UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

"ADMINISTRACIÓN DE RIESGOS EN LAS TECNOLOGÍAS DE INFORMACIÓN"

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN

P R E S E N T A:

YESENIA CAMPOS VALDOVINOS

DIRECTOR DE TESIS:

ING. ALEJANDRA BARTOLO GERVACIO

Ciudad Universitaria 2010

A DIOS

Por llevarme hasta este rumbo donde actualmente me encuentro, por la confianza y la vida que día a día disfruto.

Por dotarme de defectos y virtudes específicos que hicieron de mí todo lo que soy y el cómo soy, me ha puesto pruebas difíciles en la vida pero tengo que seguir enfrentándolas para continuar dando amor, consuelo y apoyo a mis seres amados. Lo más importante que te tengo que decir es que aprecio infinitamente todos los paisajes, circunstancias y personas hermosas que me has puesto en el camino.

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

La UNAM se merece todo mi corazón por estar dotada de lugares preciosos, eres tan enorme y diversa que te voy a extrañar inmensamente, jamás olvidaré tu cultura, tu deporte, tu ciencia, tus instalaciones, tus reconocimientos y todo el personal que influye para que seas tan grande a nivel mundial.

Pondré todo mi esmero para siempre portar en alto tu nombre con honor.

A MIS PADRES

Papi, Mami:

He llagado al final de este camino, son las personas más importantes de mi vida esta tesis es un testimonio de gratitud y eterno reconocimiento, por el apoyo que siempre me han brindado y con el cual he logrado terminar mi carrera profesional, siendo para mí, la mejor de las herencias. Han sacrificado gran parte de su vida para formarme y porque nunca podré pagar todos sus desvelos ni aún con las riquezas más grandes del mundo. Por lo que soy y por todo el tiempo que les robé pensando en mi… Gracias.

Gracias también por llevarme de paseo, de compras y a lugares maravillosos que juntos visitamos, por cuidarme desde bebé y dotarme de hermosos valores y cualidades que me enseñaron. Los amo mucho.

Con admiración y respeto, su hija.

A MI HERMANO

Manito

Eres una parte de mi vida, eres el apoyo y por mucho tiempo fuiste la persona que me motivó a seguir con mis estudios porque te vi progresar y eso me inspiraba a alcanzarte, de niños compartimos una vida maravillosa, me cuidaste, me enseñaste y me escuchaste, junto a ti durante el kínder y hasta la secundaria siempre me sentía bien de saber que estabas ahí en algún lado jugábamos juntos y salíamos junto con mis padres de paseo, de domingo, de fiesta, de compras y todo eso me gustaba sólo porque nos acompañabas.

Tu presencia es fundamental para mí y me gusta charlar contigo, deseo que sigamos frecuentándonos y platicando de cualquier cosa: de tu vida, de mi vida, de lo que pasó, de lo que quieras que pase, espero tenerte toda la vida de apoyo. Hermano te quiero infinitamente y te deseo lo mejor porque te lo mereces, algún día encontrarás el rumbo en tu vida y enfréntalo con fortaleza porque siempre hay obstáculos en nuestra vida, pero al pasar por momentos difíciles es cuando valoras todo, cuida a papá, a mamá y valóralos. Lo más importante ábrete un camino de éxito para ti y tus seres queridos, más que tu hermana soy tu amiga cuentas conmigo.

A MI ESPOSO

Esposito, amor mío:

Eres mi complemento ideal tu apoyo, comprensión y tolerancia espero tenerlas siempre. Te agradezco todos los momentos sin excepción nunca me dejes de amar. Eres un chavo excepcional, me encanta estar contigo día a día, me complementas al 100%; gracias a ti y a tu constante esfuerzo en el trabajo y en la casa es que llegue a este día. Te debo todo el mundo y tu apoyo emocional es el que me hizo salir adelante, te debo un agradecimiento eterno por tu amor y tu esfuerzo.

A MIS MAESTROS

Estimado profesor:

Gracias a usted llegué a este día en los primeros semestres fueron difíciles, pero gracias a su tolerancia, transmisión de ideales, conocimientos y en su momento opiniones.

Reitero agradecimiento especial a los siguientes profesores:

ING. FRANCISCO JAVIER MONTOYA CERVANTES
ING. ALEJANDRA BARTOLO GERVACIO
ING. CRUZ SERGIO AGUILAR DÍAZ
ING. GABRIELA BETZABÉ LIZÁRRAGA RAMÍREZ
ING. JESUS ANTONIO PATIÑO RAMÍREZ
ING. JORGE FERAT TOSCANO
ING. MARGARITA CARRERA FOURNIER
ING. MARÍA DEL CARMEN MELO DÍAZ
ING. MARÍA DEL ROSARIO CABEZA LUNA
ING. MARTHA ANGÉLICA NAKAYAMA CERVANTES
ING. ORLANDO ZALDÍVAR ZAMORATEGUI
LIC. CARLOS AURELIO BERNAL ESPONDA
M. en E. ROSALBA RODRÍGUEZ CHÁVEZ
M.I. AURELIO RODOLFO MILLÁN NÁJERA
M.I. JORGE VALERIANO ASSEM
M.I. NORMA ELVA CHÁVEZ RODRÍGUEZ

M.I. RICARDO GARIBAY JIMÉNEZ
MEM. MARGARITA RAMIREZ GALINDO

A MIS AMIGOS

En especial a Mitzy Anaid Sotelo Benito, Erika Patricia Arias Ildefonso y Arturo Ramos Ortega, por escucharme y brindarme apoyo y opiniones que en circunstancias difíciles me dieron.

Gracias por todos los momentos divertidos del propedéutico y de la prepa y su amistad sincera e incondicional.

PERSONAS ESPECIALES:

Un agradecimiento doble a Sergio Cruz Rodríguez y su esposa Ale quienes me enseñaron muchas cosas sobre la vida, el trabajo y la escuela. Me dieron muchos consejos sobre la Familia y pláticas amenas que recuerdo día con día y tampoco olvido los momentos graciosos. Son un ejemplo de familia, sigan así, los quiero.

A la Sra. Lourdes, Minerva y Rosa Martínez Huerta por brindarme su compañía y apoyo en momentos críticos en especial en los de salud, siempre estuvieron ahí para ayudar en lo necesario. Lo que nunca voy a olvidar de ustedes son sus pláticas donde me daban la motivación para seguir adelante a pesar de sus compromisos.

A Karla, Miriam, Daniel, Manuel, Javier, Gerson, Areli, Luis, Rosa, Memo y toda esa gran familia de UNICA los llevo en mi corazón siempre porque pasamos momentos inolvidables.

EN MEMORIA DE

Mi bebé, mi abuelita y mis primos, nunca los olvidaré, algún día nos volveremos a ver.

Descansen en Paz

Índice **Página**

INTRODUCCIÓN

Las Tecnología de Información (TI) agrupan los conceptos de información, comunicación y tecnología que desde su surgimiento hasta la actualidad no cesan de evolucionar, y por lo tanto nos sorprende; la administración de riesgos es un tema reciente, el cual está tomando la importancia que debió haber adquirido desde el surgimiento del Internet, la innovación en tecnología y las comunicaciones que tienen tanto las instituciones, organizaciones, empresas, etc. y la misma sociedad en general, se ha notado que no sólo la seguridad es importante para las TI, sino también, lo es la disponibilidad (evitar que los sistemas tengan interrupciones), cumplimiento, así como el desempeño para cuidar estos factores es necesario administrar los riesgos o mejor dicho identificar, determinar el impacto, planificar, controlar y monitorear todas las causas que afectan el cumplimiento de los requerimientos.

Actualmente no basta con definir políticas, normas, procedimientos o seguir una buena guía de buenas prácticas para proyectos, porque todos en común se complementan, así, al tener bien definido y en orden todo lo antes mencionado, el administrar los riesgos garantiza calidad, un correcto funcionamiento de operaciones, ambiente confiable y sano para el desarrollo de cualquier actividad dentro del sector al que se pertenece como: comercio, minería, agricultura, industria manufacturera, servicios profesionales, de salud, etc. sí y sólo sí se hace de manera permanente, cíclica y constante.

En la administración de riesgos, si se lleva a cabo un buen análisis de riesgo se descubren áreas de oportunidad, las cuales dejan beneficios que se transforman en rentabilidad de producto o servicios proporcionados por la empresa, institución u organismo.

El administrar riesgos no equivale a hacer mejoras, sino estar preparados para el siguiente cambio tecnológico y global, más propiamente dicho, los cambios de mercado internacional (adaptarnos a los cambios), la ayuda que se tiene para gestionar los riesgos se basa en métodos que surgen del esfuerzo de personas, quienes ya se han enfrentado a problemas de integridad, disponibilidad, fiabilidad, pérdida económica, así como de recursos y calidad, entre otros, se formularon los procesos como un medio de aumentar la flexibilidad o de evitar las amenazas a la infraestructura tecnológica, física y como un medio de ayudar a la empresa, a lograr sus objetivos de desarrollo.

Dentro de una estructura jerárquica al no administrar los riesgos hay pérdidas y efectos no deseados a veces irremediables en todos los niveles de trabajo, desde el operativo hasta el nivel gerencial.

La empresa, organización o institución, debe tener conciencia de la información o al menos la suficiente para conocer el ¿por qué?, ¿cuándo?, ¿cómo? y ¿dónde? de las cosas, de lo contrario se tienen efectos no deseados en todos los niveles de trabajo, que afectan el óptimo desempeño y el cumplimiento de los objetivos planteados. Lo que nos lleva a reflexionar cuanto las Tecnologías de Información han definido hoy en día el rumbo operativo de una organización.

Es necesario enfatizar la formalización de la administración de riesgos como una disciplina o rama; en la actualidad el responsable de seguridad además de llevar a cabo la seguridad ahora debe administrar y analizar los riesgos, si realmente se quiere llegar al cumplimiento de la misión y la visión definidas, es indispensable una administración de riesgos concientizada y no verlo como un proceso de mejora. Los riesgos típicos a los que se enfrentan las empresas, instituciones, organizaciones, etc., las cuales no tiene una buena administración de riesgos son: la pérdida de productividad o negocios debido al tiempo de inactividad, responsabilidad por brechas de seguridad que exponen la información de los clientes, violaciones de normas y la imposibilidad de defenderse de demandas, debido a la conservación inadecuada de información. Sólo los riesgos que provienen de sucesos ajenos al factor humano, como una inundación o un terremoto son en una escala, el nivel más alto de peligro, pero no por ello, no tiene un plan de recuperación y si nos anticipamos a él; se disminuye el nivel de incertidumbre e impacto debido a que estamos preparados para una situación extrema como esa, en cambio muchos de los riesgos informáticos son provocados por contratiempos operacionales, procesos inadecuados, no cumplimiento de requisitos normativos u otros factores que también podemos controlar.

Es necesario tener conciencia de la administración de riesgos como un sector clave porque de ella depende nuestra información, la cual se emplea para llevar a cabo la misión y visión, así como los servicios o productos que se brinden, sin ella no se hace nada pero, si se tiene y no se sabe qué hacer con ella tampoco sirve de nada; es por esta razón que el proceso de gestionar o administrar debe ser íntegro, permanente y cíclico, en caso de que alguna etapa se lleve a cabo de forma superficial, incompleta o no se tome en cuenta por considerar que las medidas ya están aplicadas y no necesitan retroalimentación, todo el proceso se afecta lo que lleva a un fracaso de determinado objetivo o proyecto.

Aquí en México se practica la administración de riesgos desde la década de los 90’s como es el caso de IBM, pero a raíz de la crisis internacional del año 2009 se vio la necesidad de contar con un sistema de administración de riesgos eficiente o las prácticas de administración de riesgos requieren de una revisión urgente.

En la encuesta realizada por PricewaterhouseCoopers (PwC) en marzo de 2010 se observo que los empresarios se enfocarán en asignar recursos para actividades de análisis de riesgos (97%) y en prepararse con el fin de saber enfrentar riesgos sistémicos y acontecimientos de alto impacto (97%).Estas son las áreas en las que los (Chief Executive Officer) CEO's o encargados la gestión y dirección administrativa enfocarán sus estrategias de administración y manejo de riesgos:

- Asignación de recursos a actividades de análisis de riesgos 97%.
- Preparación para enfrentar riesgos sistémicos y acontecimientos de alto impacto 97%.
- Creación de estructuras de rendición de cuentas 95.3%.

- Reevaluación de niveles de tolerancia a los riesgos 94.3%.
- Colaboración con proveedores en la cadena de suministro para el manejo conjunto de riesgos 93.4%.
- Integración de las capacidades de administración de riesgos en las unidades de negocio 89.7%.

Empresas que no tuvieron estos problemas son: IBM, BBVA Bancomer, HP, Red Uno, Neoris, Unisys, Hildebrando, Softtek, Bursatek y Mexis.

Objetivos Generales

Mostrar el significado, uso, implantación e importancia de la administración de riesgos en el marco de las tecnologías de información, basado en conocimiento, evaluación y manejo de los riesgos y sus impactos.

Objetivos Particulares

- Que las entidades que proporcionan productos o servicios para una sociedad tengan una guía y un panorama general para conocer, cómo administrar sus riesgos.
- Explicar los diversos tratamientos que existen para administrar riesgos.
- Concientizar sobre la importancia de un análisis constante y permanente de la evolución del riesgo.
- El proceso de administración de riesgos en la TI se debe de ver como una disciplina formal, la cual conste de una base sólida, así como integral, desarrollándose dentro de las organizaciones, empresas o instituciones.

CAPÍTULO 1

TECNOLOGÍAS DE INFORMACIÓN (TI)

1.1 Las Tecnologías de Información (TI)

El concepto de Tecnología de Información es reciente surge de la agrupación de los siguientes elementos:

- Información pura (Conjunto organizado de datos que permite resolver problemas y tomar decisiones, su uso racional es la base del conocimiento).
- Tecnología (Concepto que abarca un conjunto de técnicas, conocimientos y procesos, que sirven para el diseño y construcción de objetos para satisfacer necesidades humanas).
- Comunicación (Implica la emisión de señales como sonidos, gestos, señas, etc. con la intención de dar a conocer un mensaje).

De ahí las siglas TI ó TIC referentes a Tecnología de Información y Tecnologías de Información y Comunicación respectivamente.

Las siguientes fechas indicadas cronológicamente muestran el rumbo del desarrollo de la Tecnología:

- 1705 - Primera máquina de vapor efectiva (Thomas Newcomen)
- 1768 - Nicholas Joseph Cugnot construye un vagón a vapor autopropulsado
- 1769 - James Watt mejora significativamente la máquina a vapor de Newcomen
- 1774 - Primera calculadora fabricada en serie (Philipp Matthäus Hahn)
- 1775 - Primer submarino (David Bushnell)
- 1780 - Invención de la prensa de copia (James Watt)
- 1785 - Se inventa el telar mecánico (Edmund Cartwright)
- 1793 - Telégrafo (Claude Chappe)
- 1800 - Primera batería (Alessandro Volta)
- 1804 - Primera locomotora a vapor (Richard Trevithick)
- 1810 - Prensa de impresión (Frederick Koenig)
- 1821 - Motor eléctrico (Michael Faraday)
- 1825 - Primera línea pública de ferrocarril en Inglaterra
- 1827 - Primera turbina de agua, y patente del primer propulsor para barcos Josef Ressel)
- 1854 - Invención de la bombilla incandescente (Heinrich Göbel)
- 1859 - Se desarrolla el motor a gas (Etienne Lenoir)
- 1861 - Primer teléfono funcionando (Johann Philipp Reis)
- 1875 - Invención del refrigerador (Carl von Linde)
- 1876 - Se patenta el uso del teléfono (Alexander Graham Bell)
  - Motor de cuatro tiempos (Nicolaus August Otto)
- 1877 - Invención del fonógrafo (Thomas Alva Edison)
- 1879 - Primera locomotora eléctrica (Werner von Siemens)
- 1881 - Abastecimiento de energía con corriente alterna de alta frecuencia (George Westinghouse)
- 1883 - Desarrollo de la turbina a vapor (Carl de Laval)
- 1886 - Primer automóvil (Karl Benz)

- 1895-Descubrimiento de los rayos X (Wilhelm Conrad Röntgen)
  - Invención del cinematógrafo (Auguste y Louis Jean Lumière)
- 1896 - Descubrimiento de la radioactividad (Antoine Henri Becquerel)
- 1897 -Invención del tubo de rayos catódicos (Karl Ferdinand Braun)
  - Diesel construye el motor diesel
- 1903 - Primer vuelo impulsado exitoso (Orville y Wilbur Wright)
- 1913 - Línea de ensamble para la producción automovilística (Henry Ford)
- 1930 - Primera turbina a gas para aeroplanos
- 1931 - Primer microscopio electrónico (Ernst Ruska)
- 1938 - Se divide el átomo del uranio (Otto Hahn y Fritz Straßmann)
- 1941 - "Z3", la primera computadora funcionando (Konrad Zuse)
- 1948 - Transistor (William B. Shockley, John Bardeen y Walter Brattain)
- 1954 - Primera central nuclear en Obninsk, cercana a Moscú
- 1955 - Fibra óptica (Narinder Singh Kapany, London)
- 1957 - Se lanza el primer satélite terrestre "Sputnik 1" (URSS)
- 1961 - Primer humano en el espacio y primera orbitación terrestre (Yuri Gagarin, URSS)
- 1964 - Circuitos integrados (Jack Kilby para Texas Instruments)
- 1969 - Primer descenso del hombre en la luna ("Apollo 11", USA)
- 1970 - Desarrollo del microprocesador (Intel)
  - Primera calculadora de bolsillo
- 1977 - Apple II, la primera computadora compacta
- 1979 - Disco compacto (CD) para almacenamiento digital de audio (Sony y Philips)
- 1981 - Primera computadora personal de IBM
- 1992 - Primer libro en CD-ROM (la Biblia)
- 1993 - Advenimiento del “Ancho mundo de la Internet” (World Wide Web)
- 1996 - Surgimiento de la memoria USB
- 2000 – Invento de la consola de videojuegos Play Station2
- 2002 – Adopción de redes inalámbricas en México y Publicación de la nueva ley de Ciencia y Tecnología
- 2003 –Desarrollo de la Web 2.0
- 2004 – Nace la primera red social: Facebook
- 2005 –Transmisión de televisión de alta definición en Europa y nace YouTube
- 2007 –Evolución paulatina a redes de fibra óptica
- 2008 – Cámaras fotográficas con sensor de movimiento
- 2009 – Lanzamiento de telefonía 3G en México, lectores de libros digitales.
- 2010 –En junio se concreta la 23 expedición a la Estación Espacial Internacional, telefonía 4G, proyecto NATAL, Televisores para visualizar en 3D.

La información se asocia junto con su tratamiento y su medio de transmisión; es decir, con la comunicación. La evolución de la información fue un proceso lento.

El camino de la información a grandes rasgos es el siguiente:

- Siglos V a X. Alta Edad Media: El almacenamiento, acceso y uso limitado de la información se realiza en las bibliotecas de los monasterios de forma manual.

- Siglo XII. Los Incas (Perú) usan un sistema de cuerdas para el registro de información numérica llamada Quipu, usado principalmente para contar ganado.

- Siglo XV. Edad Moderna: Con el nacimiento de la imprenta (Gutenberg), los libros comienzan a fabricarse en serie. Surgen los primeros periódicos.

- Siglo XX. 1926. Se inicia la primera retransmisión de televisión que afectará al manejo y tratamiento de la información con gran impacto en los métodos de comunicación social durante todo el siglo.

- Siglo XX. 1940. Jeremy Campbell, definió el término información desde una perspectiva científica, en el contexto de la era de la comunicación electrónica.

- Siglo XX.1943. El austro-húngaro Nikola Tesla inventa la radio, aunque inicialmente dicho invento se atribuye a Guglielmo Marconi y la patente no se reconoce a su autor hasta los años 1960.

- Siglo XX. 1947. En diciembre John Bardeen, Walter Houser Brattain y William Bradford Shockley, inventan el transistor. Serán galardonados por ello con el Premio Nobel de Física en 1956. Acaban de sentar sin saberlo la primera de las dos bases para una nueva revolución económica.

- Siglo XX.1948. Claude E. Shannon, elabora las bases matemáticas de la Teoría de la Información. Acaba de dar la segunda base de la revolución: la aplicación del Álgebra de Boole será el fundamento matemático para industrializar el procesamiento de la información. Nace así la Ciencia de la Computación o Ingeniería informática. La nueva revolución económica está preparada. La humanidad entra en la Era Digital usando el transistor y la numeración binaria para simbolizar la información.

- Siglo XX.1948. Norbert Wiener, elabora la idea de cibernética en su famosa obra: “Cibernética o el control y comunicación en animales y máquinas (Cybernetics or Control and Communication in the Animal and the Machine)” (1948) donde se encargó de "mantener el orden" en cualquier sistema natural o artificial de información.

- Siglo XX.1951-1953. James Watson y Francis Crick descubren los principios de los códigos de ADN, que forman un sistema de información a partir de la doble espiral de ADN y la forma en que trabajan los genes.

- Siglo XX. 1969. Nace la embrionaria Internet cuando se estable la primera conexión de computadoras, conocida como ARPANET, entre tres universidades en California y una en Utah, Estados Unidos.

- Siglo XXI, Hay proliferación de redes de transmisión de datos e información, de bases de datos con acceso en línea, ubicadas en cualquier lugar, localizables mediante Internet, permiten el hallazgo de otras redes y centros de información de diferentes tipos en cualquier momento desde cualquier lugar.

- Siglo XXI, Datos gestionados a través de aplicaciones informáticas donde los datos son procesados y transformados en información que posteriormente es manejada como signo integrador y característico de progreso económico del siglo XXI.

La comunicación surge con el hombre, su primera comunicación la hizo con su eco, posteriormente con sonidos en la edad de piedra se mandaban mensajes de humo otra forma de comunicarse muy primitiva fue cuando a los náufragos se les ocurrió enviar un recado escrito dentro de una botella para que con el movimiento de las olas ésta llegará a islas remotas para que alguien recogiera el mensaje.

Otro medio usado fueron las cartas incluso en la Biblia ya se habla de correos y en el imperio azteca en tiempos de Moctezuma, el emperador tenía personas dedicadas a llevar los recados y escritos que comunicaban el Golfo de México con la metrópoli a casi 500 km de distancia, la manera de avanzar tanta distancia se hacía mediante carrera de relevos había mensajeros a cierta distancia y se iban transmitiendo el mensaje.

