conectividad.

Como consecuencia, expusieron a sus organizaciones a riesgos de los cuales no eran concientes, se negaban a aceptar o frecuentemente estaban poco preparados para manejar. Un escenario similar se ha presentado en la migración a las redes de área local inalámbricas. El uso de redes inalámbricas requiere de razonamientos distintos a los de la seguridad alambrada.

Es entonces evidente que se requiere de arquitecturas de seguridad dinámicas, que sean altamente adaptables a los cambios en el entorno y en el sistema de información mismo, así como capaces de resistir a ataques no previstos. Se ha buscado alcanzar esas características imitando los mecanismos adaptativos de los seres vivos, tomando como modelo, por ejemplo, el sistema inmune.

En el presente trabajo proponemos una metodología de análisis y diseño de arquitecturas de seguridad informática basada en las técnicas de control adaptativo.

b) Controles de seguridad adaptativos.

En la mayoría de los casos, los controles de seguridad son de lazo abierto, esto es, el resultado de su funcionamiento no es retroalimentado para mejorar el desempeño del control. Por ejemplo, el cortafuego es uno de los controles más comúnmente

utilizados en las redes informáticas. Sus reglas de generalmente son fijas, y ante un cambio en los requerimientos de tráfico en la red, se deben cambiar manualmente las reglas de filtraje.

Una manera de convertir al cortafuego en un mecanismo de lazo cerrado sería acoplarlo a un detector de intrusiones de modo tal que ante la detección de un posible ataque las reglas se modifiquen automáticamente para bloquear el tráfico sospechoso. En general, la clave para lograr controles de seguridad adaptativos es convertirlos en controles de lazo cerrado. Para que el control pueda adaptarse a los cambios debe contar con un mecanismo de ajuste de sus parámetros de acuerdo al comportamiento actual del sistema y a un modelo de referencia que indique cuál debería ser el comportamiento deseado.

El primer punto es entonces establecer objetivos de control que se desean alcanzar mediante mecanismo. Estos deben estar relacionados a la confidencialidad, integridad y/o disponibilidad de los datos, la información, los sistemas, etc. En segundo lugar, y como aspecto esencial, debe establecerse un indicador de monitoreo de cumplimiento de los objetivos de seguridad para determinar cuándo es necesario un ajuste en los parámetros del controlador. Este punto supone que existe un modelo del comportamiento normal del sistema así como de las acciones requeridas para restablecerlo a la normalidad cuando se presente una anomalía. La construcción de modelos para la detección de anomalías está siendo investigada como una técnica para la detección de intrusiones.

c) Metodología propuesta

La metodología propuesta de análisis y diseño de una arquitectura de seguridad informática está centrada en el concepto de control adaptativo, si bien reconociendo que por la complejidad inherente a los sistemas de información, este concepto se aplicará como una referencia más que como una aplicación estricta de la teoría del control.

Esbozaremos solamente las etapas de la metodología propuesta:

1. Establecer los objetivos de control a alcanzar y/o mantener, en términos de confidencialidad, integridad y/o disponibilidad de los subsistemas del sistema a analizar.
2. Definir una medida que permita cuantificar el grado de logro de los objetivos de control o la desviación del mismo. Denominaremos a dicha medida, la *función de control*, la cual medirá el grado de confidencialidad, integridad y/o disponibilidad del subsistema.
3. El control de seguridad deberá diseñarse en términos de tres componentes: el *detector*, que medirá en tiempo real a la función objetivo, alimentándola al *ajustador* que en base a un modelo de referencia deberá establecer un ajuste de parámetros en el *controlador*.

El esquema anterior se utiliza frecuentemente cuando en el perímetro de una red se coloca a un detector de intrusiones, cuya función es analizar el tráfico de red y

determinar si existe evidencia de un posible ataque, y de ser así, establecer reglas de filtraje adecuadas en un cortafuego. En este ejemplo, el IDS realiza las funciones del detector, el cortafuego las del controlador y el modelo de referencia estaría implícito en la programación de acoplamiento del IDS y del cortafuegos.

Un ejemplo: integridad de servidores

Para ilustrar como debería desplegarse la metodología previamente esbozada, discutiremos a continuación un ejemplo relacionado a la integridad de un servidor de red.

La integridad del sistema operativo de un servidor de red es una de las propiedades más relevantes a preservar. Existen diferentes herramientas para verificar la integridad de los archivos de un sistema operativo, que se basan en el uso de funciones de hash o MAC (*message authentication codes*) para detectar cuando un archivo ha sido alterado. Por sí mismas, dichas estas herramientas no previenen la alteración o pérdida de archivos de sistema, sin embargo, pueden ser de mayor utilidad cuando se integran a un mecanismo de control de acceso del sistema operativo.

Recientemente se han desarrollado implementaciones de modelos de control de acceso tales como el control de acceso obligatorio, seguridad multinivel o control de acceso basado en reglas que pueden ser utilizados como mecanismos de control de la integridad del sistema.

Un elemento crítico para el éxito y la supervivencia de las organizaciones, es la administración efectiva de la información y de la Tecnología de Información (TI) relacionada con ella. En esta sociedad global esta criticidad emerge de:

- La creciente dependencia de la información y de los sistemas que proporcionan dicha información.
- La creciente vulnerabilidad y un amplio espectro de amenazas.
- La administración debe comprender y valorar básicamente los riesgos y limitaciones del empleo de las TI proporcionando una dirección eficaz y con los controles adecuados.
- Se hacía necesario establecer un marco de referencia de objetivos de control para las T.I., conjuntamente con una investigación continua aplicada a dichos controles basada en dicho marco.

3.3.2. Metodologías de control interno y auditoría informática

La proliferación de metodología en el mundo de la auditoría y el control informático se pueden observar en los primeros años de la década de los ochenta paralelamente al nacimiento y comercialización de determinadas herramientas metodológicas (como el software de análisis de riesgos).

Pero el uso de métodos de auditoría es casi paralelo al nacimiento de la informática, en la que existen muchas disciplinas en las que el uso de metodologías constituye una práctica habitual. Una de ellas es la seguridad de los sistemas de información.

Si definimos la seguridad de los sistemas de información como la doctrina que trata de los riesgos informáticos o creados por la informática, entonces la auditoría es una de las figuras involucradas en este proceso de protección y preservación de la información y de sus medios de proceso.

Por tanto, el nivel de seguridad informática en una empresa es un objetivo a evaluar y está directamente relacionado con la calidad y eficacia de un conjunto de acciones y medidas destinadas a proteger y preservar la información de la empresa y sus medios de proceso.

Resumiendo, la informática crea unos riesgos informáticos de los que hay que proteger y preservar a la empresa con un entramado de contramedidas y la calidad y la eficacia de las mismas es el objetivo a evaluar para poder identificar así sus puntos débiles y mejorarlos. Esta es una de las funciones de los auditores informáticos. Por tanto, deben profundizar más en ese entramado de contramedidas para ver qué papel tienen las metodologías y los auditores en el mismo. Para explicar este aspecto diremos que cualquier contramedida nace de la composición de varios factores expresados en el "gráfico valor" según se indica en la figura adjunta. Todos los factores de la pirámide intervienen en la composición de una contramedida.

El proceso seguido en una auditoría es similar al siguiente:

1. Determinación de la finalidad y objetivos del informe, precisando su alcance.
2. Conseguir información previa sobre el dominio, proceso o actividad a auditar.

3. Planificación del trabajo a desarrollar para cumplir con la finalidad del informe y alcanzar los objetivos.
4. Llevar a cabo los trabajos de recogida de información y documentación, que puedan efectuarse antes de la presentación de los auditores "in situ"
5. Comienzo de la auditoría: presentación ante los auditados y desarrollo de la planificación establecida.
6. Análisis y síntesis de la información obtenida con el desarrollo del programa
7. Verificación de la misma.
8. Comprobación de que se han alcanzado los objetivos señalados, cumpliendo la finalidad del informe.
9. Elaboración del informe.
10. Discusión del mismo.
11. Distribución a la dirección y afectados

El auditor debe crear las metodologías necesarias para auditar los distintos aspectos o áreas que defina en el plan auditor que se detalla en el siguiente punto.

a) El plan de auditoría informática.

Las partes de un plan de auditoría informática deben ser al menos las siguientes:

- **Funciones.** Ubicación de la figura en el organigrama de la empresa. Debe existir una clara segregación de funciones con la informática y de control interno informático, y éste debe ser auditado también. Deben describirse las

funciones de forma precisa, y la organización interna del departamento, con todos sus recursos.

- **Procedimientos** para las distintas tareas de las auditorías. Entre ellos están el procedimiento de apertura, el de entrega y discusión de debilidades, entrega de informe preliminar, cierre de auditoría, redacción de informe final, etc.

- **Tipos de auditorías** que realiza. Metodologías y cuestionarios de las mismas. Ejemplo: revisión de la aplicación de facturación, revisión de seguridad física, revisión de control interno, etc. Existen tres tipos de auditoría según su alcance: la completa de una área (por ejemplo: control interno, informática); limitada a un aspecto por ejemplo: una aplicación, la seguridad lógica, el software de base, etc.; la correctiva que es la comprobación de acciones de auditorías anteriores.

- **Sistema de evaluación** y los distintos aspectos que evalúa. Independientemente de que exista un plan de acciones en el informe final, debe hacerse el esfuerzo de definir varios aspectos a evaluar como nivel de gestión económica, gestión de recursos humanos, cumplimiento de normas, etc. así como realizar una evaluación global de resumen para toda la auditoría.

- **Nivel de exposición.** El nivel de exposición es en este caso un número del uno al diez definido subjetivamente y que me permite en base a la evaluación final de la última auditoría realizada sobre ese tema definir la fecha de la repetición

del mismo examen. Este número no conviene confundirlo con ninguno de los parámetros utilizados en el análisis de riesgos que está enfocado a probabilidad de ocurrencia. En este caso el valor del nivel de exposición significa la suma de factores como impacto, personal del área, situación de control en el área. O sea se puede incluso rebajar el nivel de un área auditada porque está muy bien y no merece la pena revisarla tan a menudo.

- **Lista de distribución de informes**

- **Seguimiento de las acciones correctoras.**

- **Plan quinquenal.** Todas las áreas a auditar deben corresponderse con cuestionarios metodológicos y deben repartirse en cuatro o cinco años de trabajo. Esta planificación, además de las repeticiones y valor agregado de las auditorías no programadas que se estimen oportunas, deberá componer anualmente el plan de trabajo anual.

- **Plan de trabajo anual.** Deben estimarse tiempos de manera racional y componer un calendario que una vez terminado nos dé un resultado de horas de trabajo previstas y por tanto de los recursos que se necesitarán.

- **Las metodologías de auditoría informática son del tipo cualitativo/subjetivo.** Podemos decir que son subjetivas por excelencia. Por tanto están basadas en profesionales de gran nivel de experiencia y

conocimientos, capaces de asesorar con recomendaciones técnicas, operativas y jurídicas efectivas, que exigen una gran profesionalidad y capacitación permanente. Sólo así ésta función se consolidará en las empresas, esto es, por el "respeto profesional" a los que ejercen la función. En el futuro la auditoría informática sólo podrá efectuarse con equipos multidisciplinarios.

b) Metodologías para el control interno.

Dos son los tipos de metodologías utilizadas para el establecimiento y definición de controles internos:

1) Metodología para clasificación de la información

Entidad de información es el objetivo a proteger en el entorno informático, y que la clasificación de la información nos ayudará a proteger especializando las contramedidas según el nivel de confidencialidad o importancia que tengan.

Ejemplos de entidades de información son: Una pantalla, un listado, un fichero de datos, un fichero en un dispositivo, una microficha de saldos.

Los factores a considerar son los requerimientos legales, la sensibilidad a la divulgación (confidencialidad), a la modificación (integridad), y a la destrucción.

Las jerarquías suelen ser cuatro, y según se trate de óptica de preservación o de protección, los cuatro grupos serían: Vital-Crítica-Valuada-No sensible o Altamente confidencial-Confidencial-Restringida-No sensible.

Esta metodología básicamente define:

- Estratégica (información muy restringida, muy confidencial, vital para la subsistencia de la empresa).
- Restringida (a los propietarios de la información).
- De uso interno (a todos los empleados).
- De uso general (sin restricciones)

Los pasos de la metodología son los siguientes:

1. Identificación de la información.
2. Inventario de entidades de información residente y operativa. Inventario de programas, ficheros de datos, estructuras de datos, soportes de información, etc.
3. Identificación de propietarios. Son los que necesitan para su trabajo, usan o custodian la información.
4. Definición de jerarquías de información. Suelen ser cuatro, porque es difícil distinguir entre más niveles.
5. Definición de la matriz de clasificación. Consiste en definir las políticas, estándares, objetivos de control y contramedidas por tipos y jerarquías de información.

6. Confección de la matriz de clasificación. Realización del plan de acciones. Se confecciona el plan detallado de acciones. Por ejemplo, se reforma una aplicación de nóminas para que un empleado utilice el programa de incremento de salario y su supervisor lo apruebe.

7. Implantación y mantenimiento.

2) Metodología para la obtención de los procedimientos de control

Es frecuente encontrar manuales de procedimientos en todas las áreas de la empresa que explican las funciones y cómo se realizan las distintas tareas diariamente, siendo éstos necesarios para que los auditores realicen sus revisiones operativas, evaluando si los procedimientos son correctos y están aprobados y sobre todo si se cumplen.

Una metodología para la obtención de controles se expone a continuación:

Fase I. Definición de objetivos de control.

Se compone de tres tareas.

Tarea 1. Análisis de la empresa. Se estudian los procesos, organigramas y funciones.

Tarea 2. Recopilación de estándares. Se estudian todas las fuentes de información necesarias para conseguir definir en la siguiente fase los objetivos de control a cumplir

Tarea 3. Definición de los objetivos de control.

Fase II. Definición de los controles.

Tarea 1. Definición de los controles. Identificados los objetivos de control, se analizan los procesos y se definen los distintos controles que se necesitan.

Tarea 2. Definición de necesidades tecnológicas (hardware y herramientas de control).

Tarea 3. Definición de los procedimientos de control. Se desarrollan los distintos procedimientos que se generan en las áreas usuarias, informática, control informático y control no informático.

Tarea 4. Definición de las necesidades de recursos humanos.

Fase III. Implantación de los controles.

Una vez definidos los controles, las herramientas de control y los recursos humanos necesarios, no resta más que implantarlos en forma de acciones específicas.

Terminado el proceso de implantación de acciones habrá que documentar los procedimientos nuevos y revisar los afectados de cambio. Los procedimientos resultantes serán:

- Procedimientos propios de control de la actividad informática.
- Procedimiento de distintas áreas usuarias de la informática, mejorados.
- Procedimientos de áreas informáticas, mejorados.

- Procedimientos de control dual entre control interno informático y el área informática, los usuarios informáticos, y el área de control no informático.

Fase IV. Estrategia de aplicación

La ejecución de proyectos de autoevaluación de control (AEC) debe realizarse de acuerdo con un método sistemático y estructurado, que asegure en todo tiempo que los esfuerzos llevados a cabo por los distintos participantes, se realicen en un orden y secuencia apropiados al fin que se persigue.

Un método bien diseñado permite, entre otras cosas, precisar cuáles son los diferentes ámbitos de participación, asegurar una ejecución eficaz, eficiente del proceso y que los resultados posean las características de calidad que cumplan con las expectativas de la administración, del personal responsable de las operaciones y de los auditores internos.

Los elementos constitutivos de la estrategia pueden ser establecidos de acuerdo con las etapas que a continuación se proponen:

1) Proceso de involucramiento y preparación de la AEC.
2) Selección y aplicación de la metodología.
3) Desarrollo de la AEC
4) Determinación de las acciones de mejora.
5) Comunicación de resultados.

Con el fin de ilustrar la manera en que el proceso opera, a continuación se describe cada una de las etapas antes mencionadas.

La naturaleza del proceso, como ya se ha mencionado, requiere de la participación de los diferentes niveles de la organización, lo que asegura que los esfuerzos se traduzcan en resultados tangibles. Muy importante en este sentido, es la actitud entusiasta y propositiva del auditor.

Al inicio del proceso, es necesario que el auditor tenga un acercamiento con la máxima autoridad de la organización con el fin de inducirlo al debido entendimiento del objetivo, enfoque, alcance y metodología de la AEC y de cómo éste proceso puede favorecer el mejoramiento de los controles que dan apoyo a su responsabilidad principal, que es el cumplimiento de los objetivos de la organización.

Con ello se busca lograr un apoyo amplio de su parte, con el fin de que las acciones de mejora derivadas del proceso sean aplicadas oportunamente por todos los responsables de lograr los objetivos.
Este mismo proceso debe llevarse a cabo con los mandos directivos dependientes de la dirección general.

Para lograr éxito en la implementación de estos procesos, se requiere que el director general y otros miembros prominentes de la alta administración muestren en los hechos una actitud de respaldo a los objetivos, premisas y técnicas de la AEC, adoptándola como una herramienta integrada al proceso administrativo.

Esta actitud debe apoyar la filosofía que persigue este proceso, así como también a los principios en los que se sustentan las distintas etapas. También implica el reconocimiento y respeto al trabajo del auditor dentro de la organización. Los más altos directivos deben dar una señal clara y contundente a todos los demás niveles sobre la importancia y beneficios que aporta la AEC al cumplimiento de los objetivos fundamentales de la organización. También deben resaltar en su mensaje la importancia de la participación constructiva de quienes específicamente habrán de involucrarse en el proceso.