Pero el servicio postal era lento comparado con la velocidad telegráfica fue Samuel Morse quien concibió la primera idea de un telégrafo electromagnético; el 13 de Octubre de 1832, pero sus señales viajaban sólo por tierra hasta que Guillermo Marconi en 1896, invento la telegrafía inalámbrica y envió el primer mensaje a través del Atlántico comunicando a América con Europa triunfo cumbre de la comunicación después del telégrafo inalámbrico; el mayor triunfo de la radio difusión fue cuando el físico norteamericano Lee De Forest inventó la lámpara aurion o bulbo en 1906, que convierte la electricidad en sonido de onda larga y onda corta, de esta última se logró transmitir para la televisión y con el mismo bulbo surgen las primeras computadoras y la comunicación mediante satélites.

1.2 Definición de Tecnologías de Información (TI)

La información de todo tipo es de vital importancia para cualquier situación e individuo. La información es todo aquello que responde a cualquier interrogante que se puede plantear (¿por qué?, ¿cómo?, ¿cuándo?, ¿dónde?, etc.) y relacionándolo con una situación definida.

Una tecnología es un medio que se requiere para mantener, producir, procesar y recuperar recursos. De acuerdo a su origen griego, está formado por *tekne* (**"arte, técnica u oficio"**) y por *logos* (**"conjunto de saberes"**). Se utiliza para definir a los conocimientos que permiten fabricar objetos y modificar el medio ambiente, con el objetivo de satisfacer las necesidades humanas.

Mientras que un sistema de información es un recurso el cual nos permite recuperación, control y diseminación de información.

Una **tecnología** de **información** será aquel sistema de información enfocado a las tecnologías que integran la información de una empresa, institución u organismo que realizan actividades con el fin de ofrecer un bien o servicio a una sociedad.

Para tener una buena base de tecnología de información se requiere un ciclo de actividades retroalimentadas las cuales se muestran de forma general en la figura 1.1.

FIGURA 1.1 Ciclo de vida de un Sistema de Información

Planificación: Se refiere a todas las acciones llevadas a cabo para realizar los procesos o las tareas en un sistema de información.

Recopilación y Análisis de requerimientos: Es la etapa donde se juntan e identifican todos los requerimientos o necesidades que van a condicionar a nuestro Sistema de Información (SI).

Diseño: Es el conjunto de bocetos, dibujos y diagramas que van a componer nuestro Sistema de Información (SI) entre los diseños más comunes están el de diagramas en Lenguaje Unificado de Modelado (UML), diagramas de flujo, gráficas, etc.

Prototipo: Es la pauta previa del SI definitivo, mediante éste se identifican posibles fisuras del SI.

Implantación: Es la puesta en marcha del prototipo que mejor se haya adecuado a nuestros requerimientos y si no presenta fisuras será el que se implanta. Finalmente el Mantenimiento es parte de toda la vida en el ciclo del SI pues es necesario y alimenta la calidad de todo el sistema en sí.

Los componentes básicos de una tecnología de información son:

- Hardware (Son todos los componentes físicos de una computadora como: Unidad Central de Proceso, teclado, impresora, monitor, etc.)
- Software (Es todo el conjunto intangible de datos y programas de la computadora)
- Consumibles o accesorios (Tintas, dvd´s, hojas, etc.)
- Información (Bases de datos, listas de registro, manuales, etc.)
- Personas
- Servicios (Consultoría, outsourcing, etc.)

1.3 Importancia de las Tecnologías de Información

Son actualmente los agentes más dinámicos de cambio, así como de innovación en la ciencia y la tecnología. Además, son estratégicas para los procesos de globalización y de competitividad, por lo que se requiere formar científicos e intermediarios tecnológicos y capacitar a los usuarios. El mercado global constantemente está cambiando, así que como manejadores de tecnologías de información se tiene que adaptar a los cambios, por ejemplo, si antes se solicitaba información mediante un giro postal y tardaba 3 días ahora se tiene que proporcionar esa misma información tal vez vía correo electrónico en el mismo día e incluso en menos de una hora; para ello se cuenta con la computadora e internet.

Debido a que se basan en el conjunto de disciplinas científicas básicas y aplicadas que estudian en lo general los procesos formales, en lo particular, la generación, procesamiento y empleo eficiente del conocimiento junto con la información, las tecnologías de información no son fijas la actualización es constante (dinámicos como ya se ha mencionado). El ser humano como ser pensante es el principal ejecutor para mantener en pie el funcionamiento de su empresa, institución u organismo que emplea las tecnologías de información como principal gestor.

Durante la Cumbre Mundial sobre la Sociedad de la Información celebrada en Túnez en 2005, se hizo un llamado a la Asamblea General de las Naciones Unidas para declarar el 17 de mayo como el Día Mundial de la Sociedad de la Información, estableciéndose así el Día Mundial de Internet.

Por lo anterior, el Instituto Nacional de Estadística y Geografía (INEGI), presenta un panorama general sobre el uso y aprovechamiento de Internet en los hogares y por los individuos, tomando como fuente la Encuesta Nacional sobre Disponibilidad y Uso de las Tecnologías de la Información en los Hogares.El INEGI detectó que en todos los sectores económicos existentes aquí en México se pueden utilizar las tecnologías de información sectores como: el sector agricultura, comercio, manufactura, transportes, servicios de diversa índole, etc. y diversos sectores que no tengan que ver con actividades del Gobierno hasta el Gobierno mismo (ver tabla 1.1).

El uso de las tecnologías de información ya es una parte vital de todos, constituyen una herramienta privilegiada para el desarrollo, contribuyen no sólo al mejoramiento social sino también al crecimiento económico de una nación. Durante el periodo 2001-2009 los hogares con Internet han crecido a una tasa media de 17 por ciento, mientras que el crecimiento de los

hogares con computadora fue del 13.2 por ciento (figura 1.3), el crecimiento de la televisión de paga fue del 11.5 por ciento en ese mismo periodo, mientras que el de la telefonía celular alcanzó el 16 por ciento para el periodo 2004-2009, es más, se usa computadora e internet desde los hogares para por ejemplo, comprar algo o simplemente navegar(figura 1.2).

Sector de actividad económica	Total	Emplea equipo de cómputo en procesos administrativos		Emplea internet en sus relaciones con clientes y proveedores		Emplea equipo de cómputo en procesos técnicos o de diseño		Desarrolla programas o paquetes informáticos para mejorar sus procesos	
		Si	No	Si	No	Si	No	Si	No
Total	3005157	371591	2633566	245496	2759661	186392	2818765	139037	2866120
Agricultura, ganadería, aprovechamiento forestal, pesca y caza	21 252	882	20 370	369	20 883	286	20 966	237	21 015
Minería	3 077	818	2 259	559	2 518	394	2 683	285	2 792
Electricidad, agua y suministro de gas por ductos al consumidor final	2 437	71	2 366	71	2 366	71	2 366	44	2 393
Construcción	13 444	10 708	2 736	8 006	5 438	8 905	4 539	3 664	9 780
Industrias manufactureras	328 718	40 576	288 142	30 398	298 320	28 561	300 157	16 185	312 533
Comercio al por mayor	86 997	38 881	48 116	27 757	59 240	15 437	71 560	14 222	72 775
Comercio al por menor	1493590	107345	1386245	65 540	1428050	41 919	1451671	38 941	1454649
Transportes, correos y almacenamiento	41 899	12 881	29 018	8 751	33 148	4 881	37 018	5 599	36 300
Información en medios masivos	7 586	5 312	2 274	4 643	2 943	4 538	3 048	3 055	4 531
Servicios financieros y de seguros	10 417	6 547	3 870	4 244	6 173	3 173	7 244	3 044	7 373
Servicios inmobiliarios y de alquiler de bienes muebles e intangibles	45 579	10 322	35 257	6 738	38 841	4 930	40 649	3 626	41 953
Servicios profesionales, científicos y técnicos	68 589	39 608	28 981	28 758	39 831	22 564	46 025	13 723	54 866
Dirección de corporativos y empresas	349	292	57	233	116	173	176	160	189
Servicios de apoyo a los negocios y manejo de desechos y servicios de remediación	43 152	21 716	21 436	18 886	24 266	14 109	29 043	9 713	33 439

Servicios educativos	30 891	14 785	16 106	7 355	23 536	8 499	22 392	6 183	24 708
Servicios de salud y de asistencia social	102 940	21 853	81 087	11 030	91 910	9 520	93 420	6 739	96 201
Servicios de esparcimiento culturales y deportivos, y otros servicios recreativos	31 790	2 693	29 097	1 680	30 110	1 336	30 454	974	30 816
Servicios de alojamiento temporal y de preparación de alimentos y bebidas	277 436	14 821	262 615	7 759	269 677	6 023	271 413	5 378	272 058
Otros servicios excepto actividades del Gobierno	395 014	21 480	373 534	12 719	382 295	11 073	383 941	7 265	387 749

NOTA: La clasificación del sector de actividad económica corresponde al Sistema de Clasificación Industrial de América del Norte (SCIAN)

TABLA 1.1 Sectores de México que usan las TI[1]

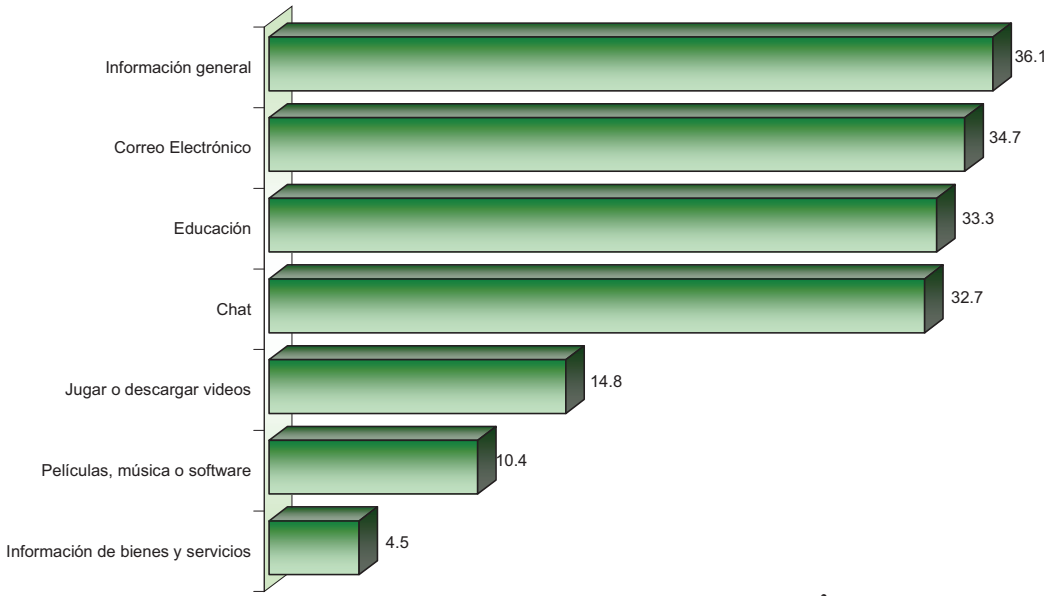


FIGURA 1.2 Proporción de usuarios de Internet por tipo de uso[2]

[1] FUENTE: INEGI. Módulo de innovación e investigación del Censo Económico Julio 2009.
[2] FUENTE: INEGI. Encuesta Nacional sobre Disponibilidad y Uso de las TI en los Hogares 2009.

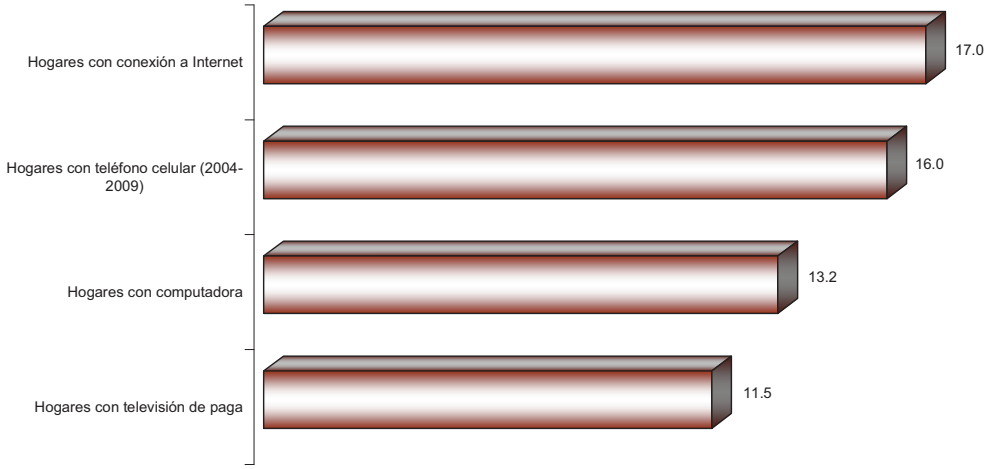


FIGURA 1.3 Tasa Media de Crecimiento Anual (TMCA) de las TI en los hogares 2001-2009 (%)[3]

1.3.1 Las Tecnologías de Información en México

México se ubica en el lugar número 39, en la lista de los 50 países que tienen habilidades para absorber y utilizar las tecnologías de información (TI), la penetración de las computadoras personales y el uso de Internet, la oferta mexicana en cuanto a tecnología, así como sus atributos es suficientemente competitiva como para encontrar un lugar entre las mejores propuestas del mundo.

Entre las empresas más importantes de esta industria en el país se encuentran: IBM, HP, Red Uno, Neoris, Unisys, Hildebrando, Softtek, Bursatek y Mexis.

En términos de industria, en México hay avances destacados en materia de calidad con programas como Modelo de Procesos para la Industria del Software (MoProsoft) y ahora México First, ambos parte de la Secretaría de Economía, además del fondo Programa para el Desarrollo de la Industria del Software (Prosoft) existen los fondos Pequeña y Mediana Empresa (PyMes).

La iniciativa MEXICO FIRST, la cual busca desarrollar suficiente capital humano especializado en el sector de TI en el país. En este programa se invertirán 40 millones de dólares en los próximos cinco años para certificar aproximadamente a 12 mil personas al año. Actualmente existen 121 universidades vinculadas con los apoyos del programa gubernamental Prosoft.

Las ventajas que ofrece México han permitido que el valor del mercado de servicios de Tecnologías de la Información incluyendo la tercerización de procesos de negocios (Bussiness Process Outsourcing o BPO por sus siglas en inglés) haya alcanzado 4 mil 200 millones de

[3] Vid pie de página 2

dólares en 2008, mientras que el mercado de software sumó 2 mil 400 millones de dólares en el mismo periodo, según Business Monitor[4].

De acuerdo con estimaciones de MéxicoIT[5], en nuestro país existen casi 600 mil profesionistas en la industria de TI, incluyendo aproximadamente 400 mil profesionistas especializados en software. Además, cada año se gradúan 65 mil nuevos profesionistas especializados en el sector; sólo el 1.5 por ciento de los profesionales que laboran en la industria de las Tecnologías de Información (TI), ha obtenido algún tipo de certificación, se estima que el 70% de las empresas prefieren contratar personal certificado, incluso con preferencia sobre los profesionistas con posgrado.

El mercado de los Servicios de TI y Software en el país ha presentado un crecimiento sostenido en los últimos años. Business Monitor estima que el mercado del sector alcanzará 10 mil 195 millones de dólares en 2013 (ver figura 1.4).

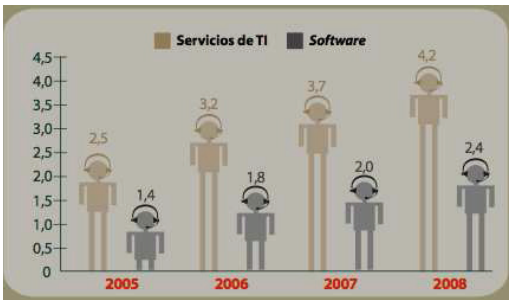


FIGURA 1.4 Crecimiento de servicios de TI y Software

Se estima que las exportaciones de servicios de TI en México alcanzaron un valor de 3 mil 164 millones de dólares durante 2008 (ver figura 1.5), lo que significó un crecimiento anual de 26 por ciento.

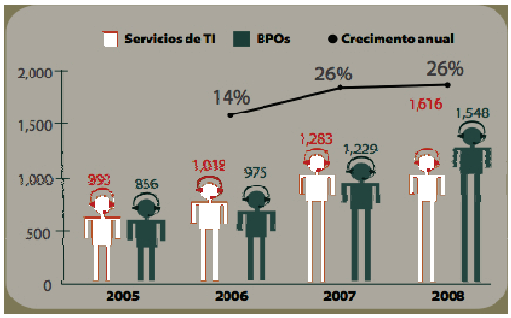


FIGURA 1.5 Exportaciones de Servicios TI y BPOs

[4] Proveedor líder independiente para informar mejor la toma de decisiones tiene presencia en 175 países y 22 sectores industriales.
[5] Es un programa que tiene por objetivo impulsar el crecimiento de la industria nacional de TI y promover su presencia en el mercado global.

El crecimiento de México en los próximos años es promisorio: Business Monitor estima que el mercado de servicios de TI y BPOs crecerá 10 por ciento anual en el periodo 2009-2013. Mientras que el mercado de software en México crecerá 9 por ciento anual en el mismo periodo.

El 77.3 por ciento de los cibernautas mexicanos tiene menos de 35 años, lo que significa que los jóvenes son quienes más uso hacen de la tecnología, la proporción de niños (6-11 años) que navegan en la red es de 8 por ciento (figura 1.6).

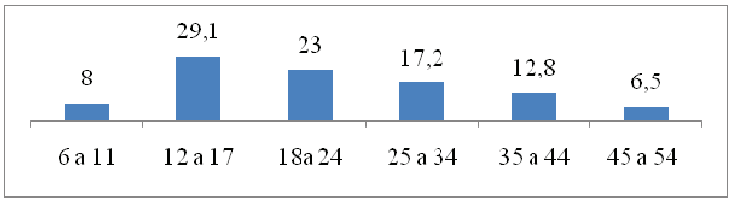


FIGURA 1.6 Proporción de usuarios de Internet por grupo de edad, 2009 (%)

Por otra parte, el comercio electrónico es poco recurrente entre los mexicanos, la proporción que realiza transacciones en línea es de 6.9 por ciento. En este sentido, de los usuarios que realizan transacciones electrónicas, 32.1% realiza sólo compras, 27.3% hace pagos, y 40.6% realizan ambos trámites.

En contraste con demás países de la Organización para la Cooperación y el Desarrollo Económico (OCDE[6]) el promedio de hogares con conexión a Internet en México es de 18.4 % y en general del 62 por ciento (ver figura 1.7), esto nos dice que el conocimiento sobre el acceso y aprovechamiento de las Tecnologías de la información en los diferentes sectores de la sociedad está muy por debajo del promedio y como tal no se ha aprovechado correctamente.

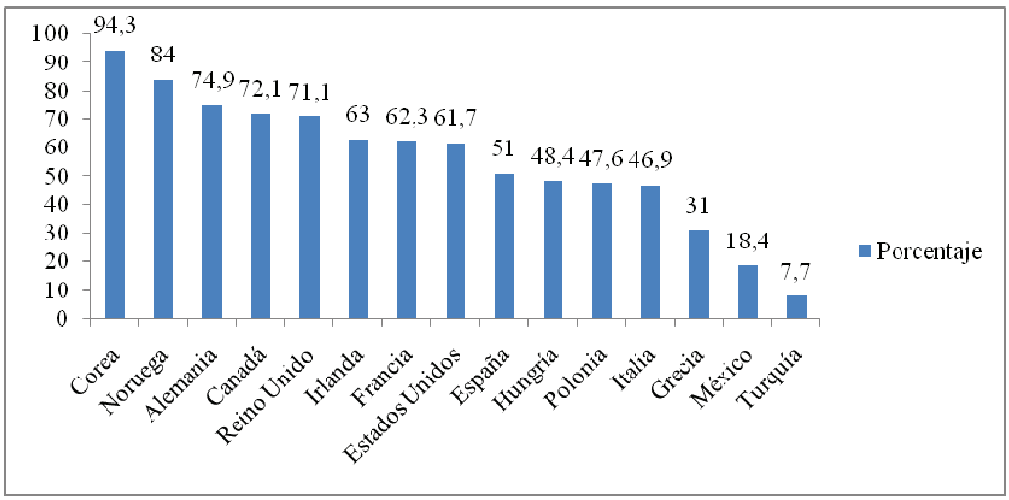


FIGURA 1.7 Proporción de hogares con conexión a internet de países de la OCDE, 2009 (%)

[6] Organización de cooperación internacional, cuyo objetivo es coordinar sus políticas económicas y sociales.

1.4 La Administración de Riesgos

La administración como tal juega un papel importante en cualquier ámbito ésta muy relacionada con los conceptos de liderazgo, comunicación y autoridad.

DEFINICIÓN

Administración: El arte de dirigir, administrar o gestionar es un conjunto de procesos que sirve para llegar a los objetivos de la institución.

Los procesos están interrelacionados y son mutuamente exclusivos (uno depende del otro y viceversa), se muestran en la siguiente figura.

FIGURA 1.5 Proceso de Administración

ADMINISTRAR ES →DIRIGIR ES →GUIAR

Elementos de la administración:

- El Jefe: Es aquel que tiene la función de dirigir.
- Los Dirigidos: Son a los que dirige el jefe.
- La Situación: Es el momento donde se lleva a cabo la dirección.
- Importancia: Estimula y dirige a las personas al logro de los objetivos propuestas o trabajo.

Elementos que se deben controlar en la administración de riesgos:

- Detección de fallas
- Diagnóstico del problema
- Darle la vuelta al problema y recuperación
- Resolución
- Seguimiento y control
- Seguridad

Estas son algunas actividades que se controlan entre otras. La administración de riesgos ayuda a proteger todos los bienes y derechos que tiene la empresa, institución u organismo (efectivo, propiedades, infraestructura, entre otros), definen estrategias que a partir de los recursos (físicos, humanos y financieros) busca, en el corto plazo minimizar las pérdidas ocasionadas por la ocurrencia de dichos riesgos y, en el largo plazo, cumplir con la misión y visión asignada. La administración de riesgos incluye por tanto:

- La investigación e identificación de las fuentes de riesgo
- La estimación de su probabilidad y evaluación de sus efectos
- La planificación de estrategias y procedimientos de control de riesgos
- La aplicación optimizadora de esas estrategias en presencia de incertidumbre

Habilidades y responsabilidades específicas para un administrador de tecnologías de información:

- Debe tener gran capacidad de liderazgo.
- Debe saber cómo establecer una visión del futuro y cómo se relaciona esta visión con las necesidades del negocio.
- Debe tener capacidades políticas.
- Debe tener capacidad de comunicación, incluyendo habilidades de escritura.
- Ser capaz de hablar de tecnología.
- Debe tener fuertes conocimientos financieros.
- Debe ser responsable ante la dirección del estado del proyecto.
- Debe responsabilizarse de realizar el seguimiento de los principales hitos del proyecto (tarea de duración cero que simboliza un logro o un punto-avance del proyecto).

A continuación se menciona a Henry Fayol como uno de los más reconocidos administradores y sus principios los cuales dieron el fundamento a la teoría de la administración de la actualidad.

PRINCIPIOS DE HENRY FAYOL DE LA ADMINISTRACIÓN

Henry Fayol: Ingeniero y teórico de la administración de empresas, es sobre todo conocido por sus aportaciones en el terreno del pensamiento administrativo. Expuso sus ideas en la obra *Administración industrial y general*, publicada en Francia en 1916.

FIGURA 1.6 Henry Fayol

Dichos principios son los siguientes:

1. **Principio de la autoridad –responsabilidad:** Los gerentes tienen que dar órdenes para que se hagan las cosas. Si bien la autoridad formal les da el derecho de mandar, los gerentes no siempre obtendrán obediencia, a menos que tengan también autoridad personal (Liderazgo).

2. **Principio de la disciplina:** Los miembros de una organización tienen que respetar las reglas y convenios que gobiernan la empresa. Esto será el resultado de un buen liderazgo en todos los niveles, de acuerdos equitativos (recompensar el rendimiento superior) y sanciones para las infracciones, aplicadas con justicia.

3. **Principio de la unidad de mando:** Cada empleado debe recibir instrucciones sobre una operación particular solamente de una persona.

4. **Principio de unidad de dirección:** Las operaciones que tienen un mismo objetivo deben ser dirigidas por un solo gerente que use un solo plan.

5. **Principio de la centralización–descentralización:** Fayol creía que los gerentes deben conservar la responsabilidad final pero también necesitan dar a su subalterna autoridad suficiente para que puedan realizar adecuadamente su oficio. El problema consiste en encontrar el mejor grado de centralización en cada caso.

6. **Principio de la equidad:** Los administradores deben ser amistosos y equitativos con sus subalternos.

7. **Principio de la iniciativa:** Debe darse a los subalternos libertades para concebir y llevar a cabo sus planes, aún cuando a veces se comentan errores.

8. **Principio de espíritu de equipo**: Hacer que todos trabajen dentro de la empresa con gusto y como si fueran un equipo, hace la fortaleza de una organización.

9. **Principio de subordinación de intereses particulares, a los intereses generales de la empresa:**

10. **Principio de jerarquía:** la jerarquía se representa mediante un organigrama desde la alta gerencia hasta los niveles más bajos de la empresa.

11. **Principio de división del trabajo:** Cuanto más se especialicen las personas, con mayor eficiencia desempeñarán su oficio.

12. **Principio de remuneración personal:** La compensación por el trabajo debe ser equitativa para los empleados como para los patrones.

13. **Principio de orden:** Los materiales y las personas deben estar en el lugar adecuado en el momento adecuado. En particular, cada individuo debe ocupar el cargo o posición más adecuados para él.

14. **Principio de estabilidad y duración del personal en un cargo:** Una alta tasa de rotación del personal no es conveniente para el eficiente funcionamiento de una organización.

Aplicando todos estos principios y controlando los elementos que se mencionan, el trabajo funcionará correctamente; las actividades que emanan de ello también, lo mejor de todo es que se puede ofrecer **CALIDAD**, la cual es el resultado de la administración eficiente, organizada, bien ejecutada y nos arroja beneficios como clientes, reconocimiento, satisfacción y recursos diversos (humanos y financieros).

CAPÍTULO 2

ANÁLISIS Y GESTIÓN DE RIESGOS EN LAS TECNOLOGÍAS DE INFORMACIÓN

2.1 Análisis de riesgo

Se cuentan con diversas definiciones pero se verá que todas ellas tienen elementos en común:

Definición 1: Es un paso importante para implementar la seguridad de la información, es realizado para detectar los riesgos a los cuales están sometidos los activos de una organización, es decir, para saber cuál es la probabilidad de que las amenazas se concreten.

Definición 2: Consiste en la identificación de peligros asociados a cada fase o etapa del trabajo y la posterior estimación de los riesgos teniendo en cuenta conjuntamente la probabilidad y las consecuencias en el caso de que el peligro se materialice.

Definición 3: También conocido como evaluación de riesgo o PHA[7] es el estudio de las causas de las posibles amenazas, y los daños y consecuencias que éstas puedan producir (¿Qué se quiere proteger?, ¿Contra quién o qué se debe proteger? y ¿Cómo se protegerá?).

Definición 4: Proceso por el cual se identifican las amenazas y vulnerabilidades de una organización, con el fin de generar controles que minimicen los efectos de los riesgos.

De las cuatro definiciones anteriores los elementos en común son: detectar, consecuencias, probabilidad y estudio, por lo tanto, uniéndolas podemos crear una definición propia.

Análisis de riesgo: Es el proceso en el que se identifican los riesgos, se crea una estimación de probabilidad, frecuencia y causas de cada riesgo, se realiza un análisis de consecuencias e impactos y como parte final se evalúan dichas consecuencias.

2.2 Esquema de análisis de riesgo

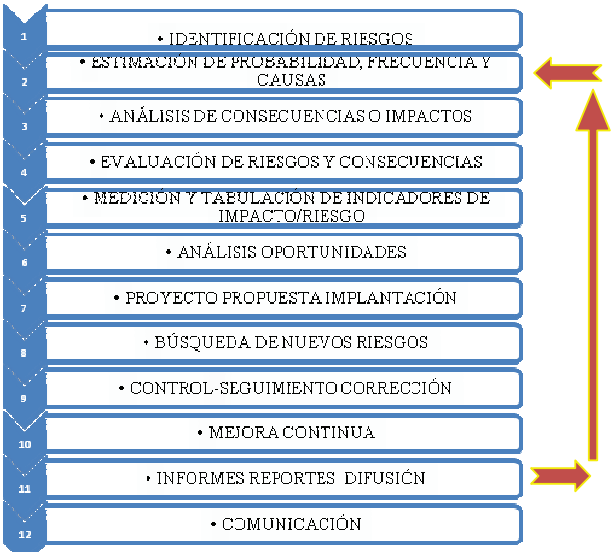


FIGURA 2.1 Esquema de análisis de riesgo

[7] Por sus siglas en inglés: Process Hazards Analysis (Proceso de Análisis de Peligros)

De la figura 2.1 se tiene la descripción de las primeras cuatro etapas que conforma al esquema de administración de riesgo, siendo estos la esencia del proceso; las demás etapas corresponden a procesos conocidos:

1. Identificación de riesgos

Se trata de conocer los riesgos que pueden afectar junto con las características las cuales acompañan a cada riesgo para determinar los recursos que se van a proteger.

Es una primera etapa del análisis de riesgo y como tal, la lista de riesgos identificados no siempre será la definitiva. Es una etapa muy flexible que forma parte de un proceso iterativo; es decir, si en un inicio no se consideró un riesgo que surgió después, éste se puede unir a la lista de los riesgos que se identificaron sin ningún problema, respetando así las etapas posteriores.

En esta etapa es muy recomendable la participación de todos los miembros del proyecto aunque comúnmente se hagan participes sólo a un gestor de riesgos, al líder o director de proyecto, en muy pocas ocasiones a los usuarios finales o los clientes. Cualquiera de las dos opciones parecería correcta, lo son, pero quién participa y con qué frecuencia siempre varía de un caso a otro.

2. Estimación de probabilidad, frecuencia y causas

Aclarando el concepto de probabilidad como el número de muestras del total de una población a estudiar, la frecuencia como el número de veces que se repite un evento en un determinado periodo de tiempo y las causas como cualquier variable la cual origina un efecto, así como las culpables en la cual, en la naturaleza no existan dos cosas completamente iguales, las variables son: medio ambiente, mano de obra, maquinaria, método, materia prima y manufactura.

Definidos los conceptos e identificados los riesgos, a cada uno, se le asigna mediante observación aleatoria y periódica su frecuencia, así como las causas que lo originan.

3. Análisis de consecuencias o impactos

Una herramienta estadística muy buena para apoyar esta etapa es el diagrama de Ishikawa o de espina de pescado también llamado diagrama de causa y efecto en honor a su creador japonés Kaoru Ishikawa[8], es una herramienta que relaciona causas y efectos (figura 2.3) generalmente, se acude a esta herramienta o a la elaboración de una lista simple (figura 2.2).

FIGURA 2.2 Lista simple

[8] 1915 – 1989 Teórico de la administración de empresas japonés, experto en el control de calidad.

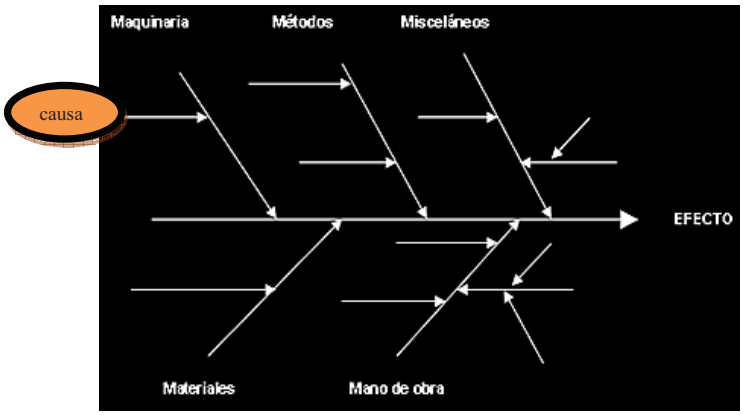


FIGURA 2.3 Diagrama de causa-efecto

4. Evaluación de riesgos y consecuencias

Para evaluar los riesgos se toma como referencia todas las posibles amenazas en función del ámbito o la forma en que se pueden producir o de una manera más fácil, tomando en cuenta todas las variables antes mencionadas: medio ambiente, mano de obra, maquinaria, método, materia prima y manufactura.

La identificación de amenazas, además requiere conocer los tipos de ataques, el tipo de acceso, la forma operacional y los objetivos del atacante. En general en las TI se cuenta con las siguientes amenazas identificadas:

- **Amenazas de imitación de identidad**

Cualquier actividad orientada a obtener acceso y utilizar, ilegalmente, la información de autenticación de otra persona, como pueden ser el nombre de usuario o la contraseña. Esta categoría incluye los ataques de intermediario y las comunicaciones de hosts de confianza con hosts que no son de confianza.

- Ataques de intermediario: Técnica común que utilizan los piratas informáticos. Esta técnica coloca un equipo entre dos equipos que se comunican en una conexión de red. Seguidamente, el equipo que está en medio suplanta a uno de los equipos originales o a ambos; la técnica proporciona al "intermediario" una conexión activa con los equipos originales y la capacidad de leer o modificar los mensajes conforme pasan entre ellos; mientras tanto, los usuarios de los equipos originales no perciben anomalía alguna en la comunicación(ver figura 2.4).

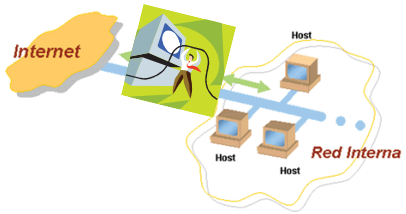


FIGURA 2.4 Ataques de Intermediario

- Comunicación de hosts de confianza con hosts que no son de confianza: Es engañar a un host de confianza para que "crea" que se está comunicando con otro host de confianza.

- **Denegación del servicio (DoS)**

Son ataques dirigidos contra un host o una red específica, estos ataques suelen enviar más tráfico a un host o enrutador del que puede gestionar en un tiempo determinado. Ello da como resultado la incapacidad de la red de gestionar el tráfico, por lo que el flujo legítimo de éste se ve interrumpido. Los ataques de denegación de servicio pueden estar distribuidos entre muchos atacantes que centran el esfuerzo en un objetivo en particular (DoS distribuido). Los equipos comprometidos se denominan zombies.

- **Distinción entre el tráfico estándar y el tráfico de un ataque**

En condiciones normales, los administradores de red pueden supervisar la mezcla de tráfico en la red y determinar las cantidades que son tráfico UDP (Protocolo de Datagramas de Usuario), tráfico TCP (Protocolo de Control de Transmisión), tráfico ICMP (Protocolo de Mensajes de Control de Internet), etc. se puede programar una directiva de estas características de forma predeterminada en los enrutadores, recopilar tendencias y estadísticas a largo plazo durante los períodos de actividad de red estándar y aplicar dichas estadísticas como colas ponderadas durante los períodos de gran congestión.

- **Divulgación de información**

Se da entre individuos que no deberían tener acceso a la misma, por ejemplo, usuarios que pueden leer archivos a los que no se les ha concedido acceso o los intrusos que leen datos en tránsito entre dos equipos. Las amenazas de esta categoría incluyen las conexiones no autorizadas y el espionaje de redes.

- Conexiones no autorizadas: Muchas configuraciones de red presentan una postura de seguridad muy confiada. Algunas directivas confían en simples comprobaciones de la dirección, pero los atacantes pueden eludir estas pruebas falsificando las direcciones. El acceso es a veces explícito (como con los servidores Web de intranet) y otras implícito, debido a la escasa protección de algunas aplicaciones.

- Espionaje de redes: Los atacantes intentan captar el tráfico de red por dos motivos: para obtener copias de archivos importantes durante su transmisión y lograr contraseñas que les permitan ampliar la penetración. En una red de difusión, los piratas informáticos utilizan herramientas de espionaje de redes para registrar las conexiones TCP y lograr copias de la información transmitida.

- **Elevación de privilegios**

En este tipo de amenazas, un usuario sin privilegios logra un acceso privilegiado que le permite poner en peligro o posiblemente destruir todo el entorno del sistema. Las amenazas de elevación de privilegios incluyen situaciones en las cuales el atacante ha superado de manera eficaz todas las defensas del sistema para explotar y dañar el sistema.

- **Gusanos y ataques de denegación de servicio**

Una forma de ataque de denegación de servicio es mediante gusanos cada uno de los equipos infectados efectúa cientos de miles de intentos de infección en objetivos indiscriminados, y el tráfico resultante invalida numerosas redes locales y hasta regionales dependiendo del dominio al que ataque.

- **Ingeniería social**

La ingeniería social es el acto de explotar las debilidades propias del comportamiento humano para lograr el acceso a un sistema u obtener más información sobre el mismo. Debido a que este tipo de ataque va dirigido al usuario del equipo, no hay herramientas ó aplicaciones que puedan proporcionar protección.

- **Manipulación de datos**

Relacionadas con la modificación malintencionada de los datos. Una amenaza específica de esta categoría es el secuestro de sesión.

  - Secuestro de sesión: Los atacantes pueden utilizar el secuestro de sesión para capturar una sesión, una vez que el usuario legítimo ha sido autenticado y autorizado ó incluso sin obtener las credenciales del usuario habitual. La manera más sencilla de secuestrar una sesión consiste, primeramente, en intentar la colocación del equipo del atacante en algún lugar de la ruta de conexión utilizando una herramienta de piratería especializada. El atacante observará el intercambio y, en algún momento, entrará en acción. Puesto que el atacante se encuentra en medio del intercambio, es capaz de finalizar uno de los lados de la conexión TCP y mantener el otro lado utilizando los parámetros TCP/IP (Protocolo de Control de Transmisión/Protocolo de Internet) y números de secuencia correctos.

- **Rechazo**

Asociados con usuarios que niegan haber ejecutado una acción, pero no existe forma alguna de probar lo contrario.

- **Seguridad de la aplicación**

Ataques que intentan explotar las vulnerabilidades existentes en las propias aplicaciones o en el sistema operativo.

- **Seguridad de red**

Una red como sistema de equipos interconectados, el acceso sencillo a ellas y la amplia disponibilidad de Internet han supuesto que muchos usuarios malintencionados centren sus esfuerzos en sistemas y servicios con el propósito de explotarlos o de provocar interrupciones.

- **Seguridad física**

La seguridad física implica proporcionar acceso físico a un sistema o recurso únicamente a la cantidad mínima de usuarios que lo necesitan. "La seguridad física es el nivel más bajo de defensa ante la mayoría de las amenazas a la seguridad de TI".

A pesar de ser el nivel bajo de defensa es el más importante porque si este nivel queda comprometido todos los niveles de seguridad quedan expuestos a las amenazas.

2.3 Tipos de riesgo

Un **riesgo** es la probabilidad de que suceda un evento, impacto o consecuencia adversos. Se entiende también como la medida de la posibilidad y magnitud de los impactos adversos, siendo la consecuencia del peligro, y está en relación con la frecuencia con que se presente el evento. No existe una clasificación formal de los riesgos, sin embargo, se puede abordar desde dos perspectivas una cualitativa y otra cuantitativa; así, dependiendo de los giros y tipo de nuestra empresa, institución u organismo del sector público ó privado realizamos una división imaginaria de todos nuestros activos[9].

Enfoque cualitativo

Son todos los recursos que son apreciados por sus cualidades o características, por ejemplo, seguridad, calidad, responsabilidades, etc. Lo más importante de este enfoque es priorizar los riesgos para realizar otros análisis o acciones posteriores, evaluando y combinando su probabilidad de ocurrencia y su impacto.

Enfoque cuantitativo

Son todos los recursos que son apreciados por sus capacidades, por ejemplo, el rendimiento, la frecuencia y el costo. Lo más importante de este enfoque es analizar numéricamente el efecto de los riesgos identificándose en los objetivos generales del proyecto.

Aunque de forma general se clasifican de la siguiente manera[10]:

- **Riesgos Físicos:** Ruido, presiones, temperatura, iluminación, vibraciones, radiación Ionizante y no Ionizante, temperaturas extremas ya sea frío o calor, y radiación infrarroja y ultravioleta.

[9] Activo es cualquier elemento importante para nuestra empresa, institución u organismo
[10] Para una definición específica de cada riesgo ver el glosario

- **Riesgos Químicos**: Polvos, vapores, líquidos y disolventes.
- **Riesgos Biológicos:** Anquilostomiasis, carbunco, alergias, muermo, tétanos, espiroquetosis, icterohemorrágica y psicosociales como el stress.

De forma general en TI tenemos los siguientes riesgos agrupados por las categorías, mostradas abajo:

- Riesgo de la estructura / proceso: estimaciones, costo, fuentes, etc.
- Riesgo de tecnología: Hardware, software y red.
- Riesgo de mercado: Proveedores, flujo de dinero y competidores.
- Riesgo financiero: equipo de apoyo, soporte de usuario y ejecutivo.
- Riesgo de personal: capacitación, comunicación y control.

2.4 Gestión de riesgo

Para poder gestionar o administrar algo siempre se parte de un antecedente o conocimiento previo, éste antecedente no lo proporciona el análisis de riesgo y se complementa con otras etapas para tener una gestión completa.

La **gestión de riesgo** consiste en dotar primero el análisis de riesgo, se procede a definir los objetivos a seguir o cambiar, se desarrollan alternativas y se asignan prioridades para ir aplicando durante o antes de cada etapa del proyecto en curso. La identificación, análisis, evaluación, tratamiento y seguimiento del riesgo es un proceso muy complejo que requiere además de tiempo, costo y recursos.

El objetivo principal de la gestión de riesgo es disminuir la probabilidad y el impacto de eventos adversos a la empresa, negocio y/o institución.

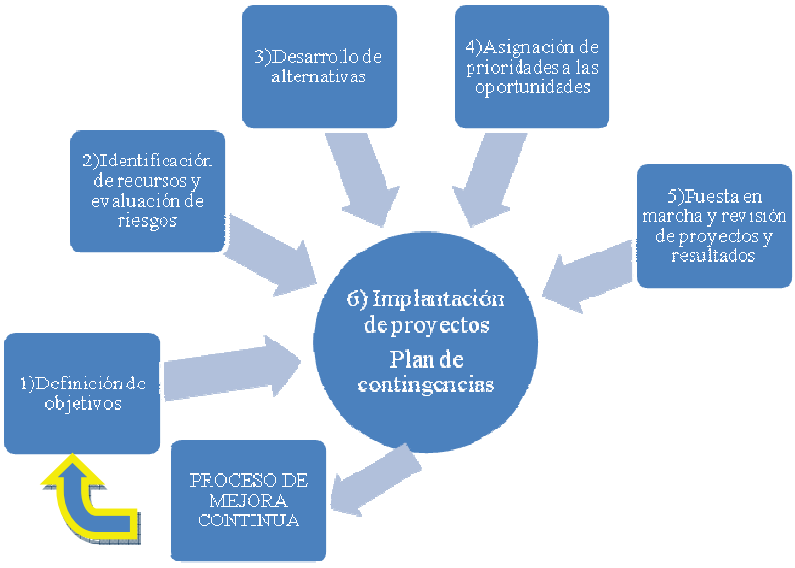


FIGURA 2.5 Esquema de administración de riesgo

1. Definición de objetivos

Se tiene que definir y redactar en un documento visible al público:

- Objetivo institucional, social y/o empresarial (misión): Es el motivo de la existencia y detalla la orientación de las actividades. En otras palabras, representa la razón de ser además de orientar su **planificación**.

- Metas institucional, social y/o empresarial (visión): Definen y describen la situación futura que desea tener la empresa, el propósito de la visión o metas es guiar, controlar y alentar en conjunto para alcanzar el estado deseable de la organización.

- Límites: Objetivos de la empresa, son los que forjaran los valores a seguir por su empresa y el móvil de todas sus acciones.

2. Identificación de recursos y evaluación de riesgos

Los recursos a identificar son los siguientes:

- Financieros: Dinero, préstamos, acciones, etc.
- Administrativos: Material de oficina, oficios, firmas, información, etc.
- Ecológicos: Cultura del agua, área verdes, extinguidores, etc.
- Público: Sanitarios, asientos, información, etc.
- Trabajador: Experiencia, creatividad, conocimiento, etc.
- Técnico: Patentes, marcas, manuales, etc.
- Externos: Capacitación, cursos, visitas, etc.
- De la organización: Clientes, empleados, supervisores, normas, etc.
- Mercado: Cotizaciones de dinero, manejo de dólar, publicidad, etc.
- Cliente: Preferencia, rechazo, venta, compra, etc.

Luego de identificar los recursos a estudiar se determinan y evalúan que riesgos pueden afectar al proyecto y se documentan sus características. La siguiente etapa consiste en enfrentar el riesgo.