Mandos directivos. Como consecuencia del respaldo otorgado por la alta administración, los mandos directivos responsables de cada una de las funciones y procesos básicos del negocio, deben comprometerse con el proceso, mediante su involucramiento en sus distintas etapas, así como también favoreciendo el cumplimiento oportuno de las acciones de mejora resultantes de la AEC. Los miembros de este nivel organizacional deben mostrar respeto a las opiniones vertidas por el personal participante, sin importar el nivel que posean, de forma tal que todos los puntos de vista converjan hacia la identificación de áreas de oportunidad para el mejoramiento de los controles. Por su parte el Auditor Interno debe lograr ser visto como un aliado en el mejoramiento del sistema de control.

Personal responsable de los procesos.- El involucramiento de este personal se basa en el hecho ya mencionado, de que ellos operan la mayor parte de los controles que ayudan a lograr los objetivos específicos del área a la que pertenecen. Este personal conoce con claridad cuáles controles son eficaces y eficientes y cuáles otros no lo

son, ya sea por su mal diseño o falta de actualización a los cambios que las operaciones tienen al transcurso del tiempo. Sus opiniones son aportaciones importantes acerca de cómo mejorar el control y por lo tanto la posibilidad de que los objetivos se alcancen conforme lo planeado.

No es necesario considerar a todo el personal, sino más bien identificar solo a aquellos que en una actitud abierta y constructiva pueden realizar las mejores aportaciones.

Facilitadores. La tarea principal de este personal es conducir ordenada y metodológicamente el proceso, asegurar que las premisas se están cumpliendo en el tiempo planificado y en su caso, también aclarar cualquier duda a los participantes de la AEC. Ayudan a enfocar la atención de los participantes en los puntos clave o críticos para el logro de los objetivos. Los facilitadores tienen la tarea importante de documentar cada una de las etapas del proceso, que servirá de base para focalizar adecuadamente los resultados del mismo.

Los facilitadores generalmente son los auditores, aunque también puede ser personal especialista contratado para estos propósitos; sin embargo, los auditores son quienes naturalmente pueden llevar a cabo esta tarea, dado que conocen con claridad cuáles son los objetivos de la organización, los objetivos de cada área y además cuentan con el conocimiento de los sistemas de control establecidos y una idea muy aproximada del nivel de eficiencia y eficacia con que operan.

1. Preparación de la AEC

En esta etapa debe llevarse a cabo una presentación en la cual se precise detalladamente el objetivo del proceso en los ámbitos de competencia particulares, se acuerde el programa de trabajo correspondiente, se identifiquen los participantes idóneos por parte del responsable del área a evaluar con la orientación del auditor interno, y se obtenga la información relativa a los objetivos y funciones, que es el punto de partida de la AEC.

Una vez obtenida la información relativa a los objetivos y funciones, es analizada por los facilitadores para llevar a cabo el proceso "alineación de objetivos", que tiene como propósito asegurar que todo el personal conoce y entiende la manera en que sus actividades y resultados, sumados al de otros, ayudan a cumplir el objetivo del área y ésta a su vez contribuye al objetivo general de la organización.

Si entre el personal de una misma área no comparten la misma visión y orientación de los objetivos, es de esperar que sus esfuerzos no se estén canalizando adecuadamente y que los objetivos no sean logrados de forma eficiente y eficaz.

Las herramientas básicas para el levantamiento y análisis de la información, son generalmente las siguientes: matrices de riesgo/control y encuestas. Parte de la información que se debe incluir en las matrices y/o encuestas se deriva del análisis realizado a la información relativa a los objetivos y funciones.

2. Selección y aplicación de la metodología

Para la implementación del proceso de autoevaluación en los 5 componentes del modelo de control COSO, es importante determinar las herramientas que se van a utilizar para la evaluación de cada uno de ellos, es decir cuáles de los componentes conviene sean autoevaluados por la vía de los talleres de autoevaluación del control (TAC) y cuales mediante la aplicación de encuestas. Las mejores prácticas relativas a la implantación del proceso de AEC, sugieren que por lo menos el componente evaluación de riesgos sea autoevaluado a través de la realización del TAC, en tanto que los otros cuatro componentes se puedan autoevaluar a través de encuestas. Lo anterior depende de la forma, cultura y tamaño de la organización; dependerá también de si se está en una etapa de aplicación inicial o si se ha alcanzado cierta madurez, así como de los auditores; la metodología aplicable en nuestro caso, se llevó a cabo de acuerdo a lo siguiente:

3. Desarrollo de las AEC

El proceso tiene como eje principal la evaluación de la efectividad de los sistemas de control, analiza la forma en que los objetivos particulares están alineados con los objetivos básicos del negocio, las fortalezas y debilidades de los procesos operativos, la identificación de riesgos que pueden afectar los objetivos principales del área, así como los controles para identificarlos, atenuarlos y administrarlos. La realización de los talleres es la esencia del proceso, ya que de ellos se deriva la identificación de las

acciones de fortalecimiento para elevar directamente la probabilidad de que los objetivos sean alcanzados.

4. Determinación de las acciones de mejora

De acuerdo a lo anteriormente enunciado, se entiende que los objetivos básicos de los talleres son recabar información acerca de los objetivos del área sujeta a evaluación, su congruencia con los objetivos de la empresa, los riesgos inherentes para el logro de esos objetivos y los controles establecidos al efecto para administrar dichos riesgos.

La autoevaluación implica un análisis de la información mencionada; el examen es realizado por el personal del área participante en los talleres y encuestas, los que determinan en principio si los objetivos del área están orientados en el mismo sentido que los de la empresa y si es que son una parte de los mismos; es decir, determinan en qué proporción y forma contribuyen al objetivo general de la empresa.

Posteriormente, de acuerdo a su conocimiento del entorno y características de operación, determinan cuales son los riesgos que eventualmente pudieran afectar el logro de los objetivos del área, en la forma y tiempo que fueron planeados. El siguiente paso es confrontar dichos riesgos, con las políticas y procedimientos establecidos en el área; de esta comparación se precisan controles excesivos y riesgos no cubiertos o partes de riesgos contra los cuales no se están protegidos.

No necesariamente se debe tener cobertura del 100% contra todos los riesgos, por lo tanto, se les debe otorgar prioridad a los más significativos. Para evitar subjetividad al asignar importancia a los riesgos no cubiertos, éstos deben ser cuantificados, determinando en términos monetarios cual pudiera ser su efecto si llegaran a concretarse y en su caso, cuantas veces se podrían presentar en un ejercicio.

Asignada la prioridad a los riesgos no cubiertos y de acuerdo a los recursos y necesidades del área, se precisan las correspondientes acciones de mejora, se señalan a los responsables de su implementación, así como la fecha límite para su aplicación.

Esta etapa de la AEC propicia que el talento y experiencia del auditor se sume a la del personal participante para lograr mejoras relevantes mediante acciones eficaces.

5. Comunicación de resultados

Un diseño adecuado de encuestas y talleres exitosos origina mucha y diversa información; por lo tanto, una función muy importante del equipo de auditores facilitadores, es recopilar y ordenar los datos que no quedaron plasmados en las matrices de riesgo y control.

Aparentemente el informe de resultados en su forma pudiera guardar cierta semejanza con los informes de auditoría, pero en realidad es totalmente diferente, ya que en el fondo el informe contiene la esencia de las discusiones efectuadas en el taller. El reporte realmente está integrado con los comentarios de los participantes, el

auditor facilitador únicamente recopila selecciona y ordena la información y finalmente, redacta de manera legible, comprensible y clara las opiniones del personal.

En este proceso, el auditor debe procurar no emitir su opinión, sino integrar objetivamente los resultados de la AEC; esta particularidad, es lo que verdaderamente marca la diferencia con un informe de auditoría.

Una diferencia adicional a la anterior, es que una copia del informe se entrega a cada uno de los participantes, como constancia de lo acordado y de los compromisos y responsables establecidos, pero sobre todo, como una evidencia de que los resultados fueron vertidos abierta y positivamente y con total apego a las opiniones emitidas.

3.4. Análisis de vulnerabilidades y amenazas.

3.4.1. Vulnerabilidades y amenazas

De acuerdo a lo descrito en capítulos anteriores, se puede establecer que el uso de computadores ha sido uno de los causales para el incremento de las capacidades de las personas, las empresas, el comercio, las organizaciones, etc. Sin embargo, y en forma general, todo incremento o mejora de capacidades representa un costo, y en el caso de las empresas fabricantes de carrocerías metálicas, el costo incide en el incremento de las vulnerabilidades. Pero la vulnerabilidad no surge del computador

en si, la vulnerabilidad surge del uso generalizado, de la interacción entre máquina con varios usuarios (inteligencias) y máquina con varias máquinas.

Así, cuando en los años 80 hubo la proliferación de computadoras conectadas a módems telefónicos se aumentó la vulnerabilidad de acceso a los sistemas informáticos, permitiendo el nacimiento de una nueva amenaza denominada "hackers", individuos capaces de ingresar ilegalmente en las redes computacionales e incluso de alterar su contenido.

Más aun, en los años 90, las vulnerabilidades se vieron acentuadas por varios factores:

a) El surgimiento de internet y su masiva penetración en la sociedad. Eso multiplicó la cantidad de módems existentes, lo cual aumentó la vulnerabilidad de muchas redes privadas (ya que las mismas pasaron a estar conectadas a Internet, que es una red de acceso público) y fomentó la proliferación de hackers, debido a que penetrar una red ilegalmente o fabricar virus capaces de infectar miles de computadoras, pasó a ser cada vez más sencillo.

b) La sensación de desconfianza generada por la proximidad de la "falla del milenio", también conocido como Y2K. Esto se debió a la incapacidad de muchas computadoras para registrar fechas posteriores a 1999, lo cual hizo temer un "apocalipsis informático" en la transición al 2000, que finalmente no se produjo gracias a la masiva inversión en prevención y adecuación de los sistemas

computacionales a nivel oficial y privado. Esto creó otra vulnerabilidad respecto a la posibilidad de que entre los técnicos contratados se infiltraran terroristas con la finalidad de obtener información clasificada, claves para futuros atentados, alterar sistemas, causar daños o introducir virus.

c) La proliferación masiva de noticias sobre el accionar de los hackers, cuyas capacidades aparecen en muchos casos exageradas, en la que los medios de comunicación difunden hipótesis catastróficas, tales como ciudades sin energía eléctrica o aeropuertos cuyas torres de control eran hackeadas por ciberterroristas con el objeto de ocasionar la colisión premeditada entre aviones, etc..

Estos factores, entre otros, hicieron que los organismos de inteligencia de los Estados Unidos comenzaran a especular sobre la posibilidad de que algún grupo terrorista pueda cometer atentados o actos de sabotaje de gran magnitud, empleando medios telemáticos, con lo cual surgió un nuevo concepto de terrorismo, el denominado "ciberterrorismo". De ahí, en adelante se dio mayor ímpetu a la toma de medidas preventivas en relación al ciberterrorismo.

A pesar de la multiplicidad de vulnerabilidades existentes, la industria tecnológica sigue introduciendo y adoptando nuevas tecnologías dando prioridad a la prestación de servicios y la facilidad de uso, dejando con un menor nivel de importancia a la seguridad. Tal es el caso de las tecnologías wireless, voz sobre protocolo de Internet (VOIP), dispositivos de identificación de radiofrecuencia (RFID), en las que su comercialización se basa en la aceptabilidad del usuario y el bajo costo, sin

considerar la seguridad, la potencial pérdida de vidas o las políticas de seguridad nacional.

En forma general, y tomando en cuenta que en todo sistema informático intervienen básicamente tres actores: el ser humano, la tecnología y la información, las amenazas pueden ser agrupadas en cuatro áreas:

- Amenazas físicas.
- Amenazas electromagnéticas.
- Amenazas cibernéticas.
- Amenazas de interoperabilidad.

a) Amenazas físicas

A pesar de que la tecnología, ha progresado rápidamente en los últimos años, y que se pueden emplear muchas técnicas sofisticadas para inutilizar uno o varios nodos de una red, todavía, el aspecto físico es de gran importancia. Un ataque físico a redes informáticas, sistemas de comunicaciones o sistemas de energía, puede ser efectuado mediante el empleo de armas convencionales como el uso de explosivos, armas de largo o corto alcance, o simplemente utilizando puñales, alicates, desarmadores, etc, para efectuar algún corte de líneas, pudiendo causar serios problemas a una red informática. Pero se debe considerar que un ataque físico no solo involucra la destrucción total o parcial de hardware en si, también puede implicar el robo físico de una computadora de la red para intervenir en ella, o el robo de información,

mediante la substracción de computadores claves, medios magnéticos, o la copia y clonación.

En consecuencia, los nodos críticos, sistemas de comunicaciones, sistemas de energía y los computadores con información clave, son vulnerables a ataques físicos, y por lo tanto se convierten en objetivos atractivos.

b) Amenazas electromagnéticas

En términos generales, las amenazas electromagnéticas se las puede concebir en dos formas: a través de una "energía dirigida" conocida como pulso electromagnético (EMP) o mediante la guerra electrónica.

Un ejemplo de pulso electromagnético corresponde a la energía liberada por la explosión de un arma nuclear, la cual genera un campo electromagnético por encima de una cierta área de acuerdo a la altura en que se haya detonado dicha arma nuclear. Otro ejemplo, de energía dirigida y de uso cotidiano, es el empleo de máquinas de combustión interna, máquinas eléctricas, señalizadores de láser, hornos microondas, máquinas de fax, escáneres, etc., las cuales generan campos electromagnéticos en su rededor, en este caso, de baja energía, pero que para ser usadas como armas se debe incrementar su potencia. En definitiva, el empleo de "energía dirigida", dependiendo de su potencia, puede afectar al funcionamiento desde los microchips hasta los sistemas de energía eléctrica y los satélites de comunicaciones en órbita

En lo referente a la guerra electrónica, su empleo es más conocido y consiste en perturbar o anular parte o todo el espectro electromagnético, en el cual se desenvuelven especialmente los sistemas de telecomunicaciones y radares. Aquí es importante recordar que los medios de comunicaciones constituyen la base fundamental para la interacción entre los sistemas informáticos. También se puede usar tecnologías de guerra electrónica para negar o perturbar el uso de sensores, como por ejemplo los GPS.

De lo anteriormente indicado, se puede establecer que todo lo que conlleva el empleo de circuitos eléctricos, electrónicos, microelectrónicas y del espectro radioeléctrico, es vulnerable ante ataques electromagnéticos.

c) Amenazas cibernéticas

Con el uso cada vez más común de la información digitalizada y los procesos automatizados, los ataques cibernéticos se constituyen en una excelente alternativa para degradar los sistemas informáticos. Esta gran alternativa se basa exclusivamente en la inversión de recursos mínimos, complementado en la mayoría de casos, con el anonimato del ejecutor del delito. La gama de delincuentes que operan en esta área es variada, puesto que van desde un estudiante, un aficionado a los programas, un compumaniaco, un terrorista, una nación hostil o una combinación de estos.

Actualmente, la facilidad de obtener información y conocimiento, y más aún con las herramientas y técnicas computacionales que proporciona la gran red mundial conocida como internet, ha incidido en el incremento significativo del número de personas con habilidades para acceder a las redes informáticas, y las horas de uso por cada usuario también se han incrementado, con la factibilidad de cometer delitos. Generalmente, para los aficionados a la programación computacional, se constituye en un reto el descubrir vulnerabilidades de los nuevos productos lanzados al mercado, y una vez descubierta ésta son difundidas.

Lo interesante de las amenazas cibernéticas, es que los ataques se pueden realizar desde sitios remotos, ofreciéndoles un cierto grado de anonimato, más aún, si los que los realizan son compumaniacos avanzados, puesto que ellos pueden cubrir sus huellas de tal forma que se hace difícil no solo identificarlos, sino también ubicar el lugar desde donde operan. De igual manera, hasta el momento se ha hecho difícil contar con una legislación estandarizada a nivel mundial, para tratar y penalizar este tipo de delitos, lo que ha generado una mayor impunidad para este tipo de actos criminales.

A pesar de que en un inicio, se estableció una tradicional clasificación de amenazas cibernéticas (virus, troyanos y gusanos), en la actualidad ha crecido la dificultad para catalogar correctamente las múltiples amenazas cibernéticas que siguen apareciendo, en consecuencia existen diferentes formas de clasificarlas. Sin embargo, se debe dejar en claro que existe diferencia entre lo que es una amenaza y lo que es el medio que se emplea.

Para ejemplarizar lo indicado, se va a tomar el caso del narcotráfico, en el cual se pueden emplear armas, medios de transporte, y por supuesto, la droga; aquí, las armas, el transporte y la droga son los elementos empleados para realizar el narcotráfico, en consecuencia las armas, los medios de transporte y la droga por si solas no constituyen amenaza alguna, la real amenaza es el narcotráfico.

Tomando como analogía el ejemplo anterior, se puede decir que los programas maliciosos y los hackers, por si solos no son amenazas, puesto que para que una actitud se constituya en una amenaza debe existir "la voluntad de hacer daño". Desde este punto de vista las amenazas cibernéticas se las puede clasificar en forma general en dos grupos el ciberterrorismo y la delincuencia cibernética o crimen cibernético. Estos pueden ser objeto de confusión, por eso es necesario dejar en claro sus conceptos.

El término ciberterrorismo apareció en los años 1996 y es una combinación de dos palabras (ciberespacio y terrorismo), un concepto que es ampliamente aceptado, es el emitido por el center for strategic and international studies, el cual lo define como: "Ataques premeditados, políticamente motivados, realizados por grupos, agencias clandestinas o individuos, contra la información y sistemas de computadores, programas computacionales y datos, que resultan en violencia contra objetivos no combatientes." En este concepto destacamos dos aspectos: la motivación política y los objetivos civiles.

En lo que respecta a delincuencia cibernética, se puede decir que es el crimen cometido a través del uso de las tecnologías de la información.

De lo anteriormente indicado se puede establecer que los sistemas informáticos que se encuentran interconectados en red y a internet, son vulnerables a los ataques cibernéticos.

d) Amenazas de interoperabilidad

Si bien es cierto que la automatización de los procesos mejora la eficiencia y disminuye el tiempo de ejecución de los procesos, no hay que dejar de lado el tipo y la cantidad de la tecnología introducida.

En los sistemas altamente sofisticados, en que los procesos fundamentales están regidos por sensores y la microtemporización de sus procesadores, es decir, en la que el tiempo real y la velocidad de respuesta constituyen la base de su funcionalidad, el acoplamiento entre dispositivos (eléctricos, ópticos, mecánicos y/o electrónicos) y la sincronización de los relojes internos representa una de las principales vulnerabilidades, puesto que una descalibración de un reloj interno o el desperfecto en un sensor, representaría el mal funcionamiento de un subsistema, ocasionando la falla en otro subsistema, produciéndose un efecto en cascada, y por ende, causando finalmente la degradación o inoperatividad parcial o total de todo un sistema automatizado.

De lo indicado anteriormente, se puede establecer que los sistemas automatizados en que sus procesos se basan en la sincronización milimétrica de sus procesadores, son vulnerables a las amenazas de interoperabilidad.

3.4.2. Elementos empleados en las amenazas cibernéticas.

Realizando un análisis de los elementos que se emplean para efectuar los ataques cibernéticos, se puede establecer que estos caen dentro de dos grupos: los hackers y los programas y/o códigos maliciosos.

a) Hackers.

En su sentido original el término hacker define a un especialista en la computación. Gracias a ellos la tecnología de computación se desarrolló mucho más rápido. Ahora hay hackers muy jóvenes, incluso los estudiantes de escuela secundaria y preparatoria tienen las técnicas y conocimientos suficientes para ser un hacker.

Los hackers existen desde los años 60, es decir, desde antes de que existieran las computadoras personales. Por aquellas épocas eran personas que se encargaban de utilizar líneas telefónicas en forma ilegal. Actualmente, quienes violan redes telefónicas son apodados phreakers.

Uno de los primeros hackers de renombre fue John Draper. En 1970, Draper descubrió que el silbato de juguete que se incluía en las cajas de la marca de cereales

Cap'n Crunch coincidía exactamente con la frecuencia de la red telefónica de AT&T. Gracias a Draper, miles de personas comenzaron a hacer llamadas de larga distancia sin costo alguno.

Al poco tiempo la pasión por hackear líneas telefónicas se trasladó a los sistemas computacionales. Las grandes computadoras o mainframes han estado conectados entre sí desde los años 60, pero las computadoras personales, manejadas por individuos desde sus casas, empezaron a conectarse a finales de los años 70. De allí en más se comenzaron a popularizar los Bulletin Board Systems (BBS).

Un BBS puede definirse como una computadora que sirve como centro de información y mensajes para usuarios que se conectan desde las líneas telefónicas mediante módems. Un módem (abreviatura de modulador-demodulador), es un aparato que traduce los impulsos digitales de las computadoras en señales analógicas audibles de un teléfono, y viceversa. Los módems conectan a las computadoras con los teléfonos y así pueden conectarse los unos con los otros.

En forma general, se pueden distinguir, tres generaciones de hackers:

- La primera estuvo integrada por los descendientes directos de los phreakers, pioneros en la materia, y se vinculó estrechamente con el crecimiento de los BBS.

- La segunda generación de *hackers* se inició alrededor de 1990, en donde las computadoras personales se hicieron realmente populares en los hogares, y dejaron de ser utilizadas sólo por ingenieros o técnicos. Cabe mencionar que de 4.000 BBS existentes en todo Estados Unidos en 1985, se pasó a más de 30.000 en 1990. A esta segunda generación pertenece el argentino Julio Ardita, el primer hacker latinoamericano procesado en Estados Unidos. En 1995, con 20 años de edad, Ardita se "colgó" desde su casa de las redes de Telecom en Argentina y de allí logró acceder ilegalmente a la marina de Estados Unidos y al mismísimo Pentágono. Tras ser rastreado por el FBI, fue detenido en Argentina y accedió a viajar voluntariamente a Estados Unidos para ser enjuiciado.

- La tercera generación está integrada por los hackers de la "era de internet", iniciada a partir de la popularización de la "red de redes", que tuvo como año clave a 1995. A continuación, se describen algunas características de esta tercera generación.

Con la era del internet y con la aparición de la tercera generación de hackers, se generó la denominada "democratización del hacking", debido a que desde esa época ha tenido un crecimiento extraordinario el número de sitios web que difunden gratuitamente herramientas destinadas a introducirse, sin autorización, a las redes informáticas, y que en muchos casos son tan fáciles de usar que cualquier persona con poco conocimiento de computación puede manejarlas en muy poco tiempo.

Pero cómo es que operan los hackers? Generalmente siguen los siguientes pasos:

1) Investigan y buscan algunos de los sitios para hackers, en donde encuentran scripts (rutinas o pequeños programas) que escanean el sitio al cual se quiere violentar, con la finalidad de determinar el sistema operativo utilizado por el servidor de sitio y qué tipo de servidor de software se emplean, es decir, establecer su arquitectura tecnológica básica.

2) Buscan fallas o agujeros en la versión específica del software que está corriendo en el sitio, con la finalidad de encontrar una entrada, romper su código y así utilizarlo, configurando un delito contra la propiedad intelectual.

3) Esta información de fallas, luego pasa a ser difundido y se convierte en dominio público en la comunidad hacker.

4) Una vez encontrada la falla o agujero, solo la persistencia del hacker hará que penetre en el sistema.

Sin lugar a dudas, los requisitos básicos para ser un destacado hacker se circunscriben a tener conocimientos profundos de programación, para lo cual manejan con habilidad varios lenguajes como C/C++, BASIC, JAVA, LISP, PERL, HTML, ASSEMBLY (lenguaje ensamblador), sistemas operativos como UNIX, DOS, LINUX, protocolos de comunicación como el TCP/IP, el INTERNET y otros más.

Es bien conocido que el ímpetu de los hackers, especialmente los de la tercera generación, no queda ahí, sino que más bien para probar sus conocimientos, capacidades y habilidades, realizan torneos competitivos de hacking.

Todo esto, desde la óptica del positivismo, han hecho que las empresas fabricantes de software tomen conocimiento rápidamente de las fallas de sus productos y se muevan rápidamente para solucionarlos mediante los denominados "parches".

Estas habilidades son aprovechadas por varias compañías, que disponen de sistemas informáticos de nivel crítico, a tal punto que ofrecen trabajo a hackers para que prueben el nivel de seguridad, para corregir los errores que puedan existir y para prevenir accidentes en el sistema. Las organizaciones gubernamentales también necesitan del apoyo de los hackers, debido a que ellos se les encargan preparar el sistema de anti-hacking.

En el del artículo the mind of a hacker, escrito por Andee Joyce para el sitio RetailTech.com, se hace una clasificación que es generalizada en el mundo del periodismo especializado y las empresas:

1) White hat hackers (hackers de sombrero blanco): Son personas que no persiguen intereses delictivos, sino que por el contrario, creen que su misión (a veces remunerada y a veces no) es encontrar brechas en la seguridad de las computadoras y luego avisar a las partes involucradas para que puedan protegerse. En otras palabras, son hackers "buenos", que colaboran con las empresas.

2) Grey hat hackers (hackers de sombrero gris): Son aquellos que en el pasado realizaron actividades de hacking, pero que actualmente trabajan para empresas en el área de seguridad. Este tipo de hackers suelen ser contratados por las empresas, "siempre y cuando no hayan hecho anteriormente nada destructivo o claramente delictivo", su función es la protección de los sistemas de los ataques cibernéticos.

3) Black hat hackers (hackers de sombrero negro): Son los que reciben la mayor atención por parte de los medios. Se trata de individuos proclives a realizar una serie de tareas que van desde ingresar ilegalmente a distintos sitios y colocar información falsa o textos e imágenes obscenos, hasta robar números de tarjetas de crédito con la intención de cometer fraudes.

En consecuencia, la amenaza de realizar ataques informáticos, empleando hackers proviene de este último grupo, que también se los conoce como crackers. Hay que tomar en consideración que, los programas que se utilizan son herramientas muy poderosas, y al entrar ilegalmente a los sistemas informáticos de otra persona pueden violar sus redes y robar los datos, pueden manejar y controlar un sistema del servidor de Internet desde un lugar remoto, etc.

Los crackers son también hackers, pero en ellos se antepone el interés personal, por encima de toda ética y de los intereses de los demás. Los crackers utilizan sus conocimientos para lograr el dinero que quieren o alguna otra satisfacción personal. Entre ellos hay tres tipos diferentes: attacker: detiene el servicio del sistema,

intruder: tiene como objetivo robar las informaciones, destroyer: destruye el sistema de servicio contaminando con virus.

b) Programas y códigos maliciosos

A los programas o códigos maliciosos se les conoce también con el termino "Malware", que se deriva de la unión de dos palabras (en inglés) **mal**icious soft**ware**, se les atribuye una gran cantidad de diversos tipos de aplicaciones y códigos dañinos y/o potencialmente peligrosos, que actúan en un computador sin el conocimiento ni consentimiento del usuario.

El crecimiento galopante de la formas y técnicas de los elementos empleados por las amenazas cibernéticas se refleja en la dificultad de establecer una clasificación consensuada, puesto que en la actualidad, un código malicioso se puede propagar como gusano, infectar como virus, robar información importante como un spyware, escanear vulnerabilidades como un troyano y distribuir spam masivo desde el computador de la víctima.

Esta personalidad múltiple o "versatilidad" de los elementos combinados tiene efectos devastadores, ya que estos malwares producen un daño mayor que sus antecesores: pudiendo también alterar servidores de páginas web, instalar troyanos ejecutables "a futuro" y lanzar ataques de denegación de servicio al protocolo IP seleccionado como blanco. Además, pueden también, inyectar códigos maliciosos dentro de archivos ejecutables del sistema, capturar pulsaciones del teclado o crear

recursos compartidos con atributos de lectura y escritura, accesibles desde cualquier parte de Internet, entre otras "gracias".

Su perfeccionamiento también los ha llevado a buscar múltiples y variados métodos de propagación: spam con attachments infectados, códigos en archivos HTML de un servidor para infectar visitantes de un sitio o utilizan vulnerabilidades detectadas y conocidas en los sistemas-víctimas. "Hoy el 100% de los ataques exitosos por hackers, virus, troyanos, gusanos, etcétera, se producen porque existen vulnerabilidades conocidas en el sistema. En la red circulan las vulnerabilidades de los sistemas, en sitios bastante serios. Los fabricantes cuando detectan estas vulnerabilidades proporcionan los parches para solucionar el problema", dice Norman Bennet y agrega, "la dificultad actualmente es que se ha acortado el tiempo que transcurre entre el descubrimiento de una vulnerabilidad y la utilización maliciosa de ella, por lo que las empresas tienen que trabajar contra el tiempo para proteger a los usuarios". En forma general, los códigos maliciosos, tienen muchas formas de introducirse, propagarse e infectar a un sistema informático. No existe una clasificación estándar, sin embargo, de acuerdo a sus características se los ha conceptualizado en la siguiente forma:

1) Virus:

Es un pequeño programa capaz de reproducirse a sí mismo, infectando cualquier tipo de archivo ejecutable, sin conocimiento del usuario. El virus tiene la misión que le ha encomendado su programador, esta puede ser desde un simple mensaje, hasta la

destrucción total de los archivos de datos almacenados en el computador, inutilizando además gran espacio de los dispositivos magnéticos.

Lo único que tienen en común todos, es que han de pasar desapercibidos el mayor tiempo posible para poder cumplir su trabajo. Una vez infectado un PC, el virus no tiene por qué cumplir su misión al momento, algunos esperan una fecha, evento o acción del sistema para llevar a fin su objetivo.

Se llaman de esta forma, por su analogía con los virus biológicos del ser humano. Al igual que estos, los informáticos tienen un ciclo de vida, que va desde que "nacen", hasta que "mueren". Creación, gestación, reproducción, activación, descubrimiento, asimilación, y eliminación. Además, existen varias técnicas que permiten a un virus ocultarse en el sistema y no ser detectado por el antivirus, como la ocultación, protección antivirus, camuflaje y evasión.

Los virus pueden utilizar varias clases de anfitriones, y algunos de los mas comunes son: archivos ejecutables, sectores de arranque, boot (partes de un código que le dice al ordenador donde encontrar las instrucciones que utiliza para iniciarse), archivos de guiones y macros dentro de los documentos.

Existen varios tipos de virus, sin embargo los más destacados son:

- Virus polimorfos, los cuales usan el polimorfismo, que es una técnica que le permite a cada nueva generación de virus asumir una forma diferente que es,

desde el punto de vista funcional, idéntica a la anterior. El objetivo de usar polimorfismo es evitar la detección del virus mediante el uso de una muestra.

- Virus satélite, los cuáles utilizan una técnica especial de infiltración, recurriendo a las variadas prioridades de inicio de los archivos ejecutables. Cuando hay más de un archivo con el mismo nombre, pero con distintas extensiones en el directorio, y el sistema operativo recibe un pedido de ejecución de un programa, procesará primero aquel que tenga la extensión con prioridad de inicio más alta. Los archivos con extensión BAT tienen la prioridad más alta, seguidos por los COM y finalmente los EXE. El virus coloca su cuerpo en el archivo de igual nombre, pero con la extensión de máxima prioridad, porque la intención es causar el mayor daño posible.

2) Gusanos

Es un código maligno cuya principal misión es reenviarse a sí mismo. Son códigos virales que, en principio, no afectan a la información de los sitios que contagian, aunque consumen amplios recursos de los sistemas, congestionándolos y son usados para infectar a otros equipos.

A diferencia de la mayoría de virus, los gusanos se propagan por sí mismos, sin modificar u ocultarse bajo otros programas. No destruyen información de forma directa, pero algunos pueden contener dentro de sí, propiedades características de los virus.

El mayor efecto de los gusanos es su capacidad para saturar, e incluso bloquear por exceso de tráfico los sitios web, aunque estos se encuentren protegidos por un antivirus actualizado.

3) Troyanos

Es un programa potencialmente peligroso que se oculta dentro de otro para evitar ser detectado, e instalarse de forma permanente en nuestro sistema. Este tipo de software no suele realizar acciones destructivas por sí mismo, pero entre muchas otras funciones, tienen la capacidad de capturar datos, generalmente contraseñas e información privada, enviándolos a otro sitio.

Otra de sus funciones es dejar indefenso nuestro sistema, abriendo brechas en la seguridad, de esta forma se puede tomar el control total de forma remota, como si realmente se estuviera trabajando delante de nuestra pantalla.

Otro grupo de software malicioso, es el que se propaga a través del correo electrónico, y estos son:

4) Spam

Es el correo electrónico no solicitado o no deseado, que se envía a múltiples usuarios con el propósito de hacer promociones comerciales o proponer ideas. Generalmente, suelen ser: publicidad, ofertas o enlaces directos a una página web. Estos mensajes

son enviados a cientos de miles de destinatarios cada vez. El correo basura es molesto y roba recursos del sistema. Su distribución causa la pérdida de ancho de banda en la Red, y multiplica el riesgo de infección por virus.

Las personas o empresas que envían este tipo de e-mails, construyen sus listas usando varias fuentes. Normalmente, utilizan programas que recogen direcciones de correo desde usenet, o recopilan las mismas de otras listas de distribución.

Muchos de los mensajes no solicitados nos ofrecen la opción de eliminarnos. La experiencia demuestra que este método es una trampa, y que sólo sirve para verificar que la dirección de correo existe realmente, y se encuentra activa. Por otro lado, si respondemos alguno de estos e-mails, el resultado es idéntico, seremos colocados automáticamente en una nueva lista de distribución, confirmando nuestra dirección, que servirá para incluirnos en bases de datos, las mismas que son vendidas a empresas multinacionales que han incursionado en el e-commerce.

5) Spyware

Los programas espía se instalan en un ordenador sin el conocimiento del usuario, para recopilar información del mismo o del ordenador, enviándola posteriormente al que controla dicha aplicación.

Existen dos categorías de spyware: software de vigilancia y software publicitario. El primero se encarga de monitorizar todo el sistema mediante el uso de transcriptores

de teclado, captura de pantallas y troyanos. Mientras, el segundo, también llamado "Adware", se instala de forma conjunta con otra aplicación o mediante controles activex, para recoger información privada y mostrar anuncios.

Este tipo de programas registran información sobre el usuario, incluyendo, contraseñas, direcciones de correo, historial de navegación por internet, hábitos de compra, configuración de hardware y software, nombre, edad, sexo y otros datos privados.