3. Desarrollo de alternativas (formas de enfrentar el riesgo)

Se tiene al alcance diversas formas de enfrentar un riesgo, todas ellas dependen en sí de la(s) características de cada riesgo.

- Comunicar (Informar al responsable del estado del riesgo).
- Impulsar (Dejar que el riesgo siga su proceso natural y no intervenir).
- Reciclar (Documentar el tratamiento del riesgo y reutilizar en otra ocasión similar).
- Responder (Aplicar las medidas pertinentes al riesgo).
- Reducir (Disminuir la magnitud del riesgo).
- Eliminar (Desaparecer completamente el riesgo del registro de incidencias).

- Reutilizar (Usar el riesgo como base para poder enfrentar otros riesgos que dependan de él).
- Magnitud (Se aumenta o disminuye la magnitud del riesgo, si es oportunidad se trata de aumentar la magnitud del mismo en caso contrario, se intenta disminuirla).
- Posibilidad (Determinar si el riesgo va a aparecer o eliminarlo).
- Aceptar (Conseguir el máximo beneficio posible de este riesgo positivo).

4. Asignación de prioridades a las oportunidades

No todos los riesgos suelen ser amenazas, en algunos casos se puede representar como un área de oportunidad, la cual es conocida como riesgo positivo, lo que se suele hacer en este caso es eliminar o aceptar el riesgo considerando los siguientes aspectos que variaran de un proyecto a otro.

- Costo estimado (Hacer un cálculo de costo aproximado).
- Costo-beneficio (Hacer un cálculo de costo-beneficio aproximado; es decir, lo que cuesta y lo que beneficia).
- Criterios de umbral (Verificar que los riesgos no rebasen nunca ningún nivel permitido, el cuál es definido por nosotros).
- Estimación de beneficios (Documentar que recursos o impactos se obtienen por cada riesgo).
- Estimación de movimientos (Documentar que alternativa(s) se adoptan por cada riesgo).

5. Puesta en marcha y revisión de proyectos y resultados

Los rubros a considerar para concluir esta etapa son:

- Asignación de recursos: Es destinar los recursos a cada etapa del proyecto.
- Programas: Se debe asignar a cada responsable un actividad.
- Puntos clave: Se debe de formular un reglamento, responsabilidades a los responsables de los programas y con esto ir conformando una guía de administrar riesgos.
- Revisión independiente: Independientemente de los resultados obtenidos se tiene que hacer una revisión de consecuencias surgida de haber aplicado cada tratamiento y documentarlas.

Al identificar todos los recursos a proteger, así como las posibles vulnerabilidades, amenazas a que se exponen y los potenciales atacantes los cuales, pueden intentar violar la seguridad, se estudiará cómo proteger los sistemas, sin ofrecer aún implementaciones concretas para protegerlos (esto ya no serían políticas sino mecanismos). Esto implica en primer lugar cuantificar los daños que cada posible vulnerabilidad puede causar teniendo en cuenta las posibilidades de que una amenaza se pueda convertir en realidad. Este cálculo puede realizarse partiendo de hechos sucedidos con anterioridad en la organización, aunque por desgracia en muchos lugares no se suelen registrar los incidentes acaecidos. En este caso, a la hora de evaluar los daños sobre recursos intangibles, existen diversas aproximaciones como el método Delphi (básicamente consiste en preguntar a una serie de especialistas de la organización sobre el daño y las pérdidas que cierto problema puede causar); no obstante, la experiencia del

administrador o experto en materias de seguridad suele tener aquí la última palabra a la hora de evaluar los impactos de cada amenaza, sin embargo, todas las opiniones son válidas y aceptables.

La clasificación de riesgos de cara a estudiar medidas de protección se obtienen en base al nivel de importancia del daño causado y a la probabilidad aproximada de que ese daño se convierta en realidad; los recursos que presenten un riesgo evaluado mayor deberán tener mayores medidas de protección, esto significa que es probable que son más propensos a ser atacados, además el ataque puede causar pérdidas importantes.

Una vez que se conoce el riesgo evaluado de cada recurso es necesario efectuar el **análisis de costo y beneficio**. El cual consiste en comparar el costo asociado a cada problema (calculado anteriormente) con el costo de prevenir dicho problema. El cálculo de este último no suele ser complejo, si se conocen las posibles medidas de prevención que se tienen a nuestra disposición. No sólo se tiene que tomar en cuenta el costo de cierta protección, sino también su implementación y su mantenimiento. Cuando ya se ha realizado este análisis se tiene que presentar cuentas a los responsables de la organización (o adecuarlas al presupuesto que un departamento destina a materias de seguridad), siempre teniendo en cuenta que el gasto de proteger un recurso ante una amenaza, ha de ser inferior al gasto que se produciría si la amenaza se convirtiera en realidad. Se debe tener siempre presente que los riesgos se pueden minimizar, pero *nunca* eliminarlos completamente, por lo que es recomendable también planificar la recuperación de un problema; en el mundo de las TI se habla de medidas:

- **Proactivas:** Son aquellas que se toman para prevenir un problema.
- **Reactivas:** Son aquellas que se toman cuando el daño se produce, para minimizar sus efectos.

6. Mejora continua, Plan de Contingencias e Implantación de proyectos

Todas las acciones recurrentes que se hacen para aumentar la capacidad de cumplir los requisitos pertenecen al proceso de mejora continua, el plan de contingencias Es la parte del sistema general de la organización, define la política de prevención e incluye la estructura organizativa, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos para llevara a cabo dicha política.

Se debe hacer una evaluación formal, por parte de la dirección, del estado, de la adecuación del plan de contingencias y la implantación del proyecto en relación con la política de prevención de riesgos que se definió en la etapa de definición de objetivos.

CAPÍTULO 3

MÉTODOS PARA EL ANÁLISIS Y GETIÓN DE RIESGOS

3.1 Introducción

Método es una palabra que proviene del término griego methodos ("camino" o "vía") y que se refiere al medio utilizado para llegar a un fin. Su significado original señala el camino que conduce a un lugar. Para el análisis y gestión de riesgos se cuenta con diversos métodos, los más usados por grandes sectores que manejan TI son: **MAGERIT, CRAMM, MARION, MELISA, MOSLER, ITIL, COBIT.**

MAGERIT: 1996, España, Ministerio de Administraciones Públicas.	**CRAMM:** 1985, Reino Unido, Agencia Central de Computación y Telecomunicaciones del Gobierno del Reino Unido.	**MARION:** 1985, Francia, Asociación de Empresas Aseguradoras Francesas (CLUSIF).	**MEHARI:**1996, Francia, sucesor de MELISA Y MARION
MELISA: 1984, Francia, origen militar.	**MOSLER:** datos desconocidos	**ITIL:** 1980, Reino Unido, origen gobierno.	**COBIT:** 1996, Auditoría de Sistemas de Información y Control Asociación y el IT Instituto de Gobierno.

TABLA 3.1 Métodos para el análisis y gestión de riesgos: año de origen, país de origen y encargado del método o fundador

3.2 Principales métodos para el análisis y gestión de riesgos

3.2.1 MAGERIT

MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) promovida por el Consejo Superior de Informática de España para el Ministerio de Administraciones Públicas, surge como respuesta a la dependencia de las tecnologías de información, tiene un objetivo doble: estudiar los riesgos que soporta un determinado Sistema de Información y recomendar las medidas apropiadas para dichos riesgos.

PASOS DEL MÉTODO PARA EL ANÁLISIS DE RIESGOS

1)Identificación de activos
2)Dependencias
3)Valoración
4)Caracterización de las amenazas
5)Estimación de impacto y riesgo
6)Caracterización de los salvaguardas
7)Estimación del estado de riesgo

1) Identificación de activos

Se denominan **activos** a los recursos del sistema de información o relacionados con éste, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección. MAGERIT clasifica los activos dentro de una jerarquía, determinando para cada uno un código que refleja su posición jerárquica, un nombre y una breve descripción de las características, un activo puede ser simultáneamente de varios tipos.

No todos los activos son de la misma especie. Dependiendo del tipo de activo, las amenazas y las salvaguardas son diferentes. El **activo esencial** o más importante es la **información** que maneja el sistema; o sea los datos. Y alrededor de estos datos se pueden identificar otros activos relevantes:

- Servicios [S]: Se pueden prestar gracias a aquellos datos, y los servicios que se necesitan para poder gestionar dichos datos.
- Datos / Información [D]: Son el corazón que permite a una organización prestar sus servicios.
- Aplicaciones *(software)* [SW]*:* Permiten manejar los datos.
- Equipos informáticos *(hardware)* [HW]: Permiten hospedar datos, aplicaciones y servicios.
- Redes de comunicaciones [COM]: Permiten intercambiar datos.
- Soportes de información [SI]: Son dispositivos de almacenamiento de datos.
- Equipamiento auxiliar [AUX]: Complementa el material informático.
- Instalaciones [L]: Donde se guardan equipos informáticos y de comunicaciones.
- Personal [P]: Explotan u operan todos los elementos anteriormente citados.

2) Dependencias

Se dice que un **"activo superior"** depende de otro **"activo inferior"** cuando las necesidades de seguridad del superior se reflejan en las necesidades de seguridad del inferior. O, dicho en otras palabras, cuando la materialización de una amenaza en el activo inferior tiene como consecuencia un perjuicio sobre el activo superior. A continuación en la figura 3.1 se muestra un esquema para ayudar a la identificación de activos.

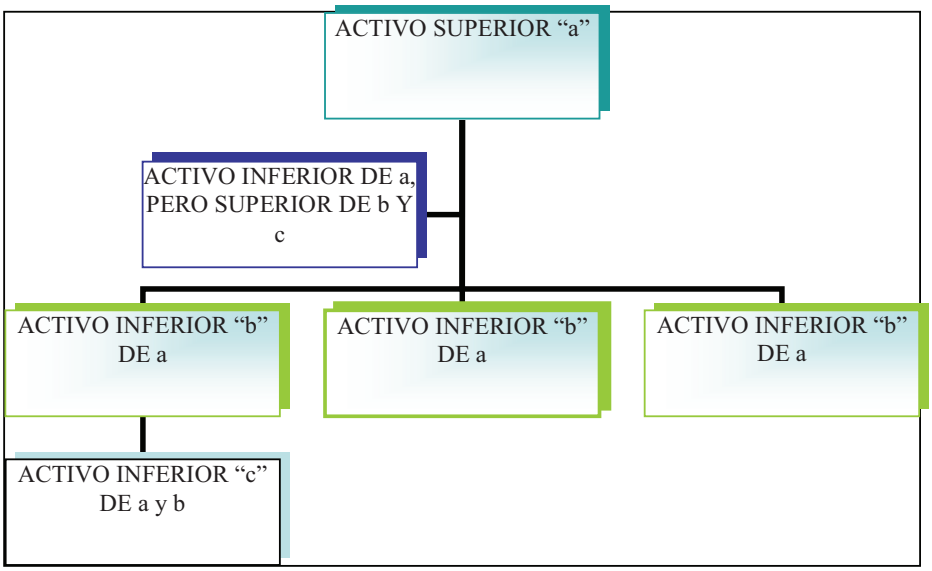


FIGURA 3.1 Activos superiores e inferiores

EJEMPLO: Se tienen los siguientes activos identificados y su tabla de dependencias (Figuras 3.2 y Tabla 3.2 respectivamente)

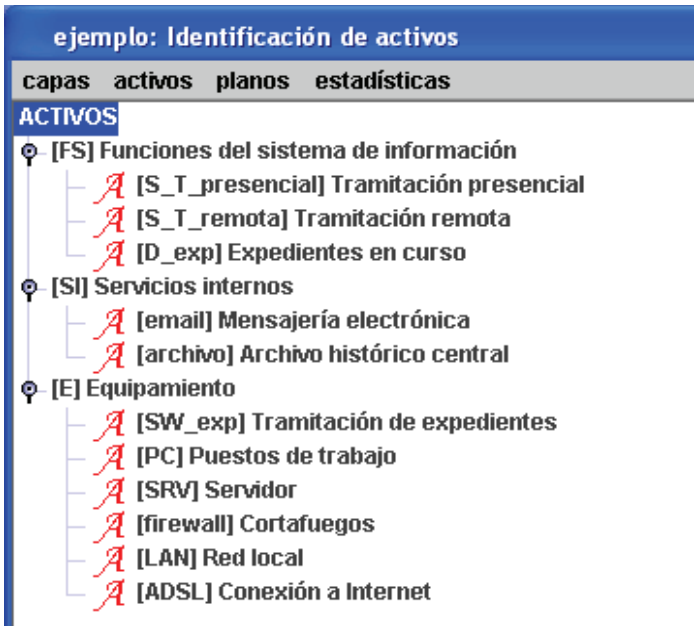


FIGURA 3.2 Identificación de activos

	[S_T_presencial]	[S_T_remota]	[D_exp]	[email]	[archivo]	[SW_exp]	[PC]	[SRV]	[firewall]	[LAN]	[ADSL]
[S_T_presencial]			√	√	√	√	√	√		√	
[S_T_remota]			√	√	√	√		√	√	√	√
[D_exp]					√	√	√	√		√	
[email]								√	√	√	√
[archivo]								√	√		√
[SW_exp]											
[PC]											
[SRV]											
[firewall]											
[LAN]											
[ADSL]											

TABLA 3.2 Tabla de dependencias

Para el caso de los datos de expedientes en curso, el gráfico de dependencias se muestra en la figura 3.3, de acuerdo al gráfico de dependencias se cuenta con dos activos superiores y 7 activos inferiores.

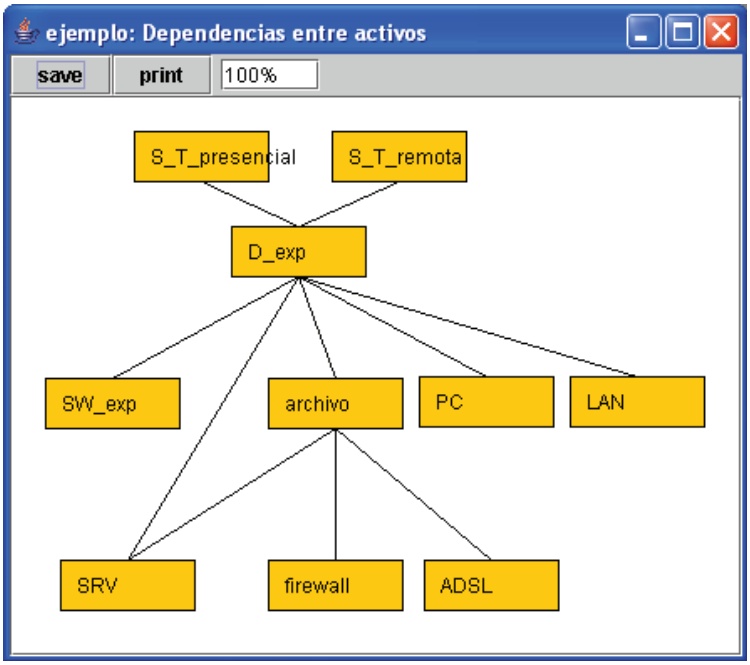


FIGURA 3.3 Dependencias entre activos

El activo superior de datos de expedientes en curso [D_exp] son: Tramitación presencial y tramitación remota [S_T_Presencial] y [S_T_remota] respectivamente y uno de sus activos inferiores es: el [firewall] (cortafuegos).

3) Valoración

Un activo interesa por lo que vale (no propiamente dicho), el valor puede ser propio (el que se le asigna a un activo superior) o acumulado. Se dice que los activos inferiores en un esquema de dependencias, acumulan el valor de los activos que se apoyan en ellos, esto es el valor acumulado; es decir, es la suma de los valores de todos los activos superiores al activo de interés.

EJEMPLO: En la tabla 3.3 tenemos unos activos con su correspondiente valor propio:

Activo	[D]	[I]	[C]	[A_S]	[A_D]	[T_S]	[T_D]
[S_T_presencial] Tramitación presencial	[5]			[7]		[6]	
[S_T_remota] Tramitación remota	[3]			[7]		[6]	
[D_exp] Expedientes en curso		[5]	[6]		[5]		[5]

TABLA 3.3 Valor propio de los activos superiores

La valoración la realiza el responsable de gestión de riesgos de acuerdo a todos los criterios que se establecen en etapas iniciales al proyecto. El valor acumulado que se obtiene de cada activo que depende del activo datos de expedientes en curso se desglosa en la tabla 3.4.

	dimensiones de seguridad						
activo	[D]	[I]	[C]	[A_S]	[A_D]	[T_S]	[T_D]
[S_T_presencial] Tramitación presencial	[5]			[7]		[6]	
[S_T_remota] Tramitación remota	[3]			[7]		[6]	
[D_exp] Expedientes en curso	[5]	[5]	[6]	[7]	[5]	[6]	[5]
[email] Mensajería electrónica	[5]			[7]		[6]	
[archivo] Archivo histórico central	[5]	[5]	[6]	[7]	[5]	[6]	[5]
[SW_exp] Tramitación de expedientes	[5]	[5]	[6]	[7]	[5]	[6]	[5]
[PC] Puestos de trabajo	[5]	[5]	[6]	[7]	[5]	[6]	[5]
[SRV] Servidor	[5]	[5]	[6]	[7]	[5]	[6]	[5]
[firewall] Cortafuegos	[5]	[5]	[6]	[7]	[5]	[6]	[5]
[LAN] Red local	[5]	[5]	[6]	[7]	[5]	[6]	[5]
[ADSL] Conexión a Internet	[5]	[5]	[6]	[7]	[5]	[6]	[5]

TABLA 3.4 Valor acumulado de los activos

4) Caracterización de las amenazas

Amenaza: Cualquier factor que afecte el desempeño adecuado de la organización es considerado una amenaza, muchas amenazas se deben a errores y ataques.

Ataque: Método por el cual un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático. Los ataques son deliberados o no intencionados.

Una amenaza puede concretarse en un ataque.

La caracterización de las amenazas lleva a realizar una correcta y rápida estimación de riesgo e impacto; las amenazas que MAGERIT identifica son:

- Por desastres naturales (Temblor, inundación, etc.).
- De origen industrial (Derrame químico, falla de maquinaria, etc.).
- Errores y fallos no intencionados (Derrame de líquidos, accidentes, incendios, etc.).
- Ataques intencionados (Robo de información, peleas, virus, etc.).
- Correlaciones de errores y ataques
    - Amenazas que sólo pueden ser errores, nunca ataques deliberados
    - Amenazas que nunca son errores: siempre son ataques deliberados
    - Amenazas que pueden producirse tanto por error como deliberadamente

5) Estimación de impacto y riesgo

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza.

- Impacto acumulado: Es el calculado sobre un activo teniendo en cuenta:
  - Su valor acumulado (el propio mas el acumulado de los activos que dependen de él) y
  - Las amenazas a que está expuesto (ver figura 3.4)

ejemplo: impacto acumulado

activo	D	I	C	A_S	A_D	T_S	T_D
ACTIVOS							
[FS] Funciones del sistema de información							
[S_T_presencial] Tramitación presencial	[4]			[7]		[6]	
[S_T_remota] Tramitación remota	[2]			[7]		[6]	
[D_exp] Expedientes en curso	[4]	[4]	[6]	[7]	[5]	[6]	[5]
[SI] Servicios internos							
[email] Mensajería electrónica	[4]			[7]		[6]	
[archivo] Archivo histórico central	[5]	[4]	[5]	[7]	[5]	[6]	[5]
[E] Equipamiento							
[SW_exp] Tramitación de expedientes	[5]	[5]	[6]	[7]	[5]	[6]	[5]
[PC] Puestos de trabajo	[5]	[2]	[5]	[6]	[2]	[6]	[5]
[SRV] Servidor	[5]	[2]	[5]	[6]	[2]	[6]	[5]
[firewall] Cortafuegos	[5]	[2]	[5]	[6]	[2]	[6]	[5]
[LAN] Red local	[5]	[2]	[6]	[7]	[5]	[6]	[5]
[ADSL] Conexión a Internet	[2]	[2]	[5]	[7]	[5]	[6]	[5]

3 exporta

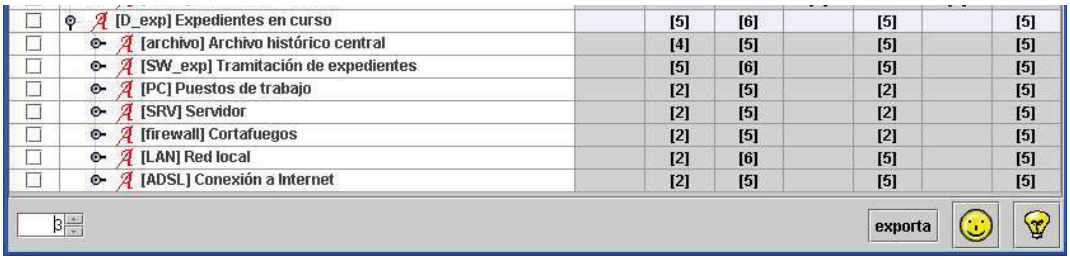
FIGURA 3.4 Impacto acumulado

- Impacto repercutido: Es el calculado sobre un activo teniendo en cuenta:
  - Su valor propio y
  - Las amenazas a que están expuestos los activos de los que depende (ver figura 3.5 a y b)

ejemplo: impacto repercutido

activo	D	I	C	A_S	A_D	T_S	T_D
ACTIVOS							
[S_T_presencial] Tramitación presencial	[5]			[7]		[6]	
[D_exp] Expedientes en curso	[4]			[7]		[6]	
[email] Mensajería electrónica	[4]			[7]		[6]	
[archivo] Archivo histórico central	[5]			[7]		[6]	
[SW_exp] Tramitación de expedientes	[5]			[7]		[6]	
[PC] Puestos de trabajo	[5]			[6]		[6]	
[SRV] Servidor	[5]			[6]		[6]	
[firewall] Cortafuegos	[5]			[6]		[6]	
[LAN] Red local	[5]			[7]		[6]	
[ADSL] Conexión a Internet	[2]			[7]		[6]	
[S_T_remota] Tramitación remota	[3]			[7]		[6]	
[D_exp] Expedientes en curso	[2]			[7]		[6]	
[email] Mensajería electrónica	[2]			[7]		[6]	
[archivo] Archivo histórico central	[3]			[7]		[6]	
[SW_exp] Tramitación de expedientes	[3]			[7]		[6]	
[PC] Puestos de trabajo	[3]			[6]		[6]	
[SRV] Servidor	[3]			[6]		[6]	
[firewall] Cortafuegos	[3]			[6]		[6]	
[LAN] Red local	[3]			[7]		[6]	
[ADSL] Conexión a Internet				[7]		[6]	

FIGURA 3.5 a Impacto repercutido



[D_exp] Expedientes en curso		[5]	[6]		[5]		[5]
[archivo] Archivo histórico central		[4]	[5]		[5]		[5]
[SW_exp] Tramitación de expedientes		[5]	[6]		[5]		[5]
[PC] Puestos de trabajo		[2]	[5]		[2]		[5]
[SRV] Servidor		[2]	[5]		[2]		[5]
[firewall] Cortafuegos		[2]	[5]		[2]		[5]
[LAN] Red local		[2]	[6]		[5]		[5]
[ADSL] Conexión a Internet		[2]	[5]		[5]		[5]

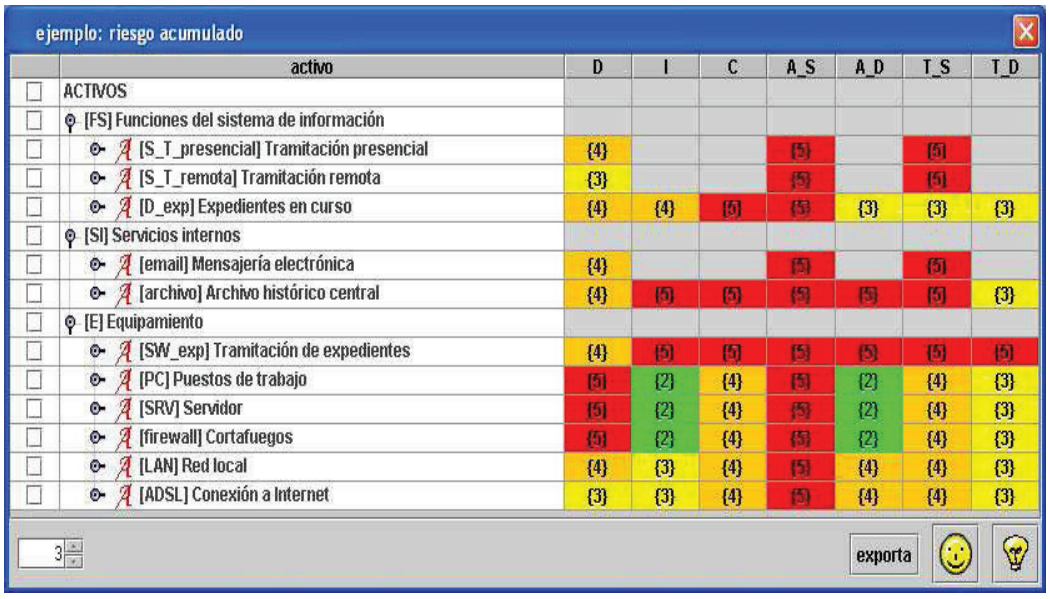
b exporta

FIGURA 3.5 b continuación Impacto repercutido

El **impacto repercutido** se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio y de la degradación causada. Al calcularse sobre los activos que tienen valor propio, permite determinar las consecuencias de las incidencias técnicas sobre la misión del sistema de información, ayuda a tomar una de las decisiones críticas de un análisis de riesgos: aceptar un cierto nivel de riesgo.

Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la frecuencia de ocurrencia. El riesgo crece con el impacto y con la frecuencia.

- Riesgo acumulado: Es el calculado sobre un activo teniendo en cuenta:
  - El impacto acumulado sobre un activo debido a una amenaza y
  - La frecuencia de la amenaza (ver figura 3.6)



ejemplo: riesgo acumulado

activo	D	I	C	A_S	A_D	T_S	T_D
ACTIVOS							
[FS] Funciones del sistema de información							
[S_T_presencial] Tramitación presencial	{4}			{5}		{5}	
[S_T_remota] Tramitación remota	{3}			{5}		{5}	
[D_exp] Expedientes en curso	{4}	{4}	{5}	{5}	{3}	{3}	{3}
[SI] Servicios internos							
[email] Mensajería electrónica	{4}			{5}		{5}	
[archivo] Archivo histórico central	{4}	{5}	{5}	{5}	{5}	{5}	{3}
[E] Equipamiento							
[SW_exp] Tramitación de expedientes	{4}	{5}	{5}	{5}	{5}	{5}	{5}
[PC] Puestos de trabajo	{5}	{2}	{4}	{5}	{2}	{4}	{3}
[SRV] Servidor	{5}	{2}	{4}	{5}	{2}	{4}	{3}
[firewall] Cortafuegos	{5}	{2}	{4}	{5}	{2}	{4}	{3}
[LAN] Red local	{4}	{3}	{4}	{5}	{4}	{4}	{3}
[ADSL] Conexión a Internet	{3}	{3}	{4}	{5}	{4}	{4}	{3}

3 exporta

FIGURA 3.6 Riesgo acumulado

- Riesgo repercutido: Es el calculado sobre un activo teniendo en cuenta:
    - El impacto repercutido sobre un activo debido a una amenaza y
    - La frecuencia de la amenaza (ver figura 3.7)

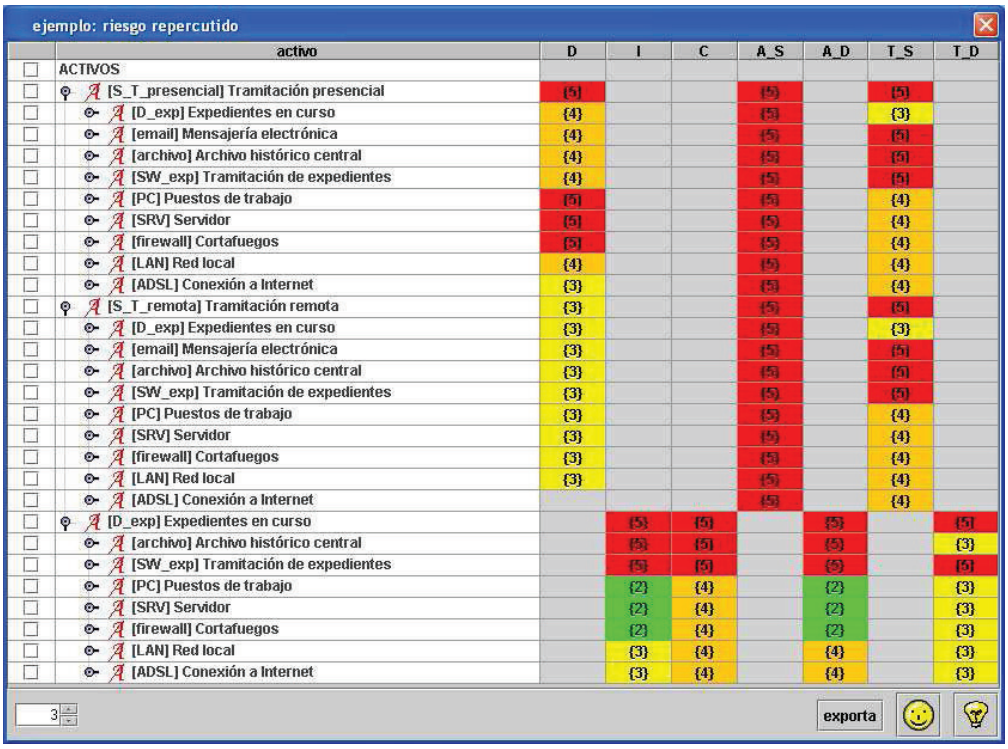


FIGURA 3.7 Riesgo repercutido

6) Caracterización de los salvaguardas

Definición: Los salvaguardas o contra medidas son aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo, es conveniente considerar las salvaguardas de tipo preventivo (que buscan que la amenaza no ocurra o su daño sea despreciable) se tienen las siguientes:

- De tipo general: Entrevistas, método Delphi, reuniones, identificar y valorar salvaguardas existentes.
- Para la protección de los servicios: Especificación, desarrollo, despliegue y operación del servicio.
- Para la protección de los datos / información: Documento de seguridad, gestión de claves [si se usa cifrado] y clasificación de datos e información.
- Para la protección de software: Protección de código fuente y gestión de cambios y configuraciones.
- Para la protección de los equipos: Inventario y control de entradas y salidas.

- Para la protección de las comunicaciones: Configuración de routers, cortafuegos y redes, monitoreo y mantenimiento.
- Seguridad física: Control de acceso, protección frente a desastres naturales, accidentes industriales y emanaciones electromagnéticas.
- Relativas al personal: Selección de personal, formación continua y especificación del puesto de trabajo.
- Externalización: Nivel de servicio, compromiso de confidencialidad y asunción de responsabilidades y penalizaciones por incumplimiento.

7) Estimación del estado de riesgo

Si hay deberes a medio hacer como normas imprecisas, procedimientos incompletos, salvaguardas inadecuadas o insuficientes, o controles que no controlan, se dice que el sistema permanece sometido a un riesgo residual. Si se han hecho todos los deberes a la perfección, el riesgo residual debe ser despreciable (algo que la mayoría de las veces es esporádico).

El cálculo del riesgo residual es sencillo. Como no se han cambiado los activos, ni sus dependencias, sino solamente la magnitud de la degradación y la frecuencia de las amenazas, se repiten los cálculos de riesgo usando el impacto residual y la nueva tasa de ocurrencia. La magnitud de la degradación se toma en consideración en el cálculo del impacto residual. La magnitud de la frecuencia tomando en cuenta la eficacia de los salvaguardas, es la proporción que resta entre la eficacia perfecta y la eficacia real.

Riesgo residual = Eficacia perfecta - Eficacia real
Riesgo residual = $\sum$ riesgo acumulado de activos inferiores.
Riesgo residual = $\sum$ riesgo repercutido de activos superiores.

Esto es, el riesgo residual puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores.

Caracterización de los activos por su riesgo residual; es decir, lo que puede pasar tomando en consideración los salvaguardas desplegados.

1. Identificación del proyecto

    - Código, descripción, propietario, organización.
    - Versión, fecha.
    - Biblioteca de referencia.

2. Activos

    Para cada activo:
    - Impacto acumulado
    - Riesgo acumulado
    - Impacto repercutido
    - Riesgo repercutido

*Si procede, se debe mostrar la evolución histórica y el efecto de la planificación actual.

PASOS DEL MÉTODO PARA LA GESTIÓN DE RIESGOS

1. Toma de decisiones: Se califican los riesgos como: Crítico, grave, apreciable o asumible; como salida se obtiene un informe de calificación de impactos y riesgos, incluyendo plazo de tiempo en que deben estar resueltos.

2. Plan de seguridad: Programas de seguridad y plan de ejecución; como salida se obtiene la relación de problemas de seguridad, el mapa de riesgos y estado de riesgo (impacto y riesgo residual) actualizado y la salvaguarda implantada.

3. Evolución de los indicadores de impacto y riesgo.

4. Evaluación según criterios de seguridad.

Durante la gestión de riesgos se elige una estrategia para mitigar impacto y riesgo, se determinan los salvaguardas oportunos, se determina la calidad necesaria para dichos salvaguardas, se diseña un plan de seguridad (plan de acción o plan director) para llevar el impacto y el riesgo a niveles aceptables, se lleva a cabo el plan de seguridad y finalmente se hace una evaluación de nuestro plan de ejecución.

VENTAJAS DE MAGERIT

- Permite el análisis de la seguridad del Sistema deseado antes de su desarrollo
- Incorpora funciones de salvaguarda antes de completarlo.
- Es más barato y efectivo y
- Controla su consistencia a lo largo de todo el ciclo de vida.

3.2.2 CRAMM

CRAMM (CCTA Risk Analysis and Management Method) es un software creado por la Agencia Central de Informática y Telecomunicaciones del Reino Unido en 1987, actualmente está disponible en las versiones: v5.2 Express y v5.2 Expert la versión fue remodelado por SIEMENS Enterprise Communications y abarca toda una gama de soluciones en seguridad tales como:

- Una completa herramienta de evaluación de riesgos que es totalmente compatible con ISO 27001.

- Wizards para crear rápidamente pro-forma las políticas de seguridad de información y demás documentación relacionada.

- Herramientas que soportan los procesos clave en la continuidad de la gestión empresarial, para ayudar a lograr la certificación o el cumplimiento de la norma ISO 27001 y para apoyar a los gerentes de seguridad de información para planificar y gestionar la seguridad.

- Una base de datos de más de 3000 controles de seguridad que se hace referencia a los riesgos pertinentes, clasificadas por la eficacia y el costo.

- Instalaciones de ayuda, funciones de priorización y herramientas de información para ayudar con la implementación de las contramedidas y la gestión activa de los riesgos identificados.

PASOS DEL MÉTODO PARA LA GESTIÓN DE RIESGOS

CRAMM consta de tres fases:

1. La identificación y valoración de activos
2. Evaluación de los riesgos y requisitos para la seguridad
3. Contramedidas de selección y recomendación

1. La identificación y valoración de activos

En esta etapa se identifican y valoran propiamente dicho los activos físicos y los activos de software que forman parte del sistema; con ello se permite al revisor determinar las propiedades físicas (por ejemplo, de computadoras y hardware en general), software (por ejemplo, paquetes de aplicaciones) y los datos.

La forma de hacer la valoración es:

- Los activos físicos se valoran en términos de costo de reemplazo.

- Los datos y activos de software se valoran en términos del impacto que se produciría si la información fuera a estar disponible, destruida, divulgada o modificada.

2. Evaluación de los riesgos y requisitos para la seguridad

Después de haber comprendido la magnitud de los problemas potenciales, el siguiente paso es identificar qué tan probable es que estos problemas se produzcan.

CRAMM cubre toda la gama de amenazas deliberadas o accidentales que puedan afectar a los sistemas de información, entre los que destacan: hacking, virus, fallas de equipos o software, daños intencionales o el terrorismo (muchas veces el terrorismo resulta ser subyacente[11] y no real) y errores por la gente

La finalidad de esta etapa es: identificar y evaluar el tipo, así como el nivel de amenazas que pueden afectar al sistema para evaluar el alcance de las vulnerabilidades del sistema a las amenazas detectadas con los valores de activos y así calcular las medidas o nivel de riesgos, el cálculo del nivel de riesgo será: subyacente[8] o real.

[11] Que está debajo o se halla oculto bajo algo

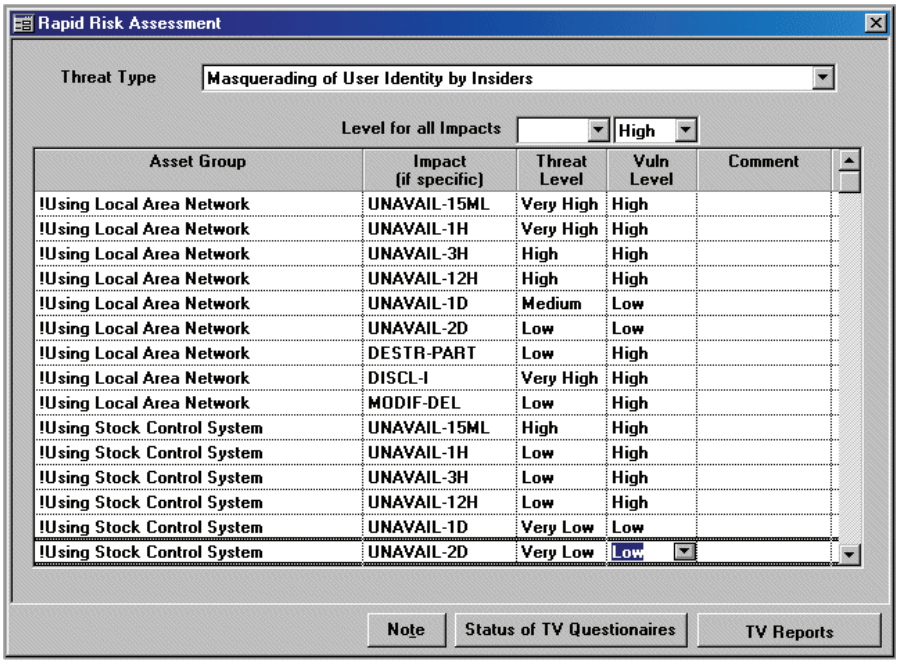


FIGURA 3.8 Evaluación Rápida de Amenazas, CRAMM v5. 2 Express

Para la evaluación de riesgos se tiene la herramienta Rapid Risk Assessment, se escoge el tipo de amenaza luego en cada renglón el tipo de activos al que pertenece la amenaza y todas las combinaciones de impacto-nivel de amenaza y vulnerabilidad que se desee pertinente y como adicional se puede poner un comentario, por ejemplo, de la figura 3.8 se coloca la amenaza: enmascaramiento de la identidad de los usuarios por intrusos[12] con niveles de impacto inválido (unavailable), destructivo (destructive), no aceptable (disclaimer) y/o modifica-deliberado (modify-deliberate) y combinaciones de nivel de amenaza y vulnerabilidad distintas desde el nivel más bajo hasta el más alto (Low-Very High).

3. Contramedidas de selección y recomendación

CRAMM contiene una biblioteca de más de 3000 contramedidas organizados en más de 70 agrupaciones lógicas. Utiliza en sus reportes automáticos el análisis ¿qué pasaría si? Junto con su resultado de costo vs beneficio.

El software CRAMM utiliza las medidas de los riesgos determinado durante la etapa anterior y los compara contra el nivel de seguridad (un nivel de umbral asociado a cada contramedida) a fin de determinar si los riesgos son lo suficientemente grandes para justificar la instalación de una contramedida en particular.

CRAMM utiliza un método cualitativo con valores del 1-7; 1 es el nivel más bajo y 7 representa una escala alta de necesidad de seguridad, para determinar que contramedidas seleccionar y recomendar CRAMM utiliza de manera implícita las siguientes tablas:

[12] Pertenece a la amenaza de imitación de identidad, véase capítulo 2 para más detalles

Si un incidente se espera que ocurra en promedio	El nivel de amenaza es
No más de una vez cada10 años	Muy bajo
Una vez en 3 años	Bajo
Una vez en 1 año	Medio
Una vez cada 4 meses	Alto
Una vez al mes	Muy alto

TABLA 3.5 Relación frecuencia-nivel de amenaza

En el peor de los casos, si un incidente iba a ocurrir	El nivel de amenaza es
No será más de 33% de probabilidad de éxito	Bajo
Tiene de 33% a 66% de probabilidad de éxito	Medio
La probabilidad de éxito será mayor al 66%	Alto

TABLA 3.6 Relación éxito-nivel de amenaza

Estas tablas no están de manera visible, el software ya hace el cálculo con base en éste último y con ayuda del árbol de contramedidas (figura 3.9), finalmente, el software nos dará las recomendaciones que más se ajusten a los datos que le proporcionamos.

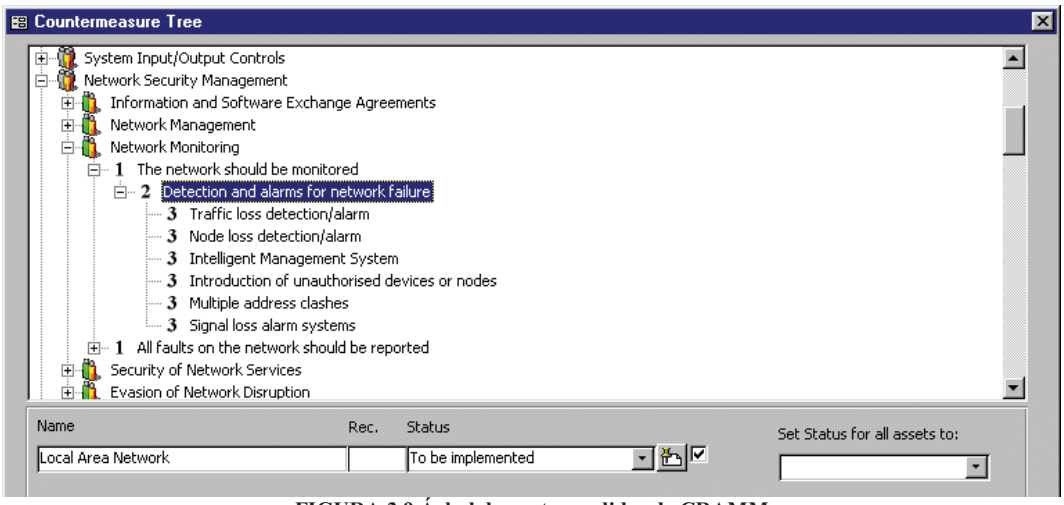


FIGURA 3.9 Árbol de contramedidas de CRAMM

El software CRAMM produce un informe que contiene las contramedidas técnicas, es decir, hardware, software y comunicaciones, que debe ser utilizado como la base de los requisitos establecidos en los requisitos operacionales. Estas contramedidas están divididas por grupos, cada grupo posee más categorías.

Las contramedidas de CRAMM son:

- Controles del sistema de entrada / salida
- Gestión de Seguridad de la Red
- Análisis de Contenido
- Autorización del Cliente
- Análisis de Vulnerabilidad

- Detección de Intrusos
- Controles Acceso de Red
- Seguridad de Tablas de Enrutamiento
- Red de Protección Física
- Seguridad de Red Inalámbrica
- Protección de Voz sobre IP (VoIP)
- Seguridad de Comercio Electrónico
- Resistencia de la red
- Controles contra el spam
- Protección contra la demora en la entrega
- Calidad de Servicio de red
- Protección contra ataques de denegación de servicio
- Integridad de datos sobre la red
- Conservación de mensajes de Secuenciación
- Planificación de Continuidad de Negocios
- Respaldos de Información
- Capacidad de Formación

La finalidad de esta etapa es identificar medidas para los riesgos detectados en la etapa 2, evaluar salvaguardas existentes para detectar áreas de debilidad o sobreprotección y hacer recomendaciones sobre salvaguardas apropiados.

Este software es famoso porque fue desarrollado originalmente por la CCTA para el uso en el centro de los departamentos de gobierno del Reino Unido, pero ha sido adoptado por las organizaciones del sector privado en los sectores financiero, editorial, los sectores manufacturero, de servicios públicos y gobiernos de todo el mundo, lo usa la OTAN (Organización del Tratado del Atlántico Norte) y el Ejército de Holanda.

Las ventajas de utilizar CRAMM son las siguientes:

- El método ya ha sido ampliamente utilizado por una gran variedad de organizaciones del sector público y privado, que han reconocido que produce recomendaciones coherentes, justificadas que den lugar a mejoras significativas en seguridad y las normas correspondientes.

- Es global ya que abarca todos los aspectos de seguridad, incluidas las contramedidas técnicas y no técnicas.