Al igual que el correo basura, el software publicitario, usa los recursos de nuestro sistema, haciendo que sea este el que pague el costo asociado de su funcionamiento. Además, utiliza el ancho de banda, tanto para enviar la información recopilada, como para descargar los banners publicitarios que nos mostrará.

Los mayores responsables de la difusión de spyware son los populares programas de intercambio de archivos (P2P) disponibles en la actualidad, tipo Kazaa, e-Donkey o e-Mule. De igual forma, mediante programas y códigos maliciosos se pueden realizar varias actividades y técnicas, que podrían estar orientadas al cometimiento de delitos, como:

6) Bulos

Son generalmente bromas y suelen formar parte de una cadena de correo electrónico, y a menudo, también, configuran las llamadas leyendas urbanas. Estos bulos

cibernéticos intentan generar miedo, incertidumbre y dudas en el receptor del mensaje, haciéndole creer que existe un "virus indetectable" en el sistema. Algunos son maliciosos en contenido y logran que el receptor elimine archivos de su sistema.

7) Capturadores de pantalla

Programas de seguimiento que registran imágenes de la actividad en la pantalla. Los capturadores de pantalla, por lo general, almacenan las imágenes y videos registrados para su posterior recuperación, o los transmiten a un proceso o persona remota. Existen algunos usos legales de estos programas, pero a menudo son utilizados por los agresores para realizar un seguimiento escondido del comportamiento del usuario en internet, para realizar otras acciones indeseadas y sin autorización.

8) Carga adicional

Es la función adicional, por ejemplo al robo de información, la eliminación de archivos, formateo de disco, la actualización de la memoria BIOS, que pueden ser incluidos en los gusanos o troyanos. No es necesario que la carga adicional sea dañina.

9) Cifrado

El cuerpo de los virus cifrados está dividido en dos partes básicas, la codificada y el descifrador. La parte ejecutable está codificada, la cual para ser procesada se utiliza

el sector del código llamado "descifrador", que la descodificada antes de su ejecución. El cifrado fue hecho para hacer más dificultoso el análisis y la detección de un virus. En la actualidad no abundan los descifradores polimorfos en uso, pero tampoco escasean.

10) Falsificación de sitios

Aquí lo que se intenta es obtener, de forma fraudulenta, información privada, como claves personales y/o detalles de las tarjetas de crédito. Generalmente esto se logra por medio de un correo electrónico (o alguna comunicación similar) simulando ser emitida por una persona o entidad confiable con un pedido de información aparentemente legítimo.

11) Fraude

Esta técnica es muy similar al Phishing, pero con la diferencia que no busca obtener detalles del usuario, sino que apela a la compasión o a la ambición humana para obtener un rédito económico. Los Scam se caracterizan por pedir al usuario el envío de dinero para cubrir los gastos "administrativos".

12) Registrador de pulsaciones

Es un programa de seguimiento que registra la actividad del teclado y/o ratón. Los registradores de pulsaciones habitualmente almacenan las pulsaciones registradas

para una posterior recuperación, o las transmiten a un proceso o persona remota que esté utilizando este programa. Si bien existen algunos usos legales de los registradores de pulsaciones, a menudo los agresores los utilizan de manera maliciosa para realizar un seguimiento escondido del comportamiento y efectuar acciones no deseadas o no autorizadas, incluyendo el hurto de identidad, aunque no limitándose a este delito.

13) Liberador de virus

Es un archivo ejecutable de baja complejidad. Su única función es instalar virus en la memoria o atacar archivos mediante los mismos. La aplicación del Drooper es normalmente utilizada para propagar diferente tipos de código malicioso que son generados al ejecutar el programa. Estos virus una vez creados, continúan actuando por su cuenta y expandiendo la infección a su manera.

14) Publicidad no solicitada

Este tipo de programa muestra publicidad emergente, específicamente ciertas aplicaciones ejecutables cuyo propósito principal es mostrar contenidos de mercado en una forma o contexto que no es esperado ni solicitado por el usuario. Muchas aplicaciones que contienen publicidad no deseada también realizan funciones de seguimiento, y por lo tanto se les puede categorizar dentro de las tecnologías de rastreo.

15) Conjunto de herramientas de administración

Un Rootkit es una colección de una o mas herramientas diseñadas para controlar de forma encubierta un ordenador y obtiene o mantiene, de manera fraudulenta, un acceso a nivel de administrador, que puede también ejecutarse de forma indetectable. Una vez que el programa tiene acceso, puede utilizarse para controlar el tráfico y las pulsaciones de teclas, crear una puerta trasera hacia el sistema para que sea utilizada por un agresor, editar archivos del registro, atacar otros equipos en la red o modificar herramientas existentes en el sistema para sortear la detección. Los Rootkis reemplazan el comando original del sistema para ejecutar instrucciones maliciosas elegidas por el agresor, y para esconder su presencia en el sistema al modificar los resultados devueltos, eliminando toda evidencia de su operación.

16) Zombie

Los ordenadores Zombies se utilizan a menudo para enviar correo electrónico no deseado o para atacar servidores remotos con una cantidad abrumadora de tráfico (un ataque distribuido de denegación de servicio).

3.4.3. Infraestructura crítica.

Una buena aproximación de lo que se concibe por infraestructura crítica, es el establecido en el Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (Public Law 107-

56), conocido como USA PATRIOT Act o simplemente Patriot Act, que fue firmado por el Presidente George W. Bush el 26 de octubre de 2001, en el que se expresa que "se considera infraestructura crítica a todos los sistemas y recursos, sean estos físicos o virtuales, tan vitales para los Estados Unidos, que la incapacidad o destrucción de tales sistemas y recursos tendrían un impacto debilitante en la seguridad nacional, la seguridad económica nacional, la seguridad y salud pública nacional, o cualquier combinación de las citadas".

Esta definición puede ser aplicada a cualquier país de cualquier región, puesto que lo que le interesa, fundamentalmente, a cada nación es su supervivencia y desarrollo sostenido y sostenible, como un todo, bajo un esquema de seguridad e integridad. De ahí la importancia de proporcionar protección a los sistemas y recursos que conforman la infraestructura crítica de una nación, sin embargo, para llegar a esta protección razonablemente aceptable es necesario adaptarse a un ciclo de vida de la tecnología, que implica adaptación a cambios permanentes, que en el peor de los casos debe contener las siguientes fases:

a) Análisis de la infraestructura y valoración: Es necesario considerarlo desde la óptica de la defensa interna y de la defensa externa, para lo cual se deben identificar los recursos críticos y sistemas vitales, determinándose sus características y configuraciones, establecer las relaciones entre los diferentes sectores de la infraestructura, valorar sus vulnerabilidades, cuantificar la relación entre los planes militares y los de los organismos que los administran, y valorar el impacto operacional y social en caso de pérdida parcial o total. En esta fase un aspecto que

hay que tomar muy en cuenta, es la priorización de la infraestructura crítica, la cual como consecuencia lógica establecerá el nivel de atención frente a incidentes simultáneos.

b) Remediación: En la que establecen medidas preventivas consideradas para mejorar la fiabilidad, disponibilidad, la supervivencia, etc., de recursos e infraestructura crítica, por ejemplo actualización de conocimientos, entrenamiento y educación; los cambios en las reglas del negocio o procedimientos de operación, diseño de mejoras, y cambio en los niveles de seguridad del sistema como la diversidad física, decepción, redundancia y respaldos.

c) Indicaciones y advertencias: Realización de indicaciones a nivel táctico a través de la supervisión y el monitoreo, indicaciones estratégicas a través del apoyo de la comunidad de inteligencia, y la coordinación con los organismos que administran los recursos y las capacidades nacionales.

d) Mitigación: Se constituyen en las reacciones pre-planeadas y coordinadas de los operadores, frente a una advertencia de la infraestructura o incidente, con la finalidad de reducir o minimizar los impactos; esta fase se complementa al apoyo de la emergencia, investigación y manejo de crisis; y ayuda al restablecimiento del sistema.

e) Respuesta: Corresponde a un tercer actor, es decir, fuera del grupo de los propietarios y fuera del grupo de los operadores de la infraestructura física, afectada.

f) Restablecimiento: En esta fase el propietario y/u operador son responsables de la restauración y restablecimiento del servicio que proporciona los recursos e infraestructura crítica.

Como se puede observar en las fases anteriormente citadas, se debe poner especial énfasis en lo fundamental de cada una de ellas que constituyen la coordinación que debe existir entre los tres actores principales: propietario, operador y entidades de manejo de crisis.

En forma general, y considerando la dependencia, vulnerabilidad y amenaza en el ámbito socio-económico de una nación, se han establecido varios sectores en los que están involucradas las infraestructuras críticas:

- Información y comunicaciones.
- Educación
- Salud y medio ambiente.
- Banca y finanzas
- Transportación
- Servicios básicos
- Energía
- Gobierno

Hay que considerar que de acuerdo a la tecnología implementada en cada uno de estos sectores, la relación de dependencia con las tecnologías de la información es

la infraestructura de la información, generalmente basada en sistemas informáticos y de comunicaciones.

3.4.4. Delitos informáticos.

Internacionalmente se considera que no existe una definición propia del delito informático, sin embargo, muchos han sido los esfuerzos de expertos que se han ocupado del tema, y aún cuando no existe una definición con carácter universal, se han formulado conceptos funcionales atendiendo a realidades nacionales concretas.

Pero en sí, a qué se lo debe considerar delito?. Según el Doctor. Eugenio Cuello, en su libro de derecho penal, para que exista delito se debe contar con los siguientes elementos:

a. El delito es un acto humano, es una acción (acción u omisión)

b. Dicho acto humano ha de ser antijurídico, debe lesionar o poner en peligro un interés jurídicamente protegido.

c. Debe corresponder a un tipo legal (figura de delito), definido por la Ley, ha de ser un acto típico.

d. El acto ha de ser culpable, imputable a dolo (intención) o a culpa (negligencia), y una acción es imputable cuando puede ponerse a cargo de una determinada persona.

e. La ejecución u omisión del acto debe estar sancionada por una pena.

En consecuencia, un delito es: una acción antijurídica realizada por un ser humano, tipificado, culpable y sancionado por una pena, todos estos elementos deben estar tipificados en la normatividad legal.

De lo expuesto y considerando otros aspectos como de la ética y del permiso autorizado. Se puede concluir quee delito informático es "la realización de una acción, que reúne los elementos constitutivos de un delito, no ética y/o no autorizada, para lo cual se ha utilizado un elemento informático o telemático, y que está relacionado con el proceso automático de datos y/o transmisión de datos".

De igual forma que en su conceptualización, no existe una clasificación consensuada a nivel mundial, sin embargo la ONU, ha reconocido la siguiente:

DELITO	CARACTERISTICAS
Fraudes cometidos mediante manipulación de computadoras	
Manipulación de los datos de entrada	Este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.
La manipulación de programas	Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

Manipulación de los datos de salida	Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.
Fraude efectuado por manipulación informática	Aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.
Falsificaciones informáticas	
Como objeto	Cuando se alteran datos de los documentos almacenados en forma computarizada.
Como instrumentos	Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.
Daños o modificaciones de programas o datos computarizados.	
Sabotaje informático	Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:
Virus	Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.
Gusanos	Se fabrica de forma análoga al virus para infiltrarlo en programas legítimos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

Bomba lógica o cronológica	Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.
Acceso no autorizado a servicios y sistemas informáticos	Por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.
Piratas informáticos o hackers	El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.
Reproducción no autorizada de programas informáticos de protección legal	Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas.

Como se puede observar, con el continuo desarrollo de las tecnologías de la información, cada vez se abren más puertas a nuevas posibilidades de delincuencia, antes impensables.

La manipulación fraudulenta de los ordenadores con ánimo de lucro, la destrucción de programas o datos y el acceso y la utilización indebida de la información que puede afectar la esfera de la privacidad, integridad y disponibilidad, son algunos de

los procedimientos relacionados con el procesamiento electrónico de datos mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños materiales o morales. Pero no sólo la cuantía de los perjuicios así ocasionados es a menudo infinitamente superior a la que es usual en la delincuencia tradicional, sino que también son mucho más elevadas las posibilidades de que no lleguen a descubrirse. Se trata de una delincuencia de especialistas capaces muchas veces de borrar toda huella de los hechos.

3.4.5. Propuesta específica para el sector carrocero de la provincia del Tungurahua

Se espera que todas las funciones del negocio agreguen valor a una compañía y la auditoría informática no debe ser la excepción.

Las empresas asociadas a la cámara nacional de fabricantes de carrocerías (CANFAC), se enfrentan a un cambio de época por diversos factores como:

- La iniciativa del gobierno nacional de promover la renovación del parque automotor de transporte público, propicia una expansión del nicho de mercado que debe ser cubierto por la producción nacional.
- Para corregir los desequilibrios en la balanza comercial se están implementando políticas económicas de restricción de las importaciones.
- Para disminuir los índices de desempleo el gobierno ha establecido políticas de legalización de los contratos laborales.

- Los fabricantes de carrocerías deben obtener la calificación del consejo nacional de calidad (CONCAL).
- Para satisfacer el incremento de la demanda y obtener los niveles de calidad exigidos se deben emprender dentro de los talleres actuales de construcción de carrocerías metálicas una gran transformación que les convierta en medianas o grandes industrias.
- La transformación debe efectuarse con una implementación ordenada de la tecnología.
- Se debe gestionar los riesgos propios ocasionados por la innovación tecnológica desde el inicio para disminuir los impactos y convertir los riesgos en oportunidades.

Con estos parámetros se debe implementar como parte de la estructura de la CANFAC, una compañía consultora, cuyos accionistas serías los mismos miembros de la CANFAC, esta compañía deberá prestar servicios a sus asociados, sus actividades principales que se incluirán en el objeto social serán:

- Asumir completamente la función de auditoría de sistemas informáticos de los miembros de la CANFAC.
- Asesorar a los miembros de la CANFAC, en los procesos de adquisición e implementación de los recursos informáticos tanto hardware como software.
- Evaluar periódicamente la eficiencia y la eficacia de los recursos tecnológicos.
- Administrar permanentemente la gestión del cambio tecnológico.

- Promover y ejecutar programas de capacitación a los usuarios de la tecnología para disminuir los riesgos relacionados con el personal.
- Revisar la función de la tecnología informática para evaluar el retorno sobre la inversión.
- Analizar las políticas y procedimientos actuales para proteger la integridad y la confidencialidad de la información suministrada por los sistemas informáticos.
- Evaluar permanentemente el funcionamiento de las redes.
- Mantener planes emergentes para casos de fallas en la tecnología, como por ejemplo sistemas de reemplazo temporal.
- Suministrar los servicios de Internet.
- Detectar a tiempo los riesgos de las redes internas y externas.
- Lograr la aplicación del conocimiento tecnológico existente en el mejoramiento continuo de los procesos estratégicos.
- Crear una plataforma competitiva estimulando la generación de servicios de apoyo necesarios para lograr el crecimiento económico del sector.
- Implementar un sistema de monitoreo continuo mediante indicadores que permitan evaluar el rendimiento técnico y económico de la tecnología.

3.5. Alcance de la propuesta.

La auditoría informática actuará dentro de parámetros establecidos, es decir que se desarrollará en un entorno y límites determinados, y es complementada con los objetivos de los clientes en este caso los miembros de la CANFAC. Estos límites

deben estar claramente estipulados en el informe final, para que quede claro hasta dónde puede llegar el análisis, evaluación y control de la auditoría y no solamente eso sino que hay aspectos dentro de las materias consideradas fronterizas que pueden ser omitidas. Cuando estos puntos no son bien definidos, puede implicar una serie de conflictos y restringir el logro de los resultados esperados.

Este trabajo es una alerta para que los fabricantes empiecen a pensar en establecer un plan de competitividad en torno a cubrir con calidad la demanda interna y proyectarse con sus productos a otros mercados como América Latina en su conjunto.

El objetivo general consiste en analizar la relación que presenta la exposición al riesgo por falta de un plan de contingencias, con la disminución de los beneficios tangibles de los proyectos de desarrollo informático en el sector carrocero de la provincia del Tungurahua.

No existe la intención de buscar soluciones totales a los problemas actuales de los fabricantes de carrocerías en el campo tecnológico, sino más bien promover el desarrollo tecnológico en forma ordenada tomando en cuenta los riesgos que han tenido proyectos similares para disminuir su impacto y obtener los mejores beneficios de la tecnología, es decir mejorar la eficiencia, la eficacia y disminuir los tiempos de entrega.

Claro está, que para hacer posible este entorno dinámico de gestión de riesgos es imprescindible desde ahora pensar en mejorar el acceso de las tecnologías a precios competitivos y con análisis integral del valor añadido.

En definitiva la propuesta está encaminada a exponer las políticas y procedimientos necesarios que debe adoptar el sector carrocero de la provincia del Tungurahua para que en el proceso de transición de talleres artesanales a empresas tecnológicas disminuyan significativamente el impacto de los riesgos.

3.6. Factibilidad de la propuesta.

Las empresas que permitan la aplicación de la propuesta obtendrán los siguientes beneficios:

3.6.1. Fortalecimiento de la gestión administrativa y financiera

- Establecimiento de procesos estructurados y automatizados, fundamentales para la aplicación eficaz de la gestión de riesgos tecnológicos.
- Establecimiento de una base que sirva para mantener un control interno más coherente y establecer un marco de gestión de riesgos sobre la base de las funciones de los usuarios, los procedimientos automatizados de aprobación y la gestión del flujo de trabajo.
- Capacidad de cumplir con las certificaciones de calidad.
- Mayor supervisión y control presupuestarios.