- Se basa en la experiencia y los conocimientos de especialistas en seguridad.

- Su enfoque ha sido evaluado por varios organismos internacionales, donde se ha recibido un amplio reconocimiento como líder mundial. Este reconocimiento ha conducido a CRAMM recibir un premio a la innovación de la Sociedad Británica de Computación.

- El método puede ser usado para el análisis y diseño de sistemas de información, así como para los sistemas existentes.

3.2.3 MARION

MARION (Méthodologie d'Analyse de Risques Informatiques Orientée par Niveaux) la Metodología del Análisis de Riesgos Informáticos por Niveles se encuentra documentado en Francia surgió en 1985, es un método cualitativo que se basa en experiencia y esperanzas matemáticas; no en probabilidades hay 2 productos: MARION AP y MARIONRsx.

MARION posee una herramienta para evaluar el nivel de seguridad existente dicha herramienta es un cuestionario correlacionado con 27 factores en 6 categorías a responder.

A las respuestas se le asigna un peso, al final todas las respuestas se reflejan en una gráfica de factores contra las diferentes soluciones o contramedidas a aplicar a cada uno de los 27 factores. Este método fue impulsado en la década de los 80's y hasta 1998 llegó una herramienta sucesora: MEHARI, impulsado también por el (Club de la Seguridad Informática Francesa) CLUSIF. Todavía existen datos de pocas empresas francesas que siguen utilizando MARION por su efectividad y que se niegan a usar al sucesor MEHARI, pues ambas herramientas son del CLUSIF. Actualmente el CLUSIF ya no promueve esta metodología y por ello se desconoce qué tipo de cuestionario es el que se aplicaba y que aún aplican en secreto esas pocas empresas en Francia.

PASOS DEL MÉTODO PARA LA GESTIÓN DE RIESGOS

1. Preparación
2. Vulnerabilidad de auditoría
3. Análisis de Riesgos
4. Plan de Acción

1. Preparación

Se utiliza para definir los objetivos de seguridad que deben alcanzarse, así como las áreas de acción de la auditoría y un desglose funcional del Sistema de Información (SI) con el fin de agilizar la realización del estudio.

2. Vulnerabilidad de auditoría

Es responder a los cuestionarios. Estas respuestas le ayudarán a identificar los riesgos y limitaciones del SI. Al final de esta auditoría, se construye una gráfica, de igual manera un diagrama que representa, respectivamente, el puntaje diferenciado para cada indicador y los factores de riesgo de especial importancia.

La forma de rosa o roseta que se forma con cada uno de los 27 indicadores son una manera de ver rápidamente las vulnerabilidades del SI para estar mejor protegido. Cada indicador se le asigna una puntuación entre 0 (inseguridad) y 4 (excelente), el valor 3 indica una seguridad correcta (ver figura 3.10).

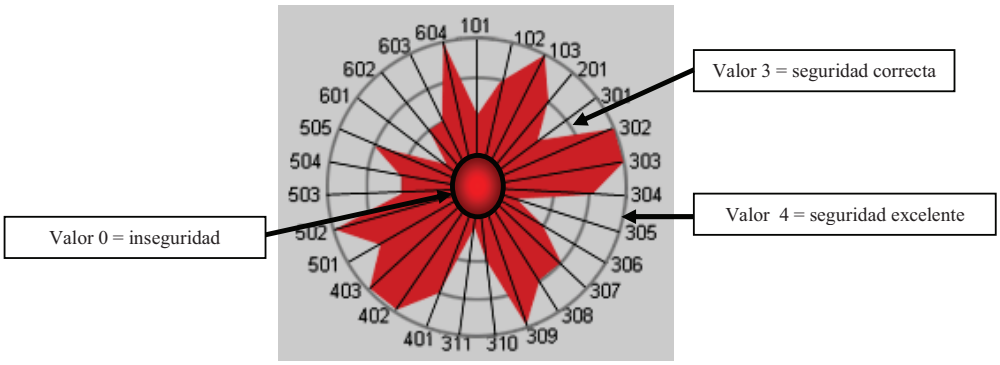


FIGURA 3.10 Roseta MARION para identificar las vulnerabilidades

3. Análisis de Riesgos

Clasifica los riesgos en función de su criticidad (en las clases: grandes riesgos y riesgos individuales). Se corre el desglose funcional del SI para un análisis detallado de las amenazas, sus impactos y su probabilidad.

La etapa de análisis de riesgos releva los diferentes riesgos por ejemplo:

- **Infundado (o improbable):** La amenaza es insostenible
- **Débil:** La amenaza tiene pocas probabilidades de existir
- **Moderada:** La amenaza es real
- **Alta:** La amenaza tiene muchas probabilidades de existir

El análisis de riesgos se encarga de 17 tipos de amenazas específicas:

1. El ataque de la red lógica
2. Error de entrada
3. Error de transmisión
4. La apropiación indebida de activos
5. La copia ilegal de software
6. La falta de personal
7. La falta de proveedores
8. La interrupción de las operaciones de red
9. Latente defecto de un software
10. Malevolencia física
11. Malversación
12. Norma de diseño / desarrollo
13. Operativos Estándar
14. Sabotaje Inmaterial
15. Indiscreción o mal uso de la información
16. La falta de SI
17. Las lesiones físicas

TABLA 3.7 Amenazas específicas de MARION

4. Plan de Acción

Propone soluciones que deben aplicarse para aumentar el valor de los 27 indicadores en el grado 3 (nivel satisfactorio de seguridad) de la auditoría de la vulnerabilidad y alcanzar los objetivos fijados en la preparación todo esto se logra con el desarrollo de un plan de acción. El costo de la actualización es evaluado y las tareas por hacer para lograr esto se han programado.

El método del cuestionario es bastante sencillo de aplicar y está bien establecido debido a su madurez. Para las empresas auditadas es una ventaja. El método MEHARI su sucesor va más lejos al proponer la creación de una política integral de seguridad.

VENTAJAS DE MARION

- El análisis se realiza por niveles
- No requiere de software complicado para ser implementado
- El análisis no se vuelve tedioso debido a sus amenaza ya identificadas
- El indicador de estado de riesgo (valores del 0 al 4) nunca presenta valores intermedios: se interpreta como es inseguro, es excelente, es correcto o es incorrecto.

3.2.4 MEHARI

MEHARI (Métodos Armonizados para el Análisis de Riesgo) está impulsado por el CLUSIF desde 1995, se deriva de los métodos de MELISA y MARION. Actualmente está en versión Francés e Inglés, es utilizado por muchas empresas públicas, sector privado; de hecho muchos de los que usaban MARION y MELISA siguen utilizándolo o han migrado a MEHARI, porque las 2 herramientas ya mencionadas sólo lanzaban el análisis, no proponían una solución concreta de seguridad y MEHARI ya lo hace. El planteamiento general de MEHARI es el análisis de cuestiones de seguridad (al igual que sus antecesores) en función de tres criterios básicos de seguridad (confidencialidad, integridad y disponibilidad).

PLANES MÉTODO MEHARI

1. **Plan Estratégico de Seguridad (PSS):** Fija los objetivos de la seguridad y las métricas para medirlos. Define la política de seguridad, la identificación de factores de reducción de riesgo proporciona una base metodológica para construir un plan de seguridad; se fundamenta en una base de conocimientos de situación de riesgos y en procedimientos automatizados para la evaluación de los factores de reducción de riesgo.

2. **Planes Operativos de Seguridad (POS):** Se desarrollan los escenarios de los servicios comprometidos y auditorías del SI. Sobre la base de esta auditoría, la evaluación de cada riesgo (probabilidad, impacto), se lleva a cabo posteriormente para expresar las necesidades

de seguridad, y por las mismas medidas de protección requerido. Por último, la planificación de la actualización de seguridad de la PSI[13] se hace.

3. **Plan Operativo de empresa (POE):** Prevé supervisión de la seguridad mediante el desarrollo de indicadores sobre los riesgos identificados y la elección de escenarios de desastre contra el que debemos evitar. Habitualmente se formula así: "¿Han sido identificados todos los riesgos, y son aceptables sus niveles?" mediante dos módulos de seguridad: el módulo rápido y el módulo detallado, aunque el módulo rápido se encuentra aún en fase de desarrollo pero ya se puede utilizar.

Este método permite construir una política de seguridad diseñada para mitigar las vulnerabilidades identificadas durante las auditorías de seguridad y los planes operacionales, para alcanzar el nivel de seguridad adecuado a los objetivos del Plan Estratégico para la Seguridad.

VENTAJAS DE MEHARI

- Es un método global de evaluación y gestión de riesgos relacionados con la información, sus tratamientos y medios utilizados.
- La versión de 2007 fue descargada en más de 100 países.
- El uso del método es libre y su distribución se realiza conforme a las disposiciones del Código Libre (Open Source).

3.2.5 MELISA

MELISA (Método para Evaluar la Vulnerabilidad de los Sistemas de Información Residual) fue inventado por Albert Harari dentro de la Dirección General de Armamento (DGA / DCN) en Francia. MELISA ha sido abandonada por sus dueños a pesar de que era ampliamente utilizado en Francia. Es un método bastante incómodo que tiene como base un cuestionario muy extenso de preguntas. Está destinada a ser utilizada por las grandes empresas, pero es muy arduo el estar respondiendo a todas las preguntas aún así sigue siendo usado o como se menciono con anterioridad se ha migrado a MEHARI.

3.2.6 MOSLER

MOSLER (Método Aplicado al Análisis y Clasificación de los Riesgos), tiene como objetivo identificar, analizar y evaluar los factores que puedan influir en la manifestación de un riesgo, permitiendo calcular la clase del mismo.
El método tiene por objeto la identificación, análisis y evaluación de los factores que pueden influir en la manifestación de un riesgo, con la finalidad de que la información obtenida, nos permita calcular la clase de riesgo.
El método es de tipo secuencial y cada fase del mismo se apoya en los datos obtenidos en las fases que le preceden. Utiliza una escala Penta (del 1 al 5 donde el 1 se refiere a menor gravedad y el 5 a mayor gravedad).

[13] Política de Seguridad Informática

Está conformado por 6 criterios:

1. Criterio de función
2. Criterio de sustitución
3. Criterio de profundidad
4. Criterio de extensión
5. Criterio de agresión
6. Criterio de vulnerabilidad

La descripción de cada uno de los criterios, así como su definición, los menciono a continuación:

- **Criterio de función F**

Las consecuencias negativas o daños pueden alterar de forma diferente la actividad:

Muy gravemente 5
Gravemente 4
Medianamente 3
Levemente 2
Muy levemente 1

- **Criterio de sustitución S**

Los bienes pueden ser sustituidos:

Muy difícilmente 5
Difícilmente 4
Sin muchas dificultades 3
Fácilmente 2
Muy fácilmente 1

- **Criterio de Profundidad P**

La perturbación y los efectos psicológicos que producirían serían de diferente graduación por sus efectos en la imagen.

Perturbaciones muy graves 5
Perturbaciones graves 4
Perturbaciones limitadas 3
Perturbaciones leves 2
Perturbaciones muy leves 1

- **Criterio de extensión E**

El alcance de los daños según su amplitud o extensión pueden ser:

De alcance internacional. 5
De carácter nacional. 4
De carácter regional. 3
De carácter local. 2
De carácter individual. 1

- **Criterio de agresión A**

La probabilidad de que el riesgo se manifieste es:

Muy alta 5
Alta 4
Normal 3
Baja 2
Muy baja 1

- **Criterio de vulnerabilidad V**

La probabilidad de que se produzcan daños es:

Muy alta 5
Alta 4
Normal 3
Baja 2
Muy baja 1

Del criterio 1 y 2 se obtiene la importancia del riesgo, del criterio 3 y 4 el daño del riesgo y finalmente del criterio 5 y 6 se tendrá el cálculo de probabilidad.

PASOS DEL MÉTODO PARA LA GESTIÓN DE RIESGOS

1. Definición del riesgo.
2. Análisis del riesgo.
3. Evolución del riesgo.
4. Cálculo de la clase de riesgo.

1. Definición del riesgo

En esta fase se identifica el riesgo, el procedimiento a seguir es mediante la identificación de sus elementos, estos son: el bien y el daño.

2. Análisis del riesgo

En esta fase se hace el cálculo de criterios que posteriormente proporcionará la evolución del riesgo. El procedimiento consiste en:

a) Identificación de las variables.
b) Análisis de los factores obtenidos de las variables y ver en qué medida influyen en el criterio considerado, cuantificando los resultados según la escala Penta (valores que van del 1 al 5).

3. **Evaluación del riesgo:** Tiene por objeto cuantificar el riesgo considerado.

a) Cálculo del carácter del riesgo **C**.

C = I + D
I = Importancia del suceso = **F** x **S**
D = Daños ocasionados = **P** x **E**

F = Criterio de Función
S = Criterio de Sustitución
E = Criterio de Extensión
P = Criterio de Profundidad

b) Cálculo de la probabilidad **Prob.**

Prob = **A** x **V**

Prob. = Probabilidad
A = Criterio de Agresión
V = Criterio de Vulnerabilidad

c) Cuantificación del riesgo considerado. Se multiplican los valores obtenido en **a)** y **b)**:

ER = **C** x **Prob**

ER = Estimación del Riesgo
C = Carácter del riesgo
Prob = Probabilidad

En resumen, se tienen que usar los 6 criterios en el orden establecido al final arroja los residuos: importancia, daño y cálculo de probabilidad; la importancia más el daño, arroja el carácter del riesgo, al multiplicar el carácter del riesgo por el cálculo de probabilidad da como resultado el riesgo esperado o la clase de riesgo.

4. Cálculo de la clase de riesgo

Esta clase tiene por objeto clasificar el riesgo en función del valor obtenido en la evolución del mismo. Dicho valor estará comprendido entre 2 y 1.250, esto es Valor ER Clase de riesgo y se determina con ayuda de la tabla mostrada abajo.

Muy bajo	2-250
Pequeño	251-500
Normal	501-750
Grande	751-1.000
Elevado	1.01-1.250

TABLA 3.8 para determinar la clase de riesgo

3.2.7 ITIL

Desarrollado a finales de 1980, la Biblioteca de Infraestructura de Tecnologías de la Información (**ITIL**) se ha convertido en el estándar mundial de de facto en la Gestión de Servicios Informáticos. Iniciado como una guía para el gobierno de UK, pertenece a la OGC (Oficina de Comercio Gubernamental), pero es de libre utilización, constaba de 10 libros centrales, los libros centrales se han agrupado en dos, cubriendo las áreas de Soporte del Servicio y Prestación.

A lo largo de todo el ciclo de los productos TI, la fase de operaciones alcanza cerca del 70-80% del total del tiempo y del costo, el resto se invierte en el desarrollo del producto u obtención.

FIGURA 3.11 Metodología ITIL

De esta manera, los procesos eficaces y eficientes de la Gestión de Servicios TI se convierten en esenciales para el éxito de los departamentos de TI, en esta parte es dónde se concentra todo debido a que es donde interviene el análisis y gestión de riesgos.

ITIL es un conjunto de las mejores prácticas para la gestión de servicios de TI, describe las mejores prácticas que se pueden utilizar y que mejor se adecuan a una organización, incluye cinco disciplinas que proporciona a las empresas flexibilidad y estabilidad para ofrecer servicios de TI, estas son:

1. Gestión de incidentes: Mejora la detección de incidentes; mejora el plazo de recuperación de incidentes en función de la importancia para la operación de la empresa.

2. Gestión de problemas: Mejora la administración de problemas recurrentes e implementa soluciones preventivas con el objetivo de reducir o incluso eliminar su ocurrencia.

3. Gestión de cambios: Establece cómo ocurrirán los cambios para anticipar efectos colaterales.

4. Gestión de versiones: Garantiza el funcionamiento correcto de los diferentes departamentos estableciendo los requisitos de trabajo.

5. Gestión de configuración: Administra la infraestructura de TI mediante un inventario de la infraestructura actual para mejorar su administración y desarrollo.

Incluye también cinco disciplinas que soportan los servicios TI de calidad y bajo costo de las empresas, estas son:

1. Gestión del nivel de servicio: Mantiene un nivel de calidad de servicio específico usando contratos de servicio renegociados periódicamente.

2. Gestión de la disponibilidad: Asegura un nivel satisfactorio de disponibilidad a un costo razonable.

3. Gestión de la capacidad: Verifica que los niveles de capacidades y rendimientos cubran los requisitos actuales y futuros.

4. Gestión financiera para servicios TI: Administra la rentabilidad de los medios adoptados para proporcionar el servicio.

5. Gestión de la continuidad de los servicios TI: Define e implementa plazos contractuales de recuperación después de un incidente.

El objetivo de ITIL en todas sus disciplinas es la definición de las mejores prácticas para los procesos y responsabilidades que hay que establecer para gestionar de forma eficaz los servicios de TI de la organización, y cumplir así los objetivos empresariales en cuanto a la distribución de servicios y la generación de beneficios.

ITIL considera tres subprocesos fundamentales para la gestión de riesgos:

1. **Análisis del Impacto y Riesgo al Negocio:** Se tiene que cuantificar el impacto de la pérdida de servicios y activos en una empresa y determinar la probabilidad de una amenaza o la vulnerabilidad ante la misma. El resultado de este proceso es el Registro de Riesgos (donde se detallan posibles riesgos y contramedidas), una lista de riesgos que deben atenderse según su prioridad.

2. **Evaluación de Mitigación de Riesgo Requerida:** Se debe determinar dónde se necesitan medidas de mitigación de riesgo e identificar a los Responsables del Riesgo, quienes están a cargo de la implementación y el mantenimiento continuo.

3. **Monitorización de Riesgo:** Se monitorea el progreso de la implementación de contramedidas, y se toma acción correctiva de ser necesario.

A continuación se mencionan 10 formas en las que se puede mejorar la gestión de riesgos de TI según ITIL.

1) Tratar el riesgo en las TI como riesgo empresarial
2) Tratar los riesgos para corto como para medio plazo
3) Corregir las fisuras y prepararse para las futuras
4) Simplificar la base
5) Crear estructuras y procesos de gestión del riesgo y adaptarlas al resto de procesos y decisiones empresariales
6) Concienciar a los trabajadores de los riesgos, vulnerabilidades y políticas que afectan a la mayoría
7) Desarrollar la cultura de la concientización del riesgo
8) Evaluar la efectividad
9) Mirar hacia el futuro
10) Predicar con el ejemplo

Matriz RACI y RASCI de ITIL

Una matriz de asignación de responsabilidades o RACI (figura 3.12) es un modelo en forma de matriz se utiliza para relacionar actividades o tareas con todos los recursos que importan a los encargados de TI. Las responsabilidades que se encuentran en un matriz RACI son 4:

1. Responsable (Responsible)
2. Aprobador (Accountable)
3. Consultado (Consulted) e
4. Informado (Informed)

En la página oficial de ITIL se encuentra disponible a la venta el mapa de procesos ITIL v3 en una adaptación para ser usado con el programa Microsoft Visio[14].

El Mapa de Procesos ITIL V3 para Visio (ver figura 3.12) contiene una matriz RACI de ITIL completa en forma de tabla de Excel. Los procesos ITIL aparecen en una columna en la parte izquierda y los roles en una fila en la parte superior de la matriz. La lista de procesos que aparece en la columna de la izquierda está provista de breves descripciones sobre los procesos ITIL V3 (mediante ventanas Pop-up) y enlaces a modelos de procesos.

En RASCI, una ampliación del modelo RACI, se encuentran las siguientes responsabilidades:

- R-Responsible (responsable de la ejecución): Alguien que desempeña una tarea determinada. Para cada tarea en un proceso ITIL existe normalmente un rol ITIL responsable de su ejecución.

- A-Accountable (responsable del proceso en conjunto): Alguien que asume la responsabilidad conjunta final por la correcta y completa ejecución de un proceso, que recibe las informaciones de los responsables de la ejecución del proceso. Normalmente, el

[14] Software de Microsoft para ver, examinar y comunicar procesos, sistemas e información complicada, como diagramas de flujo, UML y más.

responsable de proceso asume la responsabilidad conjunta de un proceso; para cada proceso existe un responsable de proceso.

- S-Support (apoyo): Alguien que apoya un rol ejecutivo en un proceso, contribuyendo a la implementación de una tarea en un proceso.

- C-Consulted (consultado): Alguien que no está implicado directamente en la ejecución de un proceso pero que da algún tipo de input para el proceso y/o al cual se pide su consejo y opinión.

- I-Informed (informado): Alguien que recibe las salidas (outputs) de un proceso o a quien se informa de los avances del proceso.

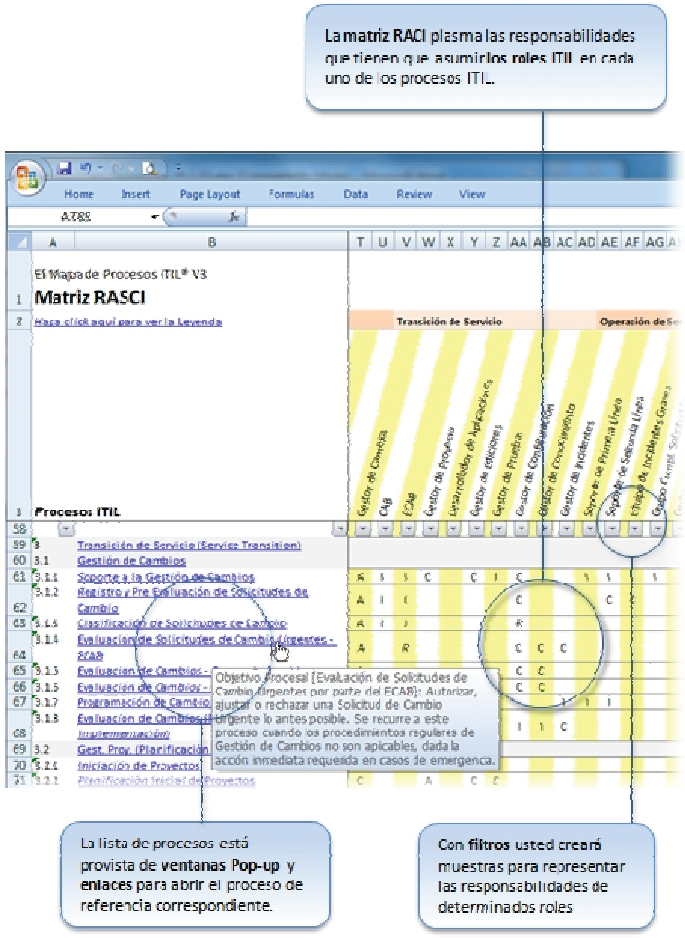


FIGURA 3.12 Matriz RASCI en Microsoft

Las matrices RACI tienen sobre todo sentido si múltiples roles asumen diferentes niveles de responsabilidad en varios procesos: ayudan como simple instrumento a comunicar responsabilidades de forma inteligible y contribuyen a evitar conflictos de competencias.