- Mantener vigentes planes de contingencia informáticos.

3.6.2. Perfeccionamiento del personal

El proyecto constituirá una excelente plataforma o vehículo para capacitar y profesionalizar al personal, hacer un uso más disciplinado de los datos y utilizar tareas analíticas más provechosas gracias a una mejor información. De este modo, la organización, incluidos el departamento de gestión y el personal, estará preparada procesar los datos en función de la gestión de riesgos tecnológicos.

3.6.3. Adquisiciones

- Actualmente, en esta esfera se acusa muy particularmente la falta de apoyo estructurado en materia de T.I.. Con un apoyo técnico se logrará obtener una razonable vida útil de la tecnología.
- Con la aprobación y vigencia del nuevo marco constitucional se universalizo el acceso a las tecnologías de la informacion y comunicación como un derecho del buen vivir.

3.6.4. Gestión de riesgos

La gestión de riesgos es un factor crucial en este tipo de enfoque. Se llevará a cabo la identificación de los principales riesgos y las alternativas que permitan disminuir el impacto en caso de ocurrir el evento. Los riesgos serán cuantificados y evaluados,

priorizándolos, en función de la probabilidad de que ocurran y de sus posibles repercusiones.

A nivel mundial por cada dólar invertido en prevención de riesgos se ahorra siete de gastos operativos relacionados con los siniestros, estos gastos son el mantenimiento correctivo, cambios en sistemas, programas de reingeniería, etc.

Es factible la aplicación de la propuesta porque ya existe una organización que debería tomar la administración de la misma como la CANFAC, esta entidad debe suministrar a sus miembros servicios que agreguen valor y que mejor que contribuir a obtener los mejores beneficios de la tecnología, mediante el asesoramiento eficiente en esta rama.

El mantener vigente un plan de contingencia disminuirá, significativamente el impacto de los riesgos en caso de ocurrencia y permitirá adoptar medidas emergentes en caso necesario.

Los recursos para la constitución de la consultora deberán capitalizarse a través de CANFAC, el retorno de la inversión será muy rápido porque además de contribuir en la transformación tecnológica de sus asociados se puede prestar servicios a otros sectores empresariales.

La gestión de riesgos de los negocios en un entorno empresarial tan complejo como el que nos movemos va más allá de ser una mera necesidad para el desarrollo de las

empresas: se ha transformado en una prioridad para la alta dirección, ligada a la propia supervivencia de las compañías. Los empresarios, los diferentes grupos de interés y hasta los organismos reguladores apuestan ahora, más que nunca, por un fortalecimiento de los sistemas de gestión y control de riesgos que permita a las empresas generar y preservar valor y, también, mantener un desarrollo sostenible en el tiempo.

De acuerdo a la metodología sugerida, la gestión de riesgos del negocio requiere un enfoque global y sistemático para ayudar a todas las organizaciones a identificar, cuantificar, priorizar y monitorearlos riesgos que asume, ayudándole a alcanzar sus objetivos, mitigando sorpresas e incertidumbres. Los objetivos sobre los que la identificación, la evaluación y la gestión de los riesgos debe actuar son los siguientes:

- El objetivo estratégico, al más alto nivel de la compañía.
- La eficacia y eficiencia de las operaciones de la firma.
- La fiabilidad de la información transmitida a terceros.
- El cumplimiento regulatorio de las leyes y normativas aplicables.

Mediante la implantación de este enfoque basado en la gestión integral de riesgos, las compañías deben obtener mejoras significativas, entre otros, en el desarrollo de los siguientes aspectos:

- Un mayor alineamiento entre la estrategia de la empresa y la gestión global de los riesgos del negocio.
- Una mejor y más rápida respuesta a los mercados y a los grupos de interés.
- Una gestión más eficiente del riesgo respecto al crecimiento de la compañía y a los retornos esperados derivados de los mismos.
- Una mejor previsión del posible impacto de los riesgos de la compañía.
- Una mejora en la identificación de oportunidades por parte de la Dirección.
- Una utilización más eficiente de los recursos destinados a la gestión de riesgos.

CAPITULO IV

CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

Se ha argumentado como el enfoque actual de análisis y gestión de riesgos de seguridad informática es inadecuado dado el constante avance tecnológico que lleva al surgimiento de amenazas emergentes. Se ha propuesto entonces una metodología que considere el diseño de controles adaptativos. Consideramos que este enfoque lleva a todo un cambio de paradigma en la gestión de la seguridad informática.

A medida que las organizaciones adquieren mayor tamaño, y una mayor sensibilidad por el control interno, en la búsqueda de la eficiencia en sus procesos, la necesidad de formalizar la función de auditoría informática se hace más patente.

La tradicional confianza que los auditores han tenido en las tecnologías de la información se les está convirtiendo en un alto riesgo que ya no pueden dejar de administrar con cautela.

La gran perspectiva que tiene la utilización del internet como medio para efectuar negocios electrónicos, constituye una potencial amenaza para la seguridad informática.

Los avances en las tecnologías de la información han reducido de manera sustancial la propensión a error en el proceso rutinario de las transacciones de los negocios.
El desconocimiento de los usos de la tecnología y la escasa capacitación profesional dificultan el desarrollo empresarias.

El significativo incremento de la diversidad y complejidad de los riesgos empresariales hace necesario adoptar un enfoque formal y coordinado para su identificación, control y gestión. Se trata de dar una respuesta global que integre la gestión del riesgo, el control interno y el buen gobierno de la tecnología.

La gestión de riesgos requiere un enfoque global y sistemático, encaminado a conseguir los objetivos estratégicos, la máxima eficiencia y eficacia, una información fiable y el cumplimiento de las leyes y normativas aplicables

5.2. Recomendaciones

A la hora de formalizar la función de auditoría informática, las organizaciones deben tener muy presentes los objetivos que se plantean con ella, sus necesidades en cuanto a recursos y las diferentes estrategias que se pueden adoptar para ello, sin olvidar la posibilidad de externalizar total o parcialmente la función.

Los auditores deben considerar centrarse en las estrategias de e-commerce para sus clientes, el riesgo de e-commerce que tiene que ser administrado para lograr el

cumplimiento de los objetivos de la auditoria y agregar valor a los clientes. Para incursionar en este campo su capacitación debe ser sólida en las tecnologías de la información y la comunicación.

El auditor necesita entender los controles internos dependientes de las tecnologías de la información.

Se debe impulsare el intercambio de información entre administraciones, a través de la interconexión telemática

Debido a que los riesgos empresariales se han incrementado muy significativamente, variando a su vez la diversidad y complejidad de su naturaleza (macroeconómicos, relacionados con la tecnología, operacionales, regulatorios, reputacionales) Parece cada vez más clara la necesidad de adoptar un enfoque formal y coordinado para su identificación, control y gestión, lo que requiere una combinación de competencias profesionales y habilidades estratégicas.

BIBLIOGRAFÍA.

Adrián Slywotzky. El arte de hacer rentable una empresa, Bogotá, Editorial Norma, 2002.

Antonio Francés. Estrategia y planes para la empresa con el cuadro de mando integral, México, Perentice Hall, 2006.

Antonio Hidalgo, Gonzalo León y Julián Pavón: La gestión de la innovación y la tecnología en las organizaciones, Madrid, Editorial Pirámide, 2002.

Asociación Española de Contabilidad y Administración de Empresas. La toma de decisiones en la empresa, Madrid, Ortega Ediciones, 2002.

Asociación internacional de parques científicos, www.ace.es.

C. Kaufman, R. Perlman y M. Speciner. *Network Security Private Communication in a Public World*. New York, Perentice Hall, 1995.

Carlos Muñoz. Auditoria en sistemas computacionales, México, Editorial Pearson, 2002.

Centro de desarrollo tecnológico industrial, www.cdti.es.

Christophe Perruchet, Marc Priel. Estimación de la incertidumbre, Madrid, AENOR, 2000.

David R. Anderson, Dennis J Sweeny, Thomas A. Williams. Métodos cuantitativos para los negocios, Thompson, 1999

Eliyahu M. Goldratt. Necesario pero no suficiente, Diaz de Santos, 2000.

Fundación COTEC. El sistema español de innovación, Madrid Gráficas Arias Montano S.A., 2004.

Institute for development policy and management, http://www.egov4dev.org/home.htm

Ignacio Vélez. Decisiones empresariales bajo riesgo e incertidumbre Bogotá, Editorial Norma, 2003.

James O'brien y George Marakas, Sistemas de información gerencial, México, Mcgraw Hill, 2006.

James W. Cortada. Management del nuevo siglo, Perentice Hall, 2001.

José Molero. Innovación tecnológica y competitividad en Europa, Madrid, Editorial Síntesis, 2001.

Madri+d, www.madridmasd.org

Nassim Nicholas Taleb. El cisne negro, Barcelona, Ediciones Paidós Ibérica, 2008.

Nueva economía, www.n-economia.com

Robert J. Shiller. El nuevo orden financiero. El riesgo del siglo xxi, Madrid, Turner Publicaciones, 2003.

Robert Johnson y Ronald Melicher. Administración financiera, México, Editorial Cegsa, 2007.

Rodrigo Estupiñán. Administración o gestión de riesgos E.R.M. y la auditoría interna, Bogotá, Ecoe Ediciones, 2006.

Thomas L. Wheelen y J. David Hunger. Administración estratégica y política de negocios, Perentice Hall,2007.

Victoria Erosa y Pilar Arroyo. Administración de la tecnología, México D.F., Editorial Limusa, 2007.

ON LINE

http://www.cisco.com

http://www.ciscopress.com/book.cfm?series=3&book=112

http://cultdeadcow.com

http://diarioit.comftp://ftp.cdrom.comftp://ftp.coast.net

http://hertz.njit.edu/%7ebxg3442/temp.html

http://www.alpworld.com/infinity/voidneo.html

http://www.danworld.com/nettools.html

http://www.eskimo.com/~nwps/index.html

http://www.geocities.com/siliconvalley/park/2613/links.html

http://www.ilf.net/Toast/

http://www.islandnet.com/~cliffmcc

http://www.simtel.net/simtel.net

http://www.supernet.net/cwsapps/cwsa.htm.

http://www.trytel.com/hack/

http://www.tucows.com

http://www.windows95.com/apps/

http://www2.southwind.net/%7emiker/hack.html

www.riesgofinanciero.com

www.riesgoycontrol.net.

GLOSARIO

A

Administrador

Persona que se encarga de todas las tareas de mantenimiento de un sistema informático.

Algoritmo

Procedimiento o conjunto de procedimientos que describen una asociación de datos lógicos destinados a la resolución de un problema. Los algoritmos permiten automatizar tareas.

Aplicación

Aunque se suele utilizar indistintamente como sinónimo genérico de 'programa' es necesario subrayar que se trata de un tipo de programa específicamente dedicado al proceso de una función concreta dentro de la empresa.

App add/appadd

Lanza una aplicación basada en texto en un puerto tcp. Esto permite que tengas el control de una aplicación de texto o MS-DOS desde una sesión de telnet (por ejemplo, command.com)

Archivo de datos

Cualquier archivo creado dentro de una aplicación: por ejemplo, un documento creado por un procesador de textos, una hoja de cálculo, una base de datos,etc.

Archivo de programa

Archivo ejecutable que inicia una aplicación o programa. Los archivos de programa tienen las extensiones EXE, PIF, COM o BAT.

Archivo de revisión de auditoría

Involucra módulos incrustados en una aplicación que monitorea continuamente el sistema de transacciones. Recolecta la información en archivos especiales que puede examinar el auditor

Archivos log

Archivo de texto que almacena generalmente datos sobre procesos determinados. Para entendernos, es como el "diario" de algunos programas donde se graban todas las operaciones que realizan, para posteriormente abrirlos y ver qué es lo que ha sucedido en cada momento.

Auditoría

Examen de las operaciones de una empresa por especialistas ajenos a ella y con objetivos de evaluar la situación de la misma.

Autenticación

La autenticación se refiere al proceso de establecer la identidad digital de una entidad a otra entidad. Comúnmente una entidad es un cliente (un usuario, un ordenador cliente, etc.) y la otra entidad es un servidor (computadora).

Autorización

La mayor parte del tiempo la concesión de un privilegio constituye la capacidad de utilizar un determinado tipo de servicio. Ejemplos de los tipos de servicio incluyen, pero no se limitan a: la dirección IP de filtrado, la dirección destino, la ruta de sesión, QoS / servicios diferenciales, control de ancho de banda / gestión del tráfico, etc.

B

Bases de Datos

Colección de datos organizada de tal modo que el ordenador pueda acceder rápidamente a ella. Una base de datos relacional es aquella en la que las conexiones entre los distintos elementos que forman la base de datos están almacenadas explícitamente con el fin de ayudar al uso y el acceso a éstos.

Batch

Es un programa que se ejecuta de forma independiente sin actuación del usuario.

Benchmarking

Técnica de auditoría informática en la cual se realiza el proceso contínuo de medir productos, servicios y prácticas contra los competidores o aquellas compañías reconocidas como líderes en la industria

Bitácoras

Es como el "diario" de algunos programas donde se graban todas las operaciones que realizan, para posteriormente abrirlos y ver qué es lo que ha sucedido en cada momento.

Boxes

Circuitos preparados para realizar phreaking. Destacan:

Bluebox => Para llamar gratis
Redbox => Emula la introducción de monedas en teléfonos públicos
Blackbox => El que llame a un teléfono con este dispositivo no pagará la llamada.

Broadcast

En castellano difusión, es un modo de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.

Browser

Un navegador web (del inglés, navigator o web browser) es una aplicación software que permite al usuario recuperar y visualizar documentos de hipertexto, comúnmente descritos en HTML, desde servidores web de todo el mundo a través de Internet.

Esta red de documentos es denominada World Wide Web (WWW).

Cualquier navegador actual permite mostrar o ejecutar gráficos, secuencias de vídeo, sonido, animaciones y programas diversos además del texto y los hipervínculos o enlaces.

Bug

Un error en un programa o en un equipo. Se habla de bug si es un error de diseño, no cuando la falla es provocada por otra cosa.

C

C.I.A

Certified Internal Auditor Certificación de Auditores Internos

C.I.M.S

Certified Information Security Manager Certificación para la Administración de la Seguridad de la Información

C.I.S.A

Certified Information Security Auditor Certificación en Auditor en Sistemas de Información

CAAT

Técnicas de Auditoría Asistidas por Computadora, son herramientas (software) que ayudan al auditor a facilitar sus tareas.

CANFAC

Cámara nacional de fabricantes de carrocerías.

CDP

CDP (Cisco Discovery Protocol, 'protocolo de descubrimiento de Cisco')

Es un protocolo de red propietario de nivel 2, desarrollado por Cisco Systems y usado en la mayoría de sus equipos. Es utilizado para compartir información sobre otros equipos Cisco directamente conectados, tal como la versión del sistema operativo y la dirección IP.

Cliente

Cliente o 'programa cliente' es aquel programa que permite conectarse a un determinado sistema, servicio o red.

Cliente-Servidor

Se denomina así al binomio consistente en un programa cliente que consigue datos de otro llamado servidor sin tener que estar obligatoriamente ubicados en el mismo ordenador. Esta técnica de consulta 'remota' se utiliza frecuentemente en redes como 'Internet'.

Confidencialidad

Se refiere a que la información solo puede ser conocida por individuos autorizados.

Contabilidad

Contabilidad se refiere al seguimiento del consumo de recursos de la red por los usuarios. Esta información puede ser utilizada para la gestión, planificación, facturación, u otros fines. En tiempo real de contabilidad se refiere a la información contable que se entrega simultáneamente con el consumo de los recursos. Lote de contabilidad se refiere a la información contable que se guarda hasta que sea entregado en un momento posterior. Típica información que se recoge en la contabilidad es la identidad del usuario, la naturaleza del servicio prestado, cuando el servicio se inició, y cuando terminó.

Cortafuegos (Firewall)

Computadora que registra todos los paquetes de información que entran en una compañía para, una vez verificados, derivarlos a otra que tiene conexión interna y no recibe archivos que no provengan de aquella.

Es como un embudo que mira si la información que desea entrar a un servidor tiene permiso para ello o no. Los hackers deben contar con gran creatividad para entrar ya sea buscando un bug (error de diseño) o mediante algún programa que le permita encontrar alguna clave válida.

Costo

Desembolso en efectivo o en especie por algún beneficio.

Costo estándar

Son los que resultan de la suma de precios obtenida sobre las especificaciones de un producto, atendiendo a las unidades básicas anticipadas para el material, trabajo y gastos que entran en su producto.

Costos de inversión (largo plazo)

Esto es equipo de cómputo, hardware, software.

Costos de operaciones

Estos gastos los origina la administración del Órgano Legislativo, así como inventarios, mano de obra, etc.

Costos de oportunidad

Son los costos que se derivan de hacer una cosa en lugar de otra.

Costos estimados

Son los cálculos anticipados de los gastos que predominarán en el futuro (mano de obra, material, etc), dentro de un periodo dado, con la intención de pronosticar un costo total.

Costos fijos:

Son los costos necesarios al inicio de las operaciones de cualquier empresa y que se mantienen constantes en los diferentes niveles de producción a corto y mediano plazo, como son los salarios de los ejecutivos, los alquileres de locales, los intereses, etc.

Costos indirectos de producción:

Son los formados por aquellos gastos que no pueden ser rápidamente asociados con el producto (técnicos, papelería, renta, herramientas)

Cracking

Modificar un programa para obtener beneficios. Normalmente se basa en quitar pantallas introductorias, protecciones o, como en unas modificaciones de cierto programa de comunicaciones, conseguir nuevos passwords de acceso a sistemas.

Criptografía

Ciencia dedicada al estudio de técnicas capaces de conferir seguridad a los datos.

El cifrado es fundamental a la hora de enviar datos a través de las redes de telecomunicaciones con el fin de conservar su privacidad.

Cyberpunk

Corriente literaria dentro de la ciencia-ficción que, entre otras cosas, se destaca por incorporar a sus argumentos el uso de la tecnología de las redes de computadoras.

D

Datos

Término general para la información procesada por un ordenador.

Dial-up

Línea de datos que permite a un usuario acceder por módem a una red o a una computadora.

Dirección IP

Dirección numérica obligatoria de un dominio 'Internet'. Está compuesta por cuatro cifras (de 0 a 255) decimales separadas por puntos. Por ejemplo: 192.168.1.250.

DNS

El Domain Name System (DNS) es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

DTP

DTP (Dynamic Trunk Protocol) es un protocolo que opera entre conmutadores, el cual automatiza la configuración de trunking (etiquetado de tramas de diferentes VLAN's con ISL o 802.1Q) en enlaces Ethernet.

E

Echo (computación)

En términos de computación, echo tiene varias acepciones. Por un lado es un servicio de red que repite aquel comando que se le envía. Es útil para hacer comprobaciones sobre el estado de la conectividad de una red. Por otro lado, Echo es un comando para la impresión de un texto en pantalla. Es utilizado en las terminales de los sistemas operativos como Unix, GNU/Linux, o MS-DOS; dentro de pequeños programas llamados scripts; y en ciertos lenguajes de programación tales como PHP.

F

Facke

Todas aquellas versiones de programas que han sido manipuladas de tal manera que figuran como versiones superiores a la original sin serlo.

FTP

FTP (File Transfer Protocol) es un protocolo de transferencia de archivos entre sistemas conectados a una red TCP basado en la arquitectura cliente-servidor, de manera que desde un equipo cliente nos podemos conectar a un servidor para descargar archivos desde él o para enviarle nuestros propios archivos independientemente del sistema operativo utilizado en cada equipo.

G

GBIC

Un convertidor de interfaz gigabit (GBIC) es un estándar para transceptores, comúnmente usado con Gigabit Ethernet y Fibre Channel. Al ofrecer un estándar, intercambiables en caliente interfaz eléctrica, un puerto Ethernet Gigabit puede apoyar una amplia gama de medios físicos, de cobre a largo de onda de un solo modo de fibra óptica, con longitudes de cientos de kilómetros.

Group

Grupos de personas que unen sus fuerzas para 'suplier' juegos o programas.

Guest

Cuenta pública de un sistema, para que la use alguien que no tiene cuenta propia.

Gusano
Programa que se reproduce, sin infectar a otros en el intento.

H

Hardware

Conjunto de dispositivos de los que consiste un sistema. Comprende componentes tales como el teclado, el Mouse, las unidades de disco y el monitor.

Hacking

Acto de hackear. Básicamente consiste en entrar de forma ilegal en un sistema, para obtener información. No conlleva la destrucción de datos ni la instalación de virus, pero pueden instalarse troyanos que proporcionen passwords nuevos. También consiste en llevar una vida acorde con el hackmode.

Hackmode

Modo de actuar del hacker. No tiene por qué estar relacionado con las computadoras, es más bien un modo de interpretar la vida. Consiste en:
No pagar lo que no es estrictamente necesario o pagar de forma "poco corriente".
Ser un poco "paranoico".
Actuar acorde con costumbres rigurosamente calculadas.

Handle

Seudónimo usado en vez del nombre verdadero.

Hostname

Hostname es el programa que se utiliza para mostrar o establecer el nombre actual del sistema (nombre de equipo). Muchos de los programas de trabajo en red usan este nombre para identificar a la máquina. El NIS/YP también utiliza el nombre de

dominio. Cuando se invoca sin argumentos, el programa muestra los nombres actuales

HTTP

HTTP son las siglas de "Hyper Text Transfer Protocol" el cual es el principal protocolo tecnológico de la red que permite enlazar y navegar por Internet. Si no tuviéramos http, no podríamos acceder e interactuar en la red de redes como lo hacemos actualmente. Las cosas serían bastante más duras y confusas para todos.

I

I.I.A

Institute of Internal Auditors

I.S.A.C.A:

Information Systems Audit and Control Association Asociación de Auditoría y Control de Sistemas de Información

ICMP

El Protocolo de Mensajes de Control de Internet o ICMP (por sus siglas de Internet Control Message Protocol) es el subprotocolo de control y notificación de errores del Protocolo de Internet (IP). Como tal, se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado

ICMP difiere del propósito de TCP y UDP ya que generalmente no se utiliza directamente por las aplicaciones de usuario en la red. La única excepción es la herramienta ping y traceroute, que envían mensajes de petición Echo ICMP para determinar si un host está disponible, el tiempo que le toma a los paquetes en ir y regresar a ese host y cantidad de hosts por los que pasa.

IDS

Un sistema de detección de intrusos (o IDS de sus siglas en inglés Intrusion Detection System) es un programa usado para detectar accesos desautorizados a un computador o a una red. Estos accesos pueden ser ataques de habilidosos hackers, o de Script Kiddies que usan herramientas automáticas.

El IDS suele tener sensores virtuales (por ejemplo, un sniffer de red) con los que el núcleo del IDS puede obtener datos externos (generalmente sobre el tráfico de red). El IDS detecta, gracias a dichos sensores, anomalías que pueden ser indicio de la presencia de ataques o falsas alarmas

IEEE

IEE corresponde a las siglas de The Institute of Electrical and Electronics Engineers, el instituto de ingenieros eléctricos y electrónicos, una asociación técnico-profesional mundial dedicada a la estandarización, entre otras cosas. Es la mayor asociación internacional sin fines de lucro formada por profesionales de las nuevas tecnologías, como ingenieros eléctricos, ingenieros en electrónica, científicos de la computación, ingenieros en informática e ingenieros en telecomunicación.

IGMP

El protocolo de red IGMP se utiliza para intercambiar información acerca del estado de pertenencia entre enrutadores IP que admiten la multidifusión y miembros de grupos de multidifusión. Los hosts miembros individuales informan acerca de la pertenencia de hosts al grupo de multidifusión y los enrutadores de multidifusión sondean periódicamente el estado de la pertenencia.

Integridad

La habilidad de determinar que la información recibida es la misma que la información enviada.

Internet

Interconexión de redes informáticas que permite a las computadoras conectadas comunicarse directamente.

IOS

IOS son las siglas de (Internetwork Operating System, Sistema Operativo de Interconexión de Redes) creado por Cisco Systems para programar y mantener equipos de interconexión de redes informáticas como switches (conmutadores) y routers (enrutadores).
IP Internet Protocol

Una dirección IP es un número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo (habitualmente una computadora) dentro de una red que

utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red o nivel 3 del modelo de referencia OSI. Dicho número no se ha de confundir con la dirección MAC que es un número hexadecimal fijo que es asignado a la tarjeta o dispositivo de red por el fabricante, mientras que la dirección IP se puede cambiar.

Es habitual que un usuario que se conecta desde su hogar a Internet utilice una dirección IP. Esta dirección puede cambiar al reconectar; y a esta forma de asignación de dirección IP se denomina una dirección IP dinámica (normalmente se abrevia como IP dinámica).

Los sitios de Internet que por su naturaleza necesitan estar permanentemente conectados, generalmente tienen una dirección IP fija (se aplica la misma reducción por IP fija o IP estática), es decir, no cambia con el tiempo. Los servidores de correo, DNS, FTP públicos, y servidores de páginas web necesariamente deben contar con una dirección IP fija o estática, ya que de esta forma se permite su localización en la red.

A través de Internet, los ordenadores se conectan entre sí mediante sus respectivas direcciones IP. Sin embargo, a los seres humanos nos es más cómodo utilizar otra notación más fácil de recordar y utilizar, como los nombres de dominio; la traducción entre unos y otros se resuelve mediante los servidores de nombres de dominio DNS. Existe un protocolo para asignar direcciones IP dinámicas llamado DHCP (Dynamic Host Configuration Protocol).

IPFILTER

IPFilter (comúnmente denominado CIP) es un paquete de software que pueden utilizarse para proporcionar traducción de direcciones de red (NAT) o firewall. Puede ser utilizado como un módulo del kernel cargables (LKM) o incorporados en el Unix núcleo; uso como carga de módulos del núcleo cuando sea posible, es altamente recomendable. Scripts se prestan a instalar el parche y los archivos del sistema, según sea necesario. El autor y mantenedor es Darren Reed.

IPS

Un sistema de prevención de intrusiones es un dispositivo de seguridad que vigila la red y / o actividades del sistema de maliciosos o no deseados de comportamiento y puede reaccionar en tiempo real, para bloquear o impedir esas actividades.

IPSec

IPsec (abreviatura de Internet Protocol Security) es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP)

autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.

ISO

(Organización Internacional para la Normalización) Organización de carácter voluntario fundada en 1946 que es responsable de la creación de estándares internacionales en muchas arreas, incluyendo la informática y las comunicaciones. Está formada por las organizaciones de normalización de sus 89 países miembro

ITU

La Unión Internacional de Telecomunicaciones (ITU) es el organismo especializado de las Naciones Unidas encargado de regular las telecomunicaciones, a nivel internacional, entre las distintas administraciones y empresas operadoras.

K

Kerberos

Kerberos es un protocolo de autenticación de redes de ordenador que permite a dos computadores en una red insegura demostrar su identidad mutuamente de manera segura. Sus diseñadores se concentraron primeramente en un modelo de cliente-servidor, y brinda autenticación mutua: tanto cliente como servidor verifican la identidad uno del otro. Los mensajes de autenticación están protegidos para evitar intromisiones y ataques de Replay.

Kerberos se basa en criptografía de clave simétrica y requiere un tercero de confianza. Además, existen extensiones del protocolo para poder utilizar criptografía de clave asimétrica.

Kpasswd

kpasswd – El comando kpasswd cambia la contraseña registrada en una base de datos de autenticación de entrada. By default, the command interpreter changes the password for the AFS user name that matches the issuer's local identity (UNIX UID). De forma predeterminada, el intérprete de comandos cambia la contraseña de la AFS nombre de usuario que coincida con la del emisor identidad local (UNIX UID). To specify an alternate user, include the -principal argument. Para especificar un usuario suplente, se incluye el principal argumento. El nombre de usuario por el principal argumento no tiene que aparecer en el archivo de contraseña local (el archivo / etc / passwd o equivalente), contraseña del emisor en la base de datos de autenticación.

L

LAN

LAN en informática designa a una red de área local, conocida por sus siglas en inglés LAN (Local Area Network).
Una red de área local, o red local, es la interconexión de varios ordenadores y periféricos. Su extensión está limitada físicamente a un edificio o a un entorno de hasta 100 metros. Su aplicación más extendida es la interconexión de computadores personales y estaciones de trabajo en oficinas, fábricas, etc., para compartir recursos e intercambiar datos y aplicaciones. En definitiva, permite que dos o más máquinas se comuniquen.

LDAP

LDAP (Lightweight Directory Access Protocol) es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP también es considerado una base de datos (aunque su sistema de almacenamiento puede ser diferente) a la que pueden realizarse consultas.

Habitualmente, almacena la información de login (usuario y contraseña) y es utilizado para autenticarse aunque es posible almacenar otra información (datos de contacto del usuario, ubicación de diversos recursos de la red, permisos, certificados, etc).

En conclusión, LDAP es un protocolo de acceso unificado a un conjunto de información sobre una red.

Lenguaje:

En informática, conjunto de caracteres e instrucciones utilizadas para escribir programas de ordenador.

Login

"/login" tiene dos comportamientos: Como requeridor de credenciales y como aceptador de credenciales.
Si el cliente ya tiene una sesión "single sing-on" con FCAS, el navegador presentará a FCAS una cookie segura conteniendo una cadena identificando un "ticket-granting ticket". Está cookie es llamada "ticket-granting cookie". Si la cookie contiene un ticket "ticket-granting" valido, FCAS podrá entregar "tickets de servicio" a las aplicaciones registradas que los soliciten.

Loops

Circuitos. Un loop (o bucle) de teléfonos son dos teléfonos que se comunican entre sí.

Lotus domino

El software IBM lotus domino ofrece excelentes funciones de colaboración que se pueden desplegar como una infraestructura central de planificación empresarial y de correo electrónico, como una plataforma de aplicaciones empresariales o como ambas cosas.

Lotus domino y sus opciones de software de cliente ofrecen un entorno seguro y fiable de mensajería y colaboración que aumenta la productividad de las personas, agiliza los procesos empresariales y mejora la capacidad de respuesta de la empresa en general

Ventajas

- Amplía la mensajería con herramientas de colaboración integradas.
- Ofrece flexibilidad y variedad de plataformas de hardware, sistemas operativos, directorios y accesos de cliente.
- Proporciona funciones punteras de seguridad que protegen la información fundamental para la empresa.
- Disminuye el coste total de propiedad (TCO) al facilitar un uso eficaz de los recursos de CPU, el ancho de banda de red y el almacenamiento en disco.
- Maximiza la disponibilidad de servidor con agrupación en clúster avanzada, registro cronológico de transacciones, recuperación de errores de servidor y herramientas de diagnóstico automático.
- Gracias a las funciones avanzadas de administración que incluye, reduce el tiempo y los costes asociados al despliegue y la gestión de la infraestructura.
- Soporta servicios web y estándares abiertos, y ofrece herramientas de integración con las aplicaciones existentes.
- Puede proporcionar una rápida recuperación de las inversiones (ROI) gracias a las soluciones basadas en software Lotus Domino para procesos empresariales como la gestión de relaciones con los clientes, la cadena de suministros y el seguimiento de proyectos.

M

MAC

En redes de computadoras la dirección MAC (Medium access control address o dirección de control de acceso al medio) es un identificador de 48 bits (6 bytes) que corresponde de forma única a una tarjeta o interfaz de red. Es individual, cada

dispositivo tiene su propia dirección MAC determinada y configurada por el IEEE (los últimos 24 bits) y el fabricante (los primeros 24 bits) utilizando el OUI. La mayoría de los protocolos que trabajan en la capa 2 del modelo OSI usan una de las tres numeraciones manejadas por el IEEE: MAC-48, EUI-48, y EUI-64 las cuales han sido diseñadas para ser identificadores globalmente únicos. No todos los protocolos de comunicación usan direcciones MAC, y no todos los protocolos requieren identificadores globalmente únicos.

Las direcciones MAC son únicas a nivel mundial, puesto que son escritas directamente, en forma binaria, en el hardware en su momento de fabricación. Debido a esto, las direcciones MAC son a veces llamadas Quemadas en las Direcciones (BIA).

MAN

Una red de área metropolitana (En inglés, Metropolitan area network o MAN) es una red de alta velocidad (banda ancha) que dando cobertura en un área geográfica extensa, proporciona capacidad de integración de múltiples servicios mediante la transmisión de datos, voz y vídeo, sobre medios de transmisión tales como fibra óptica y par trenzado (MAN BUCLE), la tecnología de pares de cobre se posiciona como una excelente alternativa para la creación de redes metropolitanas, por su baja latencia (entre 1 y 50ms), gran estabilidad y la carencia de interferencias radioeléctricas, las redes MAN BUCLE, ofrecen velocidades que van desde los 2Mbps y los 155Mbps.

MDNS

Zeroconf o Zero Configuration Networking es un conjunto de técnicas que permiten crear de forma automática una red IP sin configuración o servidores especiales. También conocida como Automatic Private IP Addressing or APIPA, permite a los usuarios sin conocimientos técnicos conectar ordenadores, impresoras de red y otros elementos y hacerlos funcionar. Sin Zeroconf, un usuario con conocimientos técnicos debe configurar servidores especiales, como DHCP y DNS, o bien configurar cada ordenador de forma manual.

MDI

Los programas de ordenador gráficos de interfaz de múltiples documentos (MDI) son aquellos cuyas ventanas se encuentran dentro de una ventana padre (normalmente con la excepción de las ventanas modales), de manera opuesta a una interfaz de documento único. Se suele utilizar el acrónimo MDI. Ha habido muchos debates sobre qué tipo de interfaz se prefiere. Generalmente se considera que SDI es más útil si los usuarios trabajan con varias aplicaciones. Las compañías han utilizado ambos sistemas con reacciones diversas. Por ejemplo, Microsoft ha cambiado la interfaz de

sus aplicaciones Office de SDI a MDI y luego otra vez a SDI, aunque el grado de implementación varía entre componentes.

MTA

Un agente de transferencia de correo (MTA) (también conocido como Agente de Transporte de Correo, Agente de Transferencia de Mensajes, o smtpd (corto para SMTP demonio), es un programa de ordenador o software agente que transfiere mensajes de correo electrónico de un ordenador a otro.

El término servidor de correo también se utiliza en el sentido de un ordenador que actúa como un MTA que se está ejecutando el software adecuado. El término intercambiador de correo (MX), en el contexto del sistema de nombres de dominio se refiere formalmente a una dirección IP asignada a un dispositivo que aloja un servidor de correo, y por extensión también indica el propio servidor.