SUBPROCESOS ITIL PARA LA GESTIÓN DE RIESGOS

Para llevar a cabo estos subprocesos ITIL incorpora el llamado Mapa de procesos (IT Process Maps GbR) elaborado de forma vertical y que se compone de 10 pasos

Paso 1: Preparación del proyecto

Paso 2: Definición de la estructura de servicios

Paso 3: Selección de roles ITIL[15] y propietarios de roles: entre estos roles encontramos al Gestor de incidentes.

Paso 4: Análisis de procesos existentes (Evaluación de ITIL)

Paso 5: Definición de la estructura de procesos

Paso 6: Definición de interfaces de procesos ITIL

Paso 7: Estableciendo controles de procesos

Paso 8: Diseñando los procesos en detalle

Paso 9: Selección e implementación de sistemas de aplicaciones

Paso 10: Implementación de procesos y adiestramiento

Uno de los roles más importantes en todo el proceso ITIL es el de gestor de riesgo; las tareas del gestor de incidentes son:

- Establecer una jerarquía de incidentes
- Proveer información relacionada con incidentes a los procesos de Gestión de Servicio
- Modelar pasos predefinidos que deben tomarse para manejar cierto tipo de Incidentes
- Proporcionar información sobre el estado del incidente
- Notificar si se presenta fallos al servicio
- Solicitud de Apoyo en la solución de un Incidente o problema (sólo en caso de requerirse)
- Hacer un registro de incidente (ver tabla 3.9): éste documento nos ayuda a comprender de una manera rápida el contexto de un incidente, ya que su estructura en forma de tabla permite identificar algún punto en específico como nombre del observador, fecha de la observación, grado de severidad objetiva, ¿qué incidente ocurrió?, ¿cómo ocurrió?, etc.

[15] Para los roles ITIL se ocupa la matriz de responsabilidades RACI O RASCI de ITIL

Como referencia del ¿Cómo hacer un registro? se tiene el ejemplo a continuación:

REGISTRO DE INCIDENTE DEL DÍA:
1. Identificación única del Incidente (ID, por regla general o por número de secuencia)
2. Fecha y hora del registro
3. Agente del Service Desk responsable por el registro
4. Método de notificación
5. Datos del cliente/ usuario que dio la notificación
6. Vía de comunicación utilizada para la respuesta
7. Descripción de síntomas
8. Usuarios / áreas del negocio afectados
9. Servicios afectados
10. Priorización, una función de los siguientes componentes:
1) Urgencia (tiempo disponible hasta la resolución del Incidente), por ej.
a) Hasta 0,5 horas
b) Hasta 2,0 horas
c) Hasta 6,0 horas
2) Grado de severidad (daño causado al negocio), por ej.
a) "Alto" (interrupción de procesos esenciales del negocio)
b) "Normal" (interrupción del trabajo de empleados individuales)
c) "Bajo" (estorbo al trabajo de empleados individuales; es posible continuar trabajando usando una solución alterna)
3) Prioridad (por ejemplo en etapas 1, 2 y 3): El resultado de la combinación de la urgencia y el grado de severidad
11. Relación con los CI's
12. Categoría del producto, seleccionado usualmente de un árbol de categorías según el ejemplo siguiente:
1) Computadora del cliente
a) Configuración estándar 1
b) ...
2) Impresora
a) Fabricante 1
b) ...
13. Categoría del Incidente, seleccionado usualmente de un árbol de categorías según el ejemplo siguiente:
1) Error de equipo
2) Error de aplicacion
3) ...
14. Enlaces a Registros de Incidentes relacionados (si existen Incidentes similares sin resolver, a los cuales se les puede atribuir el nuevo Incidente)
15. Enlaces a Registros de Problemas relacionados (si existen Problemas sin resolver, a los cuales se les puede atribuir el nuevo Incidente)
16. Registro de actividades
1) Fecha y hora
2) Persona a cargo
3) Descripción de las actividades
17. Datos de resolución y cierre
1) Fecha y hora de la resolución
2) Fecha y hora del cierre
3) Categorías del cierre (si se requiere, categorías revisadas de productos e Incidentes)

TABLA 3.9 Registro de incidentes

VENTAJAS DE ITIL

- La estructura de costos de los servicios de TI se conoce y administra.
- La plantilla de TI es más estable.
- Se dispone de planes para mantener la continuidad de servicio.
- Las inversiones en TI son más fáciles de validar.
- Se conserva el conocimiento en la organización de TI.
- Mejora la comunicación con los clientes y usuarios finales a través de los diversos puntos de contacto acordados.
- Los servicios se detallan en lenguaje del cliente y con más detalles.
- Se maneja mejor la calidad y los costos de los servicios.
- La entrega de servicios se enfoca más al cliente, mejorando con ello la calidad de los mismos y relación entre el cliente y el departamento de IT.
- Una mayor flexibilidad y adaptabilidad de los servicios.

3.2.8 COBIT

COBIT (Objetivos de Control para Tecnologías de Información) éste modelo fue definido por un grupo de expertos en aspectos técnicos, de riesgos, de calidad, de control y de seguridad mediante un consenso.

Aplicado a los sistemas informáticos, orientado al resultado o propósito que se desea alcanzar, implementando procedimientos de control específicos dentro de una actividad de tecnología de información.

Nace en 1996, los objetivos que se persiguen con COBIT son:

- Proporcionar a la dirección y a la gerencia de la empresa un modelo de administración de TI para comprender y administrar los riesgos asociados con TI.

- Ayudar a resolver los riesgos, procedimientos y aspectos técnicos dentro del área de TI.

- Generar procedimientos que satisfagan las necesidades de administración de TI, asegurando la integridad de la información y sus sistemas.

COBIT está dividido en cuatro libros:

1. Resumen ejecutivo: Consiste de una visión ejecutiva donde se proporciona un entendimiento de todos los principios y conceptos claves de COBIT.

2. Antecedentes y marco de referencia: Describe en detalle los 34 objetivos de control de TI. Identificando para cada uno de ellos los requerimientos del negocio para la información y los impactos preliminares de los recursos.

3. Guías de auditoría: Contiene pasos de auditoría sugeridos, correspondientes a los 34 objetivos de control, asistiendo a los auditores en la revisión de los procesos.

4. Herramientas de implementación

Contiene:

- Conocimiento de la administración y diagnóstico de control
- Guía de implementación
- FAQ (Frequently Asked Questions)
- Casos de estudio
- Presentaciones

DOMINIOS DE COBIT

Sirven para cubrir con los 215 objetivos de control que COBIT maneja teniendo 34 objetivos de nivel de carácter alto los cuales se mencionan a continuación:

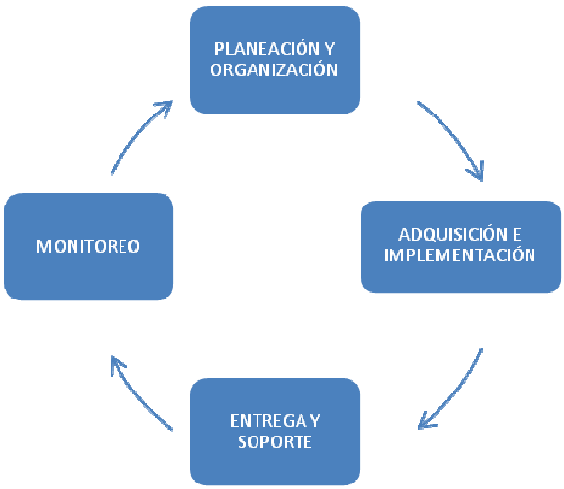


FIGURA 3.13 Etapas de COBIT para la gestión de riesgos

1. Planeación y organización

- P01 Definir un Plan Estratégico de Tecnología de Información
- P02 Definir la Arquitectura de Información
- P03 Determinar la Dirección Tecnológica
- P04 Definir la Organización y las relaciones de Tecnología de Información
- P05 Administrar la Inversión en Tecnología de Información
- P06 Comunicar la Dirección y Aspiraciones de Gerencia
- P07 Administrar Recursos Humanos
- P08 Asegurar el Cumplimiento de requerimientos externos
- P09 Evaluar Riesgos
- P010 Administrar Proyectos
- P011 Administrar Calidad

La Planificación y el dominio de Organización pueden ser usados en una empresa para ayudar a alcanzar los objetivos.

2. Adquisición e Implementación

- AI1 Identificar Soluciones
- AI2 Adquirir y Mantener Software de Aplicación
- AI3 Adquirir y Mantener Arquitectura Tecnológica
- AI4 Desarrollar y Mantener Procedimientos relacionados con TI
- AI5 Instalar y Acreditar Sistemas
- AI6 Administrar Cambios

La adquisición e implementación ayudan a identificar las exigencias de las TI, también dirige el desarrollo de un plan de mantenimiento para la cual, una empresa debería adoptar de esta manera prolongar la vida de un sistema TI y sus componentes.

3. Entrega y Soporte

- DS1 Definir Niveles de Servicio
- DS2 Administrar Servicios prestados por Terceros
- DS3 Administrar Desempeño y Capacidad
- DS4 Asegurar Servicio Continuo
- DS5 Garantizar la Seguridad de Sistemas
- DS6 Identificar y Asignar Costos
- DS7 Educar y Entrenar a los Usuarios
- DS8 Apoyar y Asistir a los Clientes de TI
- DS9 Administrar la Configuración
- DS10 Administrar Problemas e Incidentes
- DS11 Administrar Datos
- DS12 Administrar Instalaciones
- DS13 Administrar Operaciones

La entrega y soporte se enfoca en los aspectos de entrega de la tecnología de información. Esto cubre áreas como la ejecución de los usos dentro del sistema TI y sus resultados, así como, los procesos de apoyo que permiten la ejecución eficaz y eficiente de estos sistemas TI. Estos procesos de apoyo incluyen cuestiones de seguridad además de educación.

4. Monitoreo

- M1 Monitorear los Procesos
- M2 Evaluar lo adecuado del Control Interno
- M3 Obtener Aseguramiento Independiente
- M4 Proporcionar Auditoría Independiente

El monitoreo determina si el sistema todavía encuentra los objetivos para los cuales fue diseñado y los mandos necesarios de cumplir con exigencias reguladoras. La supervisión también cubre la cuestión de una evaluación independiente de la eficacia de sistema TI en su capacidad de encontrar objetivos de negocio, así como los procesos de control de la empresa por interventores internos y externos.

La metodología se deriva de sistemas aplicados mundialmente con éxito en la administración y el control de riesgos (sistema CRAMM, Reino Unido; sistema MARION, Francia)

LAS FASES DEL MODELO COBIT

FASE 1

- **Relevamiento de respuestas en aspectos de seguridad, calidad, eficacia y eficiencia:** Se trata de un relevamiento que permitirá calificar 34 procesos representativos del estado de la seguridad, calidad y eficiencia de los sistemas de tecnología informática de la institución. El permanente mejoramiento de la calificación de cada proceso mediante la puesta en práctica de distintas recomendaciones será proporcional al descenso de los riesgos de impacto de amenazas.

FASE 2

- **Verificación de la fiabilidad de las respuestas:** En esta fase se utiliza el módulo **MEYCOR-AUDIT COBIT** (figura 3.14) (CSA) permite aplicar distintas técnicas de recopilación de evidencia para asegurar que las respuestas a los cuestionarios son confiables. De no serlos en algunos casos, se harán las rectificaciones o aclaraciones correspondientes.

FIGURA 3.14 Módulo AUDIT de COBIT

FASE 3

- **Presentación del diagnóstico en gráfica de radar (figura 3.15):** Los cuatro dominios se diferencian mediante distintos colores a los efectos de facilitar la identificación de las áreas más críticas. La circunferencia azul representa el nivel deseado y el trazo rojo el nivel obtenido.

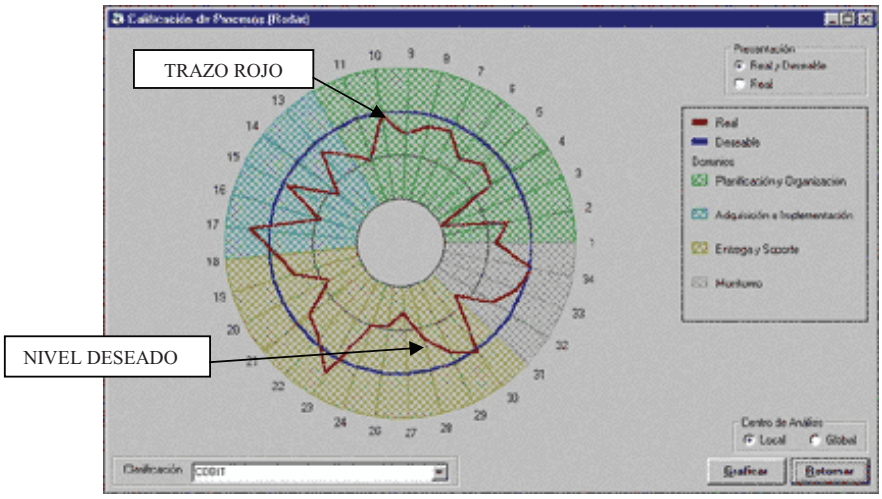


FIGURA 3.15 Diagrama de Dominios COBIT

FASE 4

- **Evaluación de restricciones:** Esta fase evalúa las restricciones (vinculadas a las instalaciones, las personas, los datos aplicativos y la infraestructura tecnológica), las cuales habrán de condicionar la ecuación decisoria de la organización respecto de las provisiones sugeridas por las recomendaciones generadas. Para evaluar las restricciones se contesta a unas preguntas con el llamado "Cuestionario de Restricciones" (ver figura 3.16)

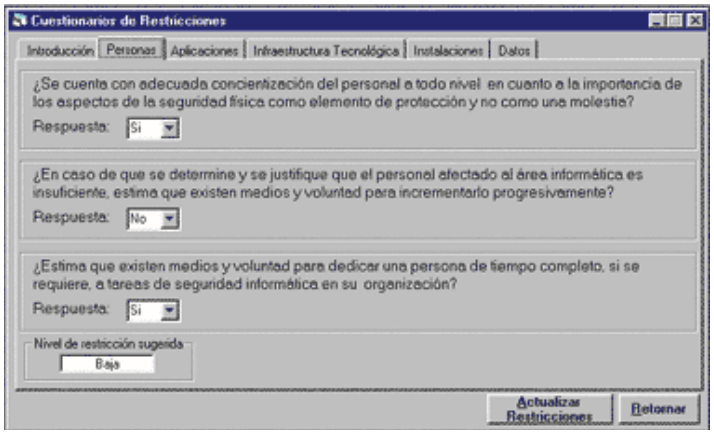


FIGURA 3.16 Cuestionario de restricciones

FASE 5

- **Administrar los riesgos, decidir políticas y seleccionar recomendaciones según las limitantes existentes:** Las políticas básicas determinadas se traducen en el mejoramiento o no de cada uno de los 34 procesos usados, postulándose objetivos de mejoramiento que se articulan mediante la aplicación de las recomendaciones. Las recomendaciones las da en forma de lista como se ve en la figura 3.17.

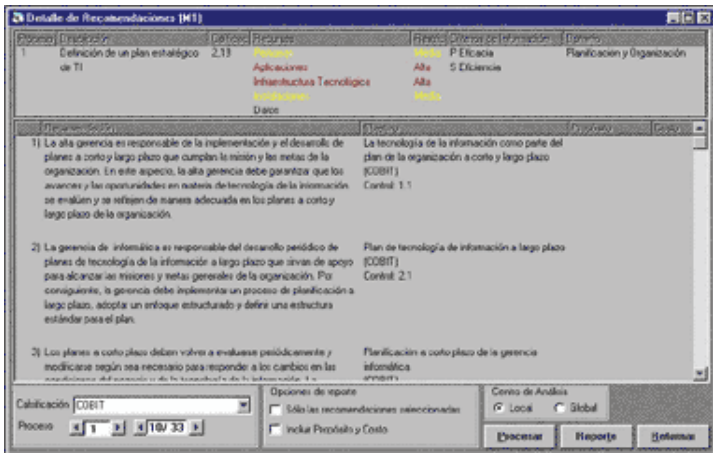


FIGURA 3.17 Detalle de recomendaciones

FASE 6

- **Incorporar las recomendaciones aceptadas a los planes de largo y corto plazo de la organización:** Se desarrolla un plan de implantación de las mismas, ajustadas al presupuesto asignado y en el marco de un determinado cronograma de trabajo que se despliega a largo y corto plazo. El plan de recomendaciones también no lo da en forma de lista el software (ver figura 3.18).

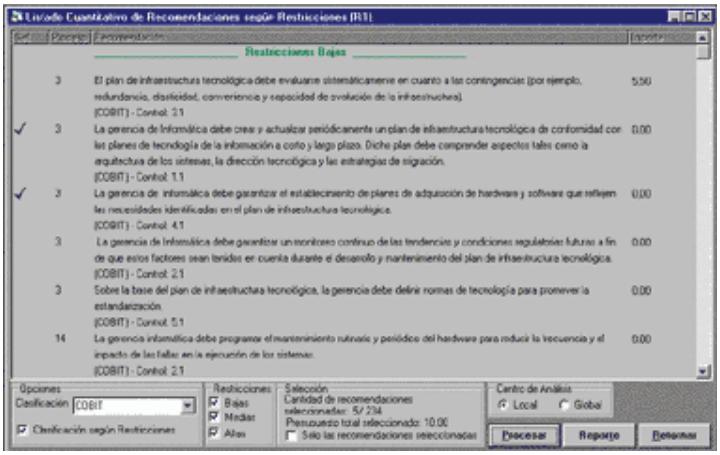


FIGURA 3.18 Plan de recomendaciones

FASE 7

- **Seguimiento de diagnósticos periódicos:** Permite realizar diagnósticos periódicos para determinar los avances y retrocesos que se van procesando a lo largo del tiempo. Concretamente, cada nuevo diagnóstico permite corroborar las mejoras logradas como producto de la implantación de las recomendaciones. En la figura 3.19 se muestra el análisis de 2 periodos diferentes.

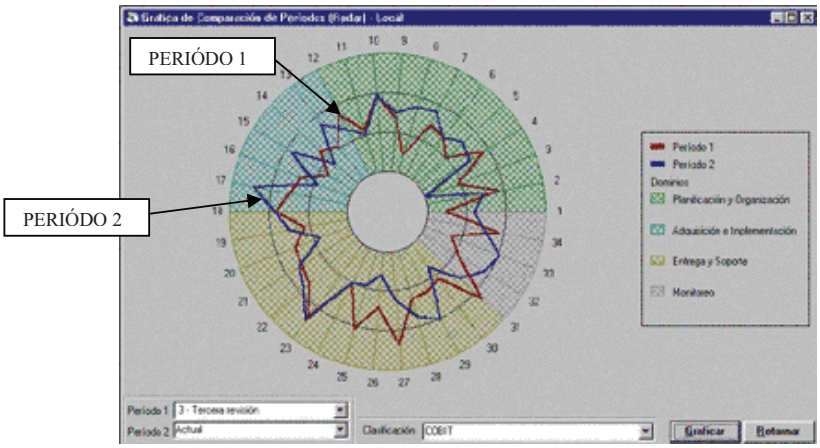


FIGURA 3.19 Dos diagnósticos con periodos sucesivos

CAPÍTULO 4

NORMAS, POLÍTICAS Y PROCEDIMIENTOS RELACIONADOS A LA GESTIÓN DE RIESGO

4.1 Normas de seguridad

Definición: Una norma es una regla a la que se debe ajustar la puesta en marcha de una operación. También se puede definir como una guía de actuación por seguir o como un patrón de referencia.

Las normas de seguridad se pueden considerar prácticamente como:

a. Normas de carácter **general**: son las universalmente aceptadas.
b. Normas de carácter **específico**: las que regulan una función, trabajo u operación específica.

Las ventajas de las normas:

- Representan un elemento de sistematización de seguridad
- Facilitan la comprensión y ejecución de las tareas de seguridad de forma clara y precisa
- Permiten la dirección eficaz del sistema de seguridad
- Impiden que existan vacíos acerca de la seguridad
- Facilitan la rápida formación y concientización del personal
- Permiten un manejo excelente de las instalaciones y equipos
- Homogenizan medios y procedimientos, además de facilitar la comunicación y la seguridad
- Aumentan el sentido de seguridad en el usuario

4.1.1 Características de las normas

- Debe hacerse una selección cuidadosa de todo aquello que se deba normalizar.

- Una vez seleccionado el objeto de normalización, debe atenderse a su conexión con las ordenanzas o reglamentos oficiales existentes, a fin de realizar un trabajo coherente con lo que está legalmente dispuesto.

- Se deberá atender también, antes de dictar una norma, a las ya existentes con objeto de evitar la duplicidad o contradicción que pueda plantearse y procurando expresar claramente la derogación de una norma que sea sustituida por otra en caso de considerar necesaria esta sustitución.

- Deben ser los más escuetas posibles, procurando no tratar más de un solo tema cada vez, a fin de lograr la máxima concreción y evitar confusiones que pudieran surgir.

- Deben utilizar un lenguaje claro en concordancia con el nivel cultural de las personas a quienes vaya dirigido, haciendo mediante notas o apéndices, todas las aclaraciones que se vayan considerando necesarias.

- La manera de redactar las notas debe ser imperativo, de forma que no queden dudas por lo que se refiere a la obligatoriedad de su cumplimiento.

- Deben ir escritas en un libro o folleto, hacer una introducción firmada por la dirección de la empresa, en la que se insista sobre la necesidad de su cumplimiento. Conviene prever la inclusión de hojas en blanco o un sistema de hojas recambiables que posibiliten la renovación, constitución y puesta al día de las normas existentes.

En México algunas de las normas con las que de preferencia se debería de contar son:

- NOM-001-STPS-2008, Edificios, locales, instalaciones y áreas en los centros de trabajo-Condiciones de seguridad. D.O.F. 24-XI-2008.

- NOM-002-STPS-2000, Condiciones de seguridad - Prevención, protección y combate de incendios en los centros de trabajo. D.O.F. 8-IX-2000. (aclaración D.O.F. 2-I-2001).

- NOM-004-STPS-1999, Sistemas de protección y dispositivos de seguridad de la maquinaria y equipo que se utilice en los centros de trabajo. D.O.F. 31-V-1999. (aclaración D.O.F. 16-VII-1999).