N

NAC

Network Access Control es un concepto de redes de computadoras y un conjunto de protocolos utilizados para definir la forma de conseguir los nodos de la red antes de acceder a los nodos de la red. NAC podría integrar el proceso de reparación automática (fijando las condiciones no conforme requeridas antes de permitir el acceso a nodos) en los sistemas de redes, permitiendo que la infraestructura de red tales como routers, switches y firewalls para trabajar junto con los servidores de back office y el equipo informático del usuario final para asegurar que el sistema de información este funcionando bien antes de la interoperabilidad permitida.

NAT

NAT (Network Address Translation - Traducción de Dirección de Red) es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles. Consiste en convertir en tiempo real las direcciones utilizadas en los paquetes transportados. También es necesario editar los paquetes para permitir la operación de protocolos que incluyen información de direcciones dentro de la conversación del protocolo.

Existen muchas variantes de traducción de direcciones que se prestan a distintas aplicaciones. Sin embargo todas las variantes de dispositivos NAT deberían compartir las siguientes características:

Asignación transparente de direcciones.

Encaminamiento transparente mediante la traducción de direcciones (aquí el encaminamiento se refiere al reenvío de paquetes, no al intercambio de información de encaminamiento). Traducción de la carga útil de los paquetes de error ICMP

NBNS

Resolución de nombres de NetBIOS sobre TCP/IP y WINS.
NetBIOS sobre TCP/IP es el componente de red que realiza la resolución o asignación de nombres de nombre de equipo a dirección IP. Actualmente hay cuatro métodos de resolución de nombres de NetBIOS sobre TCP/IP: nodo b, nodo p, nodo m y nodo h.

NBSS

SAMBA es SMB/NetBIOS sobre TCP/IP. El protocolo NetBIOS utiliza tres puertos, a saber el servicio
> 137 (tcp y udp) para resolución de nombres (nbt)
> 139 (tcp y udp) para servicio de sesiones (nbss)
> 138 (tcp y udp) para servicio de datagramas (nbdgm).

NETBIOS

NetBIOS, "Network Basic Input/Output System", es, en sentido estricto una especificación de interfaz para acceso a servicios de red, es decir, una capa de software desarrollado para enlazar un sistema operativo de red con hardware específico. NetBIOS fue originalmente desarrollado por IBM y Sytek como API/APIS para el software cliente de recursos de una red LAN.

Desde su creación, NetBIOS se ha convertido en el fundamento de muchas otras aplicaciones de red.

Norma

Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.

NNTPS

Las noticias de la red de protocolo de transferencia o NNTP es una aplicación de Internet protocolo utilizado principalmente para la lectura y publicación de artículos usenet (alias netnews), así como la transferencia de noticias entre servidores de noticias.

NTP

Network time protocol (NTP) es un protocolo de internet para sincronizar los relojes de los sistemas informáticos a través de ruteo de paquetes en redes con latencia variable. NTP utiliza UDP como su capa de transporte, usando el puerto 123. Está diseñado para resistir los efectos de la latencia variable.

Nukear

Anular un programa de un BBS recién 'subido', por ser antiguo y carecer de interés.

O

OCSP

Online Certificate Status Protocol (OCSP) es un método para determinar el estado de revocación de un certificado digital X.509 usando otros medios que no sean el uso de CRL (Listas de Revocación de Certificados). Este protocolo se describe en el RFC 2560 y está en el registro de estándares de Internet.

Los mensajes OCSP se codifican en ASN.1 y habitualmente se transmiten sobre el protocolo HTTP. La naturaleza de las peticiones y respuestas de OCSP hace que a los servidores OCSP se les conozca como "OCSP responders".

Ventajas sobre las CRL

- OCSP fue creado para solventar ciertas deficiencias de las CRL. Cuando se despliega una PKI (Infraestructura de Clave Pública), es preferible la validación de los certificados mediante OCSP sobre el uso de CRL por varias razones:
- OCSP puede proporcionar una información más adecuada y reciente del estado de revocación de un certificado.
- OCSP elimina la necesidad de que los clientes tengan que obtener y procesar las CRL, ahorrando de este modo tráfico de red y procesado por parte del cliente.
- El contenido de las CRL puede considerarse información sensible, análogamente a la lista de morosos de un banco.
- Un "OCSP responder" puede implementar mecanismos de tarificación para pasarle el coste de la validación de las transacciones al vendedor, más bien que al cliente.
- OCSP soporta el encadenamiento de confianza de las peticiones OCSP entre los "responders". Esto permite que los clientes se comuniquen con un "responder" de confianza para lanzar una petición a una autoridad de certificación alternativa dentro de la misma PKI.

Una consulta sobre el estado de un certificado sobre una CRL, debe recorrerla completa secuencialmente para decir si es válido o no. Un "OCSP responder" en el

fondo, usa un motor de base de datos para consultar el estado del certificado solicitado, con todas las ventajas y estructura para facilitar las consultas. Esto se manifiesta aún más cuando el tamaño de la CRL es muy grande.

Operador

Persona que usa una computadora. A menudo se llama 'operador' al administrador del sistema.

OSPF

Open Shortest Path First (frecuentemente abreviado OSPF) es un protocolo de enrutamiento jerárquico de pasarela interior o IGP (Interior Gateway Protocol), que usa el algoritmo Dijkstra enlace-estado (LSA - Link State Algorithm) para calcular la ruta más corta posible.

OSPF es probablemente el tipo de protocolo IGP más utilizado en grandes redes. Puede operar con seguridad usando MD5 para autentificar a sus puntos antes de realizar nuevas rutas y antes de aceptar avisos de enlace-estado. Como sucesor natural de RIP, acepta VLSM o sin clases CIDR desde su inicio. A lo largo del tiempo, se han ido creando nuevas versiones, como OSPFv3 que soporta IPv6 o como las extensiones multidifusión para OSPF (MOSPF), aunque no están demasiado extendidas. OSPF puede "etiquetar" rutas y propagar esas etiquetas por otras rutas.

Outdial

Modem de salida dentro de una misma red, que permite a un usuario de la misma salir a la red telefónica convencional. Los que permiten hacer llamadas a larga distancia se llaman 'global Outdial' (Outdial globales) o GOD.

P

Packet switching

Conmutación de paquetes.

PAP

PAP son las siglas de Password Authentication Protocol, un protocolo simple de autenticación para autenticar un usuario contra un servidor de acceso remoto o contra un ISP. PAP es un sub-protocolo usado por la autenticación del protocolo PPP (Point

to Point Protocol), validando a un usuario que accede a ciertos recursos. PAP transmite contraseñas o pasword en ASCII sin cifrar, por lo que se considera inseguro. PAP se usa como último recurso cuando el servidor de acceso remoto no soporta un protocolo de autenticación más fuerte.

Papeles de trabajo:

Registra el planeamiento, naturaleza, oportunidad y alcance de los procedimientos de auditoría aplicados por el auditor y los resultados y conclusiones extraídas a la evidencia obtenida. Se utilizan para controlar el progreso del trabajo realizado para respaldar la opinión del auditor.

Paquete de auditoría

Generalizados de computadora diseñados para desempeñar funciones de procesamiento de datos que incluyen leer archivos de computadora, seleccionar información, realizar cálculos, crear archivos de datos e imprimir informes en un formato especificado por el auditor.

Parámetro

Valor especificado para conseguir los resultados deseados. En comunicaciones existe tal cantidad de parámetros que suelen ofuscar a los usuarios noveles: bits por segundo, bits de datos, bits de parada, paridad, etc. Información que se añade al comando que inicia una determinada aplicación. Un parámetro puede ser un nombre de archivo o cualquier tipo de información de hasta 62 caracteres de largo.

Password

Conocida también como 'clave de acceso'. Palabra o clave privada utilizada para confirmar una identidad en un sistema remoto que se utiliza para que una persona no pueda usurpar la identidad de otra.

Patch o Parche

Modificación de un programa ejecutable para solucionar un problema o para cambiar su comportamiento.

Payload

Efecto visible de un software maligno.

PBX

Private Branch Exchange. Centrales telefónicas internas de empresas

PERSONAL COMPUTER

Una computadora personal (PC) es cualquier computadora cuyo precio de venta original, el tamaño y capacidad lo hacen especialmente útil para las personas, y que estén destinadas a ser explotadas directamente por un usuario final, sin intervención de operador de computadora.

Hoy en día un PC puede ser un ordenador de sobremesa, un ordenador portátil o un Tablet PC. Los más comunes son los sistemas operativos Microsoft Windows, Mac OS X y Linux, mientras que las más comunes son los microprocesadores x86 compatible CPU. Aplicaciones de software para ordenadores personales incluyen el tratamiento de textos, hojas de cálculo, base de datos, juegos, y una miríada de productividad personal y para fines especiales de software.

Modernas computadoras personales a menudo de alta velocidad o conexiones de acceso telefónico a Internet, permitiendo el acceso a la World Wide Web y una amplia gama de otros recursos.

Petar

Anular. Este término se utiliza en el supuesto de que los sistemas utilizados para 'tracear' de un BBS, se hayan anulado o caducado.

Phreaking

Acto de llamar por teléfono gratuitamente y la realización de modificaciones a los aparatos telefónicos con el fin de obtener algún tipo de beneficio.

PKI

En criptografía, una infraestructura de clave pública (o, en inglés, PKI, Public Key Infrastructure) es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas.

El término PKI se utiliza para referirse tanto a la autoridad de certificación y al resto de componentes, como para referirse, de manera más amplia y a veces confusa, al uso de algoritmos de clave pública en comunicaciones electrónicas.

Este último significado es incorrecto, ya que no se requieren métodos específicos de PKI para usar algoritmos de clave pública.
PKIX-CRL

El protocolo de los convenios descritos en el presente documento satisface algunas de las necesidades operacionales de la Internet de la infraestructura de clave pública (PKI). Este documento especifica las convenciones para utilizar el Protocolo de transferencia de archivos (FTP) y el Protocolo de transferencia de hipertexto (HTTP) a la obtención de los certificados y revocación de certificados listas (CRL) de PKI repositorios. Mecanismos adicionales para abordar las necesidades operacionales de PKIX se especifican en documentos separados.

PoE

PoE (Power over Ethernet) es una tecnología que permite la alimentación eléctrica de dispositivos de red a través de un cable UTP / STP en una red Ethernet. PoE se rige según el estándar IEEE 802.3af y abre grandes posibilidades a la hora de dar alimentación a dispositivos tales como cámaras de seguridad, teléfonos o puntos de acceso inalámbricos.

POP3

Los proveedores de Internet en informática se utilizan el Post Office Protocol (POP3) en clientes locales de correo para obtener los mensajes de correo electrónico almacenados en un servidor remoto. La mayoría de los suscriptores acceden a sus correos a través de POP3.

Las versiones del protocolo POP (informalmente conocido como POP1) y POP2 se han hecho obsoletas debido a las últimas versiones de POP3. En general cuando uno se refiere al término POP, nos referimos a POP3 dentro del contexto de protocolos de correo electrónico.

Procedimiento

Método o sistema estructurado para la ejecución de actividades

Procedimiento

En computación, una subrutina o subprograma, como idea general, se presenta como un algoritmo separado del algoritmo principal, el cual permite resolver una tarea específica.

Procesamiento de datos

Conjunto de diferentes operaciones en secuencia sistemática sobre el dato, las cuales se basan en la elaboración, manipuleo y tratamiento del mismo, mediante máquinas automáticas para producir los resultados esperados.

Proceso

Conjunto de operaciones lógicas y aritméticas ordenadas, cuyo fin es la obtención de resultados.

Programa

Secuencia de instrucciones que obliga al ordenador a realizar una tarea determinada.

Programa cliente

Programa cliente o simplemente 'cliente' es aquel programa que permite conectarse a un determinado sistema, servicio o red.

Programa emergente

Programa residente cargado en la memoria, que no es visible hasta que se presione una determinada combinación de teclas o hasta que tenga lugar un determinado hecho, tal como la recepción de un mensaje.

Programas

Proyecto o planificación ordenada de las distintas partes o actividades que componen algo que se va a realizar.

Programas de administración del sistema

Herramientas de productividad sofisticadas que son típicamente parte de los sistemas operativos sofisticados, por ejemplo software para recuperación de datos o software para comparación de códigos.

Como en el caso anterior estas herramientas no son específicamente diseñadas para usos de auditoría y deben ser utilizadas con cuidado.

Programas de utilería

Son usados por la entidad para desempeñar funciones comunes de procesamiento de datos, como clasificación, creación e impresión de archivos. Estos programas generalmente no están diseñados para propósitos de auditoría y, por lo tanto, pueden no contener características tales como conteo automático de registros o totales de control.

PSI

La seguridad informática consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida así como su modificación sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

PPPoE

PPPoE (Point-to-Point Protocol over Ethernet) es un protocolo de red para la encapsulación PPP sobre una capa de Ethernet. Es utilizada mayormente para proveer conexión de banda ancha mediante servicios de cable módem y xDSL.

En esencia, es un protocolo túnel, que permite implementar una capa IP sobre una conexión entre dos puertos Ethernet, pero con las características de software del protocolo PPP, por lo que es utilizado para virtualmente "marcar" a otra máquina dentro de la red Ethernet, logrando una conexión "serial" con ella, con la que se pueden transferir paquetes IP, basado en las características del protocolo PPP.

PPTP

(Point to Point Tunneling Protocol), es un protocolo desarrollado por Microsoft, U.S. Robotics, Ascend Communications, 3Com/Primary Access, ECI Telematics conocidas colectivamente como PPTP Forum, para implementar redes privadas virtuales o VPN. Una VPN es una red privada de computadores que usa Internet para conectar sus nodos. PPTP ha sido crackeado o descifrado, no debería usarse donde la privacidad de los datos sea importante.

PUERTO DE RED

Un puerto de red puede ser un puerto serial o un puerto paralelo; suelen ser numerados. La implementación del protocolo en el destino utilizará ese número para decidir a qué programa entregará los datos recibidos.

Q

QoS

QoS o Calidad de Servicio (En inglés, Quality of Service) son las tecnologías que garantizan la transmisión de cierta cantidad de datos en un tiempo dado (throughput). Calidad de servicio es la capacidad de dar un buen servicio.

R

RADIUS

RADIUS (acrónimo en inglés de Remote Authentication Dial-In User Server). Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1813 UDP para establecer sus conexiones.

Red

Servicio de comunicación de datos entre ordenadores. Conocido también por su denominación inglesa: 'network'. Se dice que una red está débilmente conectada cuando la red no mantiene conexiones permanentes entre los ordenadores que la forman. Esta estructura es propia de redes no profesionales con el fin de abaratar su mantenimiento.
Repositorio

Donde se almacenan los elementos definidos o creados por la herramienta, y cuya gestión se realiza mediante el apoyo de un sistema de gestión de base de datos (SGBD) o de un sistema de gestión de ficheros

RIP

RIP son las siglas de Routing Information Protocol (Protocolo de encaminamiento de información). Es un protocolo de puerta de enlace interna o IGP (Internal Gateway Protocol) utilizado por los routers (enrutadores), aunque también pueden actuar en equipos, para intercambiar información acerca de redes IP.

RMON

La Red Remote MON itoring (RMON) MIB fue desarrollado por la IETF para apoyar la vigilancia y el análisis de protocolo de LAN. La versión original (a veces denominado RMON1) se centró en la información de la Capa 1 y la Capa 2 del modelo OSI de redes Ethernet y Token Ring. Se ha prorrogado por RMON2 que

incluye soporte para la capa de red y la capa de aplicación de vigilancia y SMON que incluye soporte para redes conmutadas. Se trata de una especificación estándar de la Industria que proporciona gran parte de la funcionalidad ofrecida por los analizadores de red. Los agentes RMON se incorporan en una gama alta de switches y routers (como los construidos por ProCurve, 3Com y Cisco).

RS-232

RS-232 (también conocido como Electronic Industries Alliance RS-232C) es una interfaz que designa una norma para el intercambio serie de datos binarios entre un DTE (Equipo terminal de datos) y un DCE (Data Communication Equipment, Equipo de Comunicación de datos), aunque existen otras situaciones en las que también se utiliza la interfaz RS-232.

El puerto serie RS-232C, presente en todos los ordenadores actuales, es la forma más comúnmente usada para realizar transmisiones de datos entre ordenadores. El RS-232C es un estándar que constituye la tercera revisión de la antigua norma RS-232, propuesta por la EIA (Asociación de industrias electrónicas), realizándose posteriormente un versión internacional por el CCITT, conocida como V.24. Las diferencias entre ambas son mínimas, por lo que a veces se habla indistintamente de V.24 y de RS-232C (incluso sin el sufijo "C"), refiriéndose siempre al mismo estándar.

El RS-232C consiste en un conector tipo DB-25 de 25 pines, aunque es normal encontrar la versión de 9 pines DB-9, mas barato e incluso más extendido para cierto tipo de periféricos (como el serial del mouse del PC). En cualquier caso, los PCs no suelen emplear más de 9 pines en el conector DB-25. Las señales con las que trabaja este puerto serie son digitales, de +12V (0 lógico) y -12V (1 lógico), para la entrada y salida de datos, y a la inversa en las señales de control. El estado de reposo en la entrada y salida de datos es -12V. Dependiendo de la velocidad de transmisión empleada, es posible tener cables de hasta 15 metros.

RSA SEcur ID

RSA SecurID es un mecanismo desarrollado por RSA Security para realizar autenticación de dos factores para que un usuario de una red de recursos. El sistema de autentificación RSA SecurID® cuenta con la confianza de miles de organizaciones en todo el mundo para proteger los valiosos recursos de red. Utilizado conjuntamente con el RSA® Authentication Manager, un autentificador RSA SecurID funciona como una tarjeta ATM para una red, requiriendo que los usuarios se identifiquen con dos factores exclusivos – algo que conocen y algo que tienen – antes de permitirles el acceso. Millones de personas utilizan autentificadores RSA SecurID para acceder de forma segura a VPNs, puntos de acceso inalámbrico, cortafuegos de acceso remoto, aplicaciones de red y sistemas operativos de red. El sistema es fácil de utilizar y gestionar y tiene como consecuencia una mayor

seguridad, lo cual puede proporcionar un rendimiento de la inversión más rápido en la mayoría de iniciativas de e-business.

RSVP

El Protocolo de reserva de recursos (RSVP), que se describe en el RFC 2205, es una empresa de transporte capa de protocolo destinado a reserva de recursos a través de una red de manera integrada los servicios de Internet. ICMPIGMPRFC 2205 "RSVP no aplicación de transporte de datos, pero es más bien un protocolo de control de Internet, como ICMP, IGMP, o protocolos de enrutamiento" - RFC 2205. multicastunicast RSVP proporciona receptor-inició la configuración de las reservas de recursos para multicast o unicast los flujos de datos con la expansión y solidez.

HostsroutersQoS RSVP puede ser utilizado por cualquier hosts o router para solicitar o entregar los niveles específicos de calidad de servicio (QoS) para la aplicación de datos corrientes. RSVP define cómo las aplicaciones a cabo las reservas y la forma en que pueden renunciar a los recursos reservados una vez que la necesidad de ellos ha llegado a su fin. Operación RSVP por lo general es el resultado de que los recursos se reserven a cada nodo a lo largo de un camino. Routing protocol RSVP no es en sí misma un protocolo de enrutamiento y fue diseñado para interoperar con los actuales y futuros protocolos de enrutamiento.

Citation neededtraffic engineeringRSVP-TE RSVP es de por sí rara vez desplegados en redes de telecomunicaciones, pero la ingeniería de extensión de tráfico de RSVP, o RSVP-TE, es cada vez más ampliamente aceptada hoy en día en muchos QoS orientado a las redes.

RTSP

El protocolo de flujo de datos en tiempo real (del inglés Real Time Streaming Protocol) establece y controla uno o muchos flujos sincronizados de datos, ya sean de audio o de video. El RTSP actúa como un mando a distancia mediante la red RTSP es un protocolo no orientado a conexión, en lugar de esto el servidor mantiene una sesión asociada a un identificador, en la mayoría de los casos RTSP usa TCP para datos de control del reproductor y UDP para los datos de audio y vídeo.

S

Servidor o server

Ordenador que ejecuta uno o más programas simultáneamente con el fin de distribuir información a los ordenadores que se conecten con él para dicho fin. Vocablo más conocido bajo su denominación inglesa 'server'.

SFP

El pequeño forma-factor pluggable (SFP) es un compacto, "hot-pluggable" transceptor óptico utilizado en comunicaciones ópticas, tanto para las telecomunicaciones y comunicaciones de datos. Se trata de un formato de una industria popular apoyado por varios componentes de fibra óptica de los proveedores.

Transceptores SFP están destinados a apoyar SONET, Gigabit Ethernet, canal de fibra, y otras comunicaciones. La norma se está expandiendo a la SFP + que será capaz de soportar velocidades de hasta 10,0 Gbps (que incluyen la velocidad de transmisión de datos para el canal de fibra de 8 Gbits, y 10GbE. SFP + módulo para las versiones óptica, así como el cobre, se está introduciendo.

Sintaxis

Es el conjunto de reglas estructurales para uso del lenguaje en el ordenador.

Sistema de información

Constituye el conjunto de procedimientos manuales y/o automatizados que están orientados a proporcionar información para la toma de decisiones.

SMB

Server Message Block o SMB es un Protocolo de red que permite compartir archivos e impresoras entre nodos de una red.

SMTP

Simple Mail Transfer Protocol (SMTP), o Protocolo Simple de Transferencia de Correo. Protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras o distintos dispositivos (PDA's, teléfonos móviles, etc.). Está definido en el RFC 2821 y es un estándar oficial de Internet.

SnapShots:

Es una fotografía interna al sistema, es decir a la memoria, lo que permite obtener resultados intermedios en diferentes momentos de un proceso o conseguir valores temporales de una variable. Se activa mediante ciertas condiciones preestablecidas. Permite al auditor rastrear los datos y evaluar los algoritmos aplicados a los datos.

SNMP

El Protocolo Simple de Administración de Red o SNMP es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Es parte de la familia de protocolos TCP/IP. SNMP permite a los administradores supervisar el desempeño de la red, buscar y resolver sus problemas, y planear su crecimiento

SOCKET

Socket designa un concepto abstracto por el cual dos programas (posiblemente situados en computadoras distintas) pueden intercambiarse cualquier flujo de datos, generalmente de manera fiable y ordenada.

Software

Componentes inmateriales del ordenador: programas, sistemas operativos, etc.

Software aplicado

Programas escritos para la realización de tareas especiales, como el procesado de palabras o listas de correspondencia.

Software de sistemas

Secciones de códigos que llevan a cabo tareas administrativas dentro del ordenador o ayudan en la escritura de otros programas, pero que no se usan para realizar la tarea que se quiere que ejecute el ordenador.

Software para un propósito específico o diseñado a la medida

Son programas de computadora diseñados para desempeñar tareas de auditoría en circunstancias específicas. Estos programas pueden ser desarrollados por el auditor, por la entidad, o por un programador externo contratado por el auditor. En algunos casos el auditor puede usar programas existentes en la entidad en su estado original o modificado porque puede ser más eficiente que desarrollar programas independientes

SPAM

Se llama spam, correo basura o sms basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas)

que perjudican de alguna o varias maneras al receptor. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico. Otras tecnologías de internet que han sido objeto de correo basura incluyen grupos de noticias, usenet, motores de búsqueda, wikis, foros, blogs, también a través de popups y todo tipo de imágenes y textos en la web. El correo basura también puede tener como objetivo los teléfonos móviles (a través de mensajes de texto) y los sistemas de mensajería instantánea como por ejemplo Outlook, Lotus Notes, etc.

SSDP

Simple Servicio Discovery Protocol (SSDP) es una versión anterior del proyecto IETF de Internet de Microsoft y Hewlett-Packard. SSDP es la base del descubrimiento del protocolo Universal plug-and-play.
SSDP proporciona un mecanismo que los clientes de la red pueden utilizar para descubrir los servicios de red. Los clientes pueden utilizar SSDP con poca o ninguna configuración estática.

SSID

El SSID (Service Set IDentifier) es un código incluido en todos los paquetes de una red inalámbrica (Wi-Fi) para identificarlos como parte de esa red. El código consiste en un máximo de 32 caracteres alfanuméricos. Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID.

Existen algunas variantes principales del SSID. Las redes ad-hoc, que consisten en máquinas cliente sin un punto de acceso, utilizan el BSSID (Basic Service Set Identifier); mientras que en las redes en infraestructura que incorporan un punto de acceso, se utiliza el ESSID (E de extendido). Nos podemos referir a cada uno de estos tipos como SSID en términos generales. A menudo al SSID se le conoce como nombre de la red.

Uno de los métodos más básicos de proteger una red inalámbrica es desactivar el broadcast del SSID, ya que para el usuario medio no aparecerá como una red en uso. Sin embargo no debería ser el único método de defensa para proteger una red inalámbrica. Se deben utilizar también otros sistemas de cifrado y autentificación.

SSL

SSL proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía. Habitualmente, sólo el servidor es autenticado (es decir, se garantiza su identidad) mientras que el cliente se mantiene sin autenticar; la autenticación mutua requiere un despliegue de infraestructura de claves públicas (o PKI) para los clientes.

STP

STP, acrónimo de Shielded Twisted Pair o FUTP Par Trenzado Apantallado. El cable de par trenzado apantallado es justamente lo que su nombre implica: cables de cobre aislados dentro de una cubierta protectora, con un número específico de trenzas por pie. STP se refiere a la cantidad de aislamiento alrededor del conjunto de cables y, por lo tanto, a su inmunidad al ruido al contrario que UTP (Unshielded Twisted Pair, "Par trenzado sin apantallar") que no dispone de dicho aislamiento.

Subir o Upload

Enviar un programa a un BBS vía módem.

SYMANTEC NAC 5,1

Con Symantec la adquisición de Sygate a finales de 2005, la empresa de seguridad adquirida conocimientos y herramientas que han permitido continuar con nuevas áreas de productos. Por cuestiones de seguridad asociados, la más importante la descendencia de la unión es Symantec Network Access Control (SNAC), una línea de software y hardware para redes de ofertas de casi cualquier tamaño.

En su forma más básica, 5,1 SNAC es un producto de software único que combina un servidor de administración con el agente basado en la tecnología para hacer cumplir de punto final y bloquear las políticas o reparar los sistemas que no cumplen. Para construcción VARs de redes de mayor tamaño, Symantec ofrece tres aparatos que proporcionan LAN, puerta de enlace y física DHCP aplicación de la política.

CRN Test Center miró a los ingenieros de software de aplicación sólo de SNAC, que consistió en la Symantec Sygate Policy Manager, una aplicación agente, Sygate firewall personal y un servidor DHCP de software plug-in. La instalación del producto es relativamente sencilla, pero los instaladores deben planificar la aplicación del producto y no sólo de buceo en el asistente de instalación. Una comprensión básica del diseño de red y puntos finales es una obligación de garantizar una instalación sin complicaciones.

El gestor de la política componente está instalado en un servidor Windows 2003 y tiene varios otros requisitos previos (al igual que la mayoría de los productos NAC), como por ejemplo Internet Information Services y World Wide Web Services y, por supuesto, debe cumplir con los requisitos mínimos de hardware se indica en la guía de inicio . En aras de la simplicidad, Centro de pruebas, los ingenieros instalan el gestor de la política y sus componentes en un único servidor.

El producto del asistente de configuración del servidor hizo corto trabajo de la instalación real, y la documentación incluida de inicio rápido demostrando ser un excelente recurso para la instalación.

SYSLOG

Syslog es un estándar de facto para el envío de mensajes de registro en una red informática IP. Por syslog se conoce tanto al protocolo de red como a la aplicación o biblioteca que envía los mensajes de registro. Un mensaje de registro suele tener información sobre la seguridad del sistema, aunque puede contener cualquier información. Junto con cada mensaje se incluye la fecha y hora del envío.

T

TCP

TCP (Transmission Control Protocol, en español Protocolo de Control de Transmisión) es uno de los protocolos fundamentales en Internet. Fue creado entre los años 1973 - 1974 por Vint Cerf y Robert Kahn. Muchos programas dentro de una red de datos compuesta por ordenadores pueden usar TCP para crear conexiones entre ellos a través de las cuales puede enviarse un flujo de datos. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto. TCP da soporte a muchas de las aplicaciones más populares de Internet, incluidas HTTP, SMTP, SSH y FTP.

Funciones de TCP

En la pila de protocolos TCP/IP, TCP es la capa intermedia entre el protocolo de internet (IP) y la aplicación. Habitualmente, las aplicaciones necesitan que la comunicación sea fiable y, dado que la capa IP aporta un servicio de datagramas no fiable (sin confirmación), TCP añade las funciones necesarias para prestar un servicio que permita que la comunicación entre dos sistemas se efectúe: libre de errores, sin pérdidas y con seguridad.

Técnica

La técnica es el procedimiento o el conjunto de procedimientos que tienen como objetivo obtener un resultado determinado, ya sea en el campo de la ciencia, de la tecnología, de las artesanías o en otra actividad

TELNET

Telnet (TELecommunication NETwork) es el nombre de un protocolo de red (y del programa informático que implementa el cliente), que sirve para acceder mediante

una red a otra máquina, para manejarla como si estuviéramos sentados delante de ella. Para que la conexión funcione, como en todos los servicios de Internet, la máquina a la que se acceda debe tener un programa especial que reciba y gestione las conexiones.

El puerto que se utiliza generalmente es el 23.

TFTP

TFTP son las siglas de Trivial file transfer Protocol (Protocolo de transferencia de archivos triviales).

Es un protocolo de transferencia muy simple semejante a una versión básica de FTP. TFTP a menudo se utiliza para transferir pequeños archivos entre ordenadores en una red, como cuando un terminal X Windows o cualquier otro cliente ligero que arrancan desde un servidor de red.

TLS

Secure Sockets Layer (SSL) y Transport Layer Security (TLS) -Seguridad de la Capa de Transporte-, su sucesor, son protocolos criptográficos que proporcionan comunicaciones seguras en Internet. Existen pequeñas diferencias entre SSL 3.0 y TLS 1.0, pero el protocolo permanece sustancialmente igual. El término "SSL" según se usa aquí, se aplica a ambos protocolos a menos que el contexto indique lo contrario.

Tracear

Seguimiento exhaustivo. Se utiliza cuando se intenta desproteger un programa y se tiene instalado un Debugger.

Este término también es utilizado en caso de que la línea telefónica esté pinchada por la policía.

Trader

Persona que 'sube' y 'baja' continuamente programas y juegos de BBS.

Tunning

Técnica de observación, de medidas encaminadas a la evaluación del comportamiento del sistema en su conjunto.

U

UDP

User Datagram Protocol (UDP) es un protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. Tampoco tiene confirmación, ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros; y tampoco se sabe si ha llegado correctamente, ya que no hay confirmación de entrega o de recepción. Su uso principal es para protocolos como DHCP, BOOTP, DNS y demás protocolos en los que el intercambio de paquetes de la conexión/desconexión son mayores, o no son rentables con respecto a la información transmitida, así como para la transmisión de audio y vídeo en tiempo real, donde no es posible realizar retransmisiones por los estrictos requisitos de retardo que se tiene en estos casos.

UPS

Un sistema de alimentación ininterrumpida (UPS), también conocida como una continua fuente de alimentación (CPS) o una batería es un dispositivo que mantiene un suministro continuo de energía eléctrica para el equipo conectado mediante el suministro de energía de una fuente de suministro de energía eléctrica cuando no está disponible. Se diferencia de un auxiliar de alimentación o generador de espera, que no ofrece protección instantánea de una interrupción momentánea de energía. Sistemas integrados que tienen UPS y generan reserva de componentes son a menudo denominados sistemas de energía de emergencia.

UUCP

UUCP es una abreviatura de Unix to Unix Copy. El término generalmente se refiere a un conjunto de programas de ordenador y protocolos que permiten la ejecución remota de comandos y la transferencia de archivos, correo electrónico y en concreto, uucp es uno de los programas en la suite, que proporciona una interfaz de usuario para solicitar las operaciones de copia de archivos..

UUCP La suite también incluye uux (interfaz de usuario para la ejecución remota de comandos), uucico (programa de comunicación), uustat (informes estadísticos sobre la actividad reciente), uuxqt (ejecutar comandos enviados desde las máquinas remotas), y uuname (informes uucp el nombre del sistema local).

Aunque UUCP fue desarrollado originalmente por la mayoría y está estrechamente relacionada con Unix, existen implementaciones de UUCP para varios otros sistemas

operativos, incluyendo Microsoft, MS-DOS, Digital VAX / VMS, Commodore's AmigaOS, y Mac OS.

Un sistema de alimentación ininterrumpida (UPS), también conocida como una continua fuente de alimentación (CPS) o una batería es un dispositivo que mantiene un suministro continuo de energía eléctrica para el equipo conectado mediante el suministro de energía de una fuente de suministro de energía eléctrica cuando no está disponible.

Se diferencia de un auxiliar de alimentación o de espera generador, que no ofrece protección instantánea de una interrupción momentánea de energía. Sistemas integrados que han de UPS y generador de reserva componentes son a menudo denominados sistemas de energía de emergencia.

V

Virii

Suele encontrarse en textos en inglés. Es la acción de crear virus.

VLAN

Una VLAN (acrónimo de Virtual LAN, 'red de área local virtual') es un método de crear redes lógicamente independientes dentro de una misma red física. Varias VLANs pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el dominio de colisión y ayudan en la administración de la red separando segmentos lógicos de una red de área local (como departamentos de una empresa) que no deberían intercambiar datos usando la red local (aunque podrían hacerlo a través de un enrutador).

Una 'VLAN' consiste en una red de ordenadores que se comportan como si estuviesen conectados al mismo cable, aunque pueden estar en realidad conectados físicamente a diferentes segmentos de una red de área local. Los administradores de red configuran las VLANs mediante software en lugar de hardware, lo que las hace extremadamente flexibles. Una de las mayores ventajas de las VLANs surge cuando se traslada físicamente algún ordenador a otra ubicación: puede permanecer en la misma VLAN sin necesidad de ninguna reconfiguración hardware.

VNC

VNC son las siglas en inglés de Virtual Network Computing (Computación en Red Virtual). VNC es un programa de software libre basado en una estructura cliente-servidor el cual nos permite tomar el control del ordenador servidor remotamente a través de un ordenador cliente. También llamado software de escritorio remoto. VNC