- NOM-006-STPS-2000, Manejo y almacenamiento de materiales - Condiciones y procedimientos de seguridad. D.O.F. 9-III-2001.

- NOM-007-STPS-2000, Actividades agrícolas - Instalaciones, maquinaria, equipo y herramientas-Condiciones de seguridad. D.O.F. 9-III-2001.

- NOM-009-STPS-1999, Equipo suspendido de acceso - Instalación, operación y mantenimiento- Condiciones de seguridad. D.O.F. 31-V-2000.

- NOM-010-STPS-1999, Condiciones de seguridad e higiene en los centros de trabajo donde se manejen, transporten, procesen o almacenen sustancias químicas capaces de generar contaminación en el medio ambiente laboral. D.O.F. 21-VIII-2000.

- NOM-017-STPS-2008, Equipo de protección personal - Selección, uso y manejo en los centros de trabajo. D.O.F. 9-XII-2008.

- NOM-019-STPS-2004, Constitución, organización y funcionamiento de las comisiones de seguridad e higiene en los centros de trabajo. D.O.F. 4-I-2005.

- NOM-025-STPS-2008, Condiciones de iluminación en los centros de trabajo. D.O.F. 20-XII-2008.

- NOM-029-STPS-2005, Mantenimiento de las instalaciones eléctricas en los centros de trabajo - Condiciones de seguridad. D.O.F. 31-V-2005.

4.2 Políticas de seguridad

Definición: Conjunto de leyes, reglas y prácticas que permiten salvaguardar los activos de una organización y brindar seguridad dentro de ésta.

4.2.1 ¿Qué son las políticas de seguridad informática (PSI)?

Una política de seguridad informática es una forma de comunicarse con los usuarios y los gerentes. Las PSI establecen de manera formal las responsabilidades del personal, en relación con los recursos y servicios informáticos, importantes de la organización. Es más bien una descripción de los que se desea proteger y el por qué de ello (he aquí la relación con la gestión de riesgos).

Cada PSI es consciente y vigilante del personal por el uso, limitaciones de los recursos, así como de los servicios informáticos críticos de la compañía.

4.2.2 Elementos de una política de seguridad informática

Una PSI debe orientar las decisiones que se toman en relación con la seguridad. Por tanto, requiere de una disposición por parte de cada uno de los miembros de la empresa para lograr una visión conjunta de lo que se considera importante. Las PSI deben considerar entre otros, los siguientes elementos:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica. Es una invitación de la organización a cada uno de sus miembros a reconocer la información como uno de sus principales activos, esto es como un motor de intercambio y desarrollo en el ámbito de sus negocios. Invitación que debe concluir en una posición.

- Objetivos de la política y descripción clara de los elementos involucrados en su definición.

- Responsabilidades por cada uno de los servicios y recursos informáticos a todos los niveles de la organización.

- Requerimientos mínimos para configuración de la seguridad de los sistemas que cobija el alcance de la política.

- Definición de violaciones y de las consecuencias del no cumplimiento de la política.

- Responsabilidades de los usuarios con respecto a la información a la que ella tiene acceso.

Las PSI deben ofrecer explicaciones comprensibles acerca de ¿Por qué deben tomarse ciertas decisiones?, transmitir ¿Por qué son importantes estos u otros recursos o servicios?

De igual forma, las PSI establecen las expectativas de la organización en relación con la seguridad y lo que ella puede esperar de las acciones que la materializan en la compañía. Deben mantener un lenguaje común libre de tecnicismos, como de términos legales que impidan una comprensión clara de las mismas, sin sacrificar su precisión y formalidad dentro de la empresa.

Por otra parte, la política debe especificar la autoridad que debe hacer que las cosas ocurran, el rango de los correctivos, sus actuaciones que permitan dar indicaciones sobre la clase de sanciones que se puedan imponer. No debe especificar con exactitud qué pasara o cuándo algo sucederá; no es una sentencia obligatoria de la ley.

Finalmente, las PSI como documentos dinámicos de la organización, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes.

Toda política debe contemplar:

- Disponibilidad (que siempre sea capaz de realizar las funciones en el tiempo que sea requerida)
- Utilidad (que tenga una finalidad concreta, no sólo que este por estar)
- Integridad (que sea lo más completa posible)
- Autenticidad (que sea genuina)
- Confidencialidad (que sea autorizado para ser entendido y leído sólo por algunas personas y entidades)
- Posesión (que este en derecho de un cierto grupo de personas o entidades).

4.2.3 Diseño de una política de Seguridad

Se debe hacer un análisis de riesgos para determinar:

- ¿Qué activos se tratan de proteger? (objetivos clave)
- ¿De quién o de qué se trata de proteger los activos?
- ¿Cuáles y cómo son las amenazas que afectan a tales activos?
- ¿Qué tan importante es el activo?
- ¿Qué medidas pueden ser implementadas para proteger el bien?
- ¿Cuál es el costo de tal medida y en qué tiempo puede ser implementada?
- ¿Quién autoriza a los usuarios?

Cuando se redacta un conjunto de políticas se decide una filosofía:

a) Prohibitiva: Todo está prohibido a excepción de lo permitido.

b) Permisiva: Todo está permitido a excepción de lo que está prohibido.

Entre las políticas más comunes se tienen las siguientes:

- **Políticas de seguridad física:** Medidas que se usan para proteger las instalaciones en las que reside un sistema de cómputo: llaves, candados, tarjetas de acceso, puertas, ventanas, alarmas, vigilancia, etc.

- **Políticas de cuentas:** Establecen qué es una cuenta de usuario de un sistema de cómputo, cómo está conformada, a quién puede serle otorgada, quién es el encargado de asignarlas, cómo deben ser creadas y comunicadas.

- **Políticas de contraseñas:** Son una de las políticas más importantes, ya que por lo general, las contraseñas constituyen la primera y tal vez única manera de autenticación, por tanto, la única línea de defensa contra ataques. Éstas establecen quién asignará la contraseña, qué longitud debe tener, a qué formato deberá apegarse, cómo será comunicada.

- **Políticas de control de acceso:** Especifican cómo deben los usuarios acceder al sistema, desde dónde y de qué manera deben autentificarse.

- **Políticas de respaldo:** Para el usuario: Será responsabilidad del usuario mantener una copia de la información de su cuenta. Para el administrador: Responsable de realizar respaldos de la información crítica.

- **Políticas de Seguridad:** Correo electrónico, contabilidad o inventario del sistema, de web, de direcciones IP. De contratación y finalización de relaciones laborales de recursos humanos en sistemas informáticos.

El enfoque está estructurado en tres elementos para una efectiva **gestión** de **riesgos**:

1. Los principios para la gestión de riesgos: Son una serie de declaraciones que deberían ser seguidas y respetadas por las organizaciones para lograr una gestión de riesgos efectiva, como por ejemplo: la gestión de riesgos debe crear y proteger el valor de la compañía, debe ser parte del proceso de toma de decisiones, debe estar integrado en todos los procesos de la organización.

2. La estructura de soporte: Establece los cimientos sobre los que debería construirse un proceso de gestión de riesgos exitoso. Los principales elementos de la estructura de soporte son: política de gestión de riesgos, integración con los procesos de negocio, información interna-externa, monitoreo, evaluación y mejora continua de la estructura.

3. El proceso: Establece las principales actividades a realizar durante la administración de los riesgos; como: la identificación, análisis, evaluación y tratamiento de los riesgos.

4.3 Normas y procedimientos que aplican a la gestión de riesgos

La tarea de gestión de riesgos, como se sabe, protege de efectos indeseados, ayudan a mejorar la productividad, trabajar en un ambiente más seguro, confiable y sobre todo digno de conocerse, para tal efecto, con normas y/o procedimientos ya definidos por las principales entidades encargadas de estándares (como por ejemplo la ISO), da el antecedente perfecto para que se obtengan certificaciones de seguridad de los sistemas de información y demás mecanismos de evaluación.

4.3.1 ISO 17799

4.3.1.1 Antecedentes del ISO 17799

Es importante entender los principios y objetivos que dan vida al ISO 17799, junto con los beneficios que cualquier organización, incluyendo las instituciones públicas, privadas y ambientes educativos pueden adquirir al implementarlo en sus prácticas de seguridad de la información.

El estándar de seguridad de la información ISO 17799, descendiente del BS 7799 – Information Security Management Standard – de la BSI (British Standard Institute) que publicó su primera versión en Inglaterra en 1995, con actualizaciones realizadas en 1998 y 1999, consiste de dos partes:

- Parte 1: Código de prácticas.
- Parte 2: Especificaciones del sistema de administración de seguridad de la información.

Por la necesidad generalizada de contar con un estándar de carácter internacional que permitiera reconocer o validar el marco de referencia de seguridad aplicado por las organizaciones, se elaboró el estándar ISO17799:2000, basado principalmente en la primera parte del BS 7799 conocida como Código de Prácticas (BS 7799 Part 1: Code of Practice).

4.3.1.2 ¿Qué es el ISO 17799?

En toda organización que haga uso de las tecnologías de información se recomienda implementar buenas prácticas de seguridad, porque en muchas ocasiones, el no seguir un proceso de implementación adecuado como el que establece el ISO 17799 puede generar huecos por la misma complejidad de las organizaciones, en ese sentido, aumenta la posibilidad de riesgos en la información.

Este estándar internacional de alto nivel para la administración de la seguridad de la información, fue publicado por la ISO (International Organization for Standardization) en diciembre de 2000 con el objeto de desarrollar un marco de seguridad sobre el cual trabajen las organizaciones.

El ISO 17799, al definirse como una guía en la implementación del sistema de administración de la seguridad de la información, se orienta a preservar los siguientes principios de la seguridad informática:

1. **Confidencialidad.** Asegurar que únicamente personal autorizado tenga acceso a la información.
2. **Integridad.** Garantizar que la información no será alterada, eliminada o destruida por entidades no autorizadas.
3. **Disponibilidad.** Asegurar que los usuarios autorizados tendrán acceso a la información cuando la requieran.

Estos principios en la protección de los activos de información constituyen las normas básicas deseables en cualquier organización, sean instituciones de gobierno, educativas e investigación; no obstante, dependiendo de la naturaleza y metas de las organizaciones, éstas mostrarán especial énfasis en algún dominio o área del estándar ISO 17799.

El objetivo de la seguridad de los datos es asegurar la continuidad de las operaciones de la organización, reducir al mínimo los daños causados por una contingencia, así como optimizar la inversión en tecnologías de seguridad.

Como todo buen estándar, el ISO 17799 da la pauta en la definición sobre cuáles metodologías, normas o estándares técnicos pueden ser aplicados en el sistema de administración de la seguridad de la información, se puede entender que estos estándares son auxiliares y serán aplicados en algún momento al implementar el mismo.

La aplicación de un marco de referencia de seguridad basado en el ISO 17799 proporciona beneficios a toda organización que lo implemente, al garantizar la existencia de una serie de procesos que permiten evaluar, mantener y administrar la seguridad de la información.

Las políticas, estándares locales y los procedimientos se encuentran adaptados a las necesidades de la organización, debido a que, el proceso mismo de su elaboración integra mecanismos de control y por último, la certificación permite a las organizaciones demostrar el estado de la seguridad de la información, situación que resulta muy importante en aquellos convenios o contratos con terceras organizaciones que establecen como requisito contractual la certificación BS7799.

4.3.1.3 Los controles del ISO 17799

El éxito de la implementación del estándar de seguridad ISO 17799 requiere de una serie de procedimientos donde, inicialmente, el análisis de riesgos identificará los activos de la información y las amenazas a las cuales se encuentra expuesta.

El análisis de riesgos guiará en la correcta selección de los controles que apliquen a la organización; este proceso se conoce en la jerga del estándar como Statement of Applicability, que es la definición de los controles que aplican a la organización con objeto de proporcionar niveles prácticos de seguridad de la información y medir el cumplimiento de los mismos.

A continuación, se describirán cada una de las diez áreas de seguridad mostradas en la figura 4.1, con el objeto de esclarecer los objetivos de estos controles.

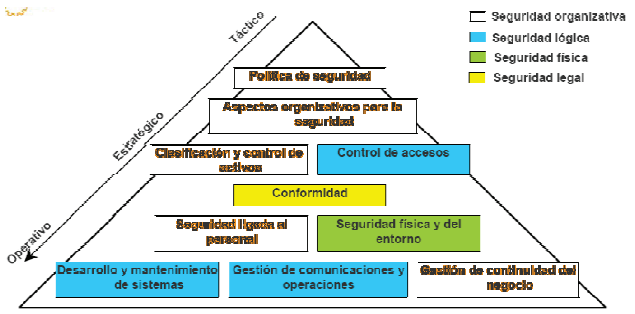


FIGURA 4.1 Controles del ISO 17799

- **Políticas de seguridad.** El estándar define como obligatorias las políticas de seguridad documentadas y procedimientos internos de la organización que permitan su actualización y revisión por parte de un Comité de Seguridad.

- **Seguridad organizacional.** Establece el marco formal de seguridad que debe integrar una organización, tales como un foro de administración de la seguridad de la información, un contacto oficial de seguridad (Information System Security Officer – ISSO), revisiones externas a la infraestructura de seguridad y controles a los servicios de outsourcing, entre otros aspectos.

- **Clasificación y control de activos.** El análisis de riesgos generará el inventario de activos que deberá ser administrado y controlado con base en ciertos criterios de clasificación y etiquetado de información, es decir, los activos serán etiquetados de acuerdo con su nivel de confidencialidad.

- **Seguridad del personal.** Contrario a lo que uno se puede imaginar, no se orienta a la seguridad del personal desde la óptica de protección civil, sino a proporcionar controles a las acciones del personal que opera con los activos de información.El objetivo de esta área es contar con los elementos necesarios para mitigar el riesgo inherente a la interacción humana, es decir, establecer claras responsabilidades por parte del personal en materia de seguridad de la información.

- **Seguridad física y de entorno.** Identificar los perímetros de seguridad, de forma que se puedan establecer controles en el manejo de equipos, transferencia de información y control de los accesos a las distintas áreas con base en el tipo de seguridad establecida.

- **Comunicaciones y administración de operaciones.** Integrar los procedimientos de operación de la infraestructura tecnológica y de controles de seguridad documentados, que van desde el control de cambios en la configuración de los equipos, manejo de incidentes, administración de aceptación de sistemas, hasta el control de código malicioso.

- **Control de acceso.** Habilitar los mecanismos que permitan monitorear el acceso a los activos de información, que incluyen los procedimientos de administración de usuarios, definición de responsabilidades o perfiles de seguridad y el control de acceso a las aplicaciones.

- **Desarrollo de sistemas y mantenimiento.** La organización debe disponer de procedimientos que garanticen la calidad y seguridad de los sistemas desarrollados para tareas específicas de la organización.

- **Continuidad de las operaciones de la organización.** El sistema de administración de la seguridad debe integrar los procedimientos de recuperación en caso de contingencias, los cuales deberán ser revisados de manera constante y puestos a prueba con la finalidad de determinar las limitaciones de los mismos.

- **Requerimientos legales.** La organización establecerá los requerimientos de seguridad que deben cumplir todos sus proveedores, socios y usuarios; éstos se encontrarán formalizados en los contratos o convenios.

Cada una de las áreas establece una serie de controles que serán seleccionados dependiendo de los resultados obtenidos en el análisis de riesgos, además, existen controles obligatorios para toda organización, como son de las políticas de seguridad cuyo número dependerá más de la organización que del estándar, el cual no establece este nivel de detalle.

4.3.1.4 Ventajas ISO/17799

- Aumento de la seguridad efectiva de los sistemas de información.
- Correcta planificación y gestión de la seguridad.
- Garantías de continuidad del negocio.
- Mejora continua a través del proceso de auditoría interna.
- Incremento de los niveles de confianza de nuestros clientes y partners.
- Aumento del valor comercial y mejora de la imagen de la organización

4.3.2 Serie 27000

La familia completa de la ISO 27000 está formada por los estándares mencionados a continuación.

ISO/IEC	Descripción
27000	Vocabulario y definiciones (*Information Technology – Information Security Management – Fundamentals and Vocabulary*).
27001	Especificación de la estructura metodológica (basada en el BS7799-2:2002) (*Information Technology –Security Techniques– Information Security Management Systems – Requirements*).
27002	Código de prácticas (*Code of Practice for Information Security Management*). Actualmente ISO/IEC 17799:2005, publicado el 15 de junio de 2005.
27003	Guía de implementación (ISMS *Implementation Guidance*, en desarrollo).
27004	Métricas y medidas (*Information Security Management Measurement,* en desarrollo).
27005	La Administración del Riesgo (basado BS 7799-3) (*Information Security Risk Managemen*t, basado e incorporado a ISO/IEC 13335 MICTS).
27006	Requerimientos para organismos de acreditación de Sistemas de Gestión de Seguridad de la Información (*Information Technology – Security Techniques – Requirements for Bodies Providing Audit and Certification of Information Security Management Systems*).

TABLA 4.1 Familia de estándares ISO 27000

Las certificaciones han pasado a ser necesidad para demostrar la existencia de sistemas de gestión, con objeto de asegurar procesos consistentes. En el campo de la seguridad informática se tenían certificaciones por parte de estándares británicos y españoles pero, hace pocos años, la ISO emitió los estándares por los sistemas de gestión de seguridad informática con objeto de certificar que las recomendaciones y buenas prácticas brinden una ventaja competitiva a las organizaciones, no dejar descubiertos todos los sistemas de información que día con día, cobran una mayor importancia para sustentar la toma de decisiones y salvaguardar el activo más importante de una organización: la información.

4.3.3 ISO 9000

Muchas veces, quienes conducen o toman decisiones tienen presente cierta cantidad de situaciones amenazantes, pero no forman parte de un proceso de decisión técnico avalado por método o procedimiento estándar. En consecuencia, no constan datos o registros estadísticos que permitan obtener proyecciones sobre cuál sería la probabilidad de que un suceso se materialice.

Ciertas organizaciones (industriales-automotrices, bioquímica, farmacéutica, servicios, etc.) no poseen un área destinada a tal análisis, sino que, en sus procesos de calidad (quienes poseen certificaciones en normas ISO u otro sistema de calidad), utilizan extractos de la metodología de riesgos solo para prevenir hitos en particular, estando más vinculado al cumplimiento de la norma que a las amenazas de todo el sistema de la empresa.

En una compañía o cualquier tipo de institución el tratamiento de los riesgos puede ser, Pasivo o Activo.

1. **El tratamiento Pasivo:** Se establecen o clasifican los distintos tipos de riesgos, primero se deben consignar los riesgos y analizar los factores que potencian esos riesgos; luego se efectúa un paneo[16] para identificar los riesgos físicos en forma tangible para finalmente dimensionar y/o ponderar el nivel de riesgo. La connotación de pasivo surge cuando una vez aplicados los controles o pautas de mitigación de riesgos, no resulta necesario efectuar procesos de análisis y evaluación de riesgos de manera diaria o constante, ya que para las condiciones de ese momento una vez mitigada la amenaza el riesgo estaría administrado; es decir, **no necesita revisiones permanentes de evaluación de riesgos**.

2. **El tratamiento Activo:** Está dirigido a situaciones donde dadas las características de la entidad o empresa, se requiere un **análisis constante y permanente de la evolución del riesgo**. Un ejemplo de esto son las empresas que poseen certificaciones en Normas ISO 9001, donde de manera constante se generan las llamadas **No Conformidades[17].**

Esta práctica resulta bastante molesta para quienes deben confeccionarlas, y si a esto se le suma las visitas de las Auditorías Internas de Calidad o las de Auditorías Externas, se vuelve una amenaza, considerando que el operador del sistema de calidad debe dar explicaciones de las no conformidades, cómo solucionó ese desvío, etc. (esto posee costo). Luego viene el informe del auditor y en este punto comienza el problema, sobre las acciones a tomar.

En cambio, si los responsables del sistema de calidad de la empresa, comienzan a relevar los puntos críticos de cada proceso, que conllevan a las "no conformidades", y procedieran a clasificar las causas de estas fallas en, "tipos de riesgos", podría montarse mini-sistemas de riesgos para cada hito evitando las No Conformidades con los costos que estas acarrean.

Si la empresa le asigna un valor cuantitativo a las no conformidades estará en condiciones de conocer cuantas veces se equivocó en un período determinado y a la vez comparándolo de

[16] Una observación en ambas direcciones de izquierda a derecha y viceversa,
[17] En ISO 9000 las No Conformidades son el incumplimiento de un requisito

manera porcentual con el total producido (Probabilidad o Frecuencia). Luego se puede asignar un valor o un costo a estos errores, costo de reproceso, costo de mano de obra, costo de insumos, otros costos (Impacto). Entre probabilidad o frecuencia y el impacto surge una nueva resultante, Consecuencia, donde la empresa estará en condiciones de evaluar:

- No aceptar ese nivel de pérdidas.
- El muy elevado nivel de error
- Pérdida de imagen frente a clientes por demoras en entrega; y en el caso de servicios, disconformidades por la prestación del mismo. Alto nivel de reproceso.
- Los empleados no están considerando como importante el estándar de calidad asumido.
- Otras consecuencias.

Si los requisitos de la norma **ISO 9001:2000** ya se han implementado en las prácticas, la organización deberá evaluar su sistema de calidad actual. Una forma rápida y eficaz para implementar el sistema ISO 9001:2000 es la de utilizar un paquete de documentación y productos de capacitación que incluye:

- Análisis de la situación
- Manual de calidad
- Procedimientos de la norma y documentos solicitados por la organización diseñados para construir el sistema requerido por la norma ISO 9001:2000
- Formularios
- Capacitación para los empleados
- Capacitación para el jefe de proyecto
- Capacitación para el auditor interno

Utilizando el paquete se podrá implementar un Sistema de Gestión de Calidad eficaz que llevará a la organización más allá de la simple documentación de los procesos: “una administración de riesgos eficaz”.

Al emplear métodos de implementación de Certificación ISO 9000, la empresa se beneficiará durante todos esos años de una gran experiencia, además, estará siguiendo el camino seguro hacia el éxito en su evolución y crecimiento futuro.

4.3.4 AS/NZS 4360:1999

Conjunto de Estándares de Australia y Nueva Zelanda de Administración de Riesgos(AS/NZS). Estándar australiano de administración de riesgos, es un proceso iterativo que consta de pasos, los cuales, cuando son ejecutados en secuencia, posibilitan una mejora continua en el proceso de toma de decisiones. El beneficio máximo se obtiene generalmente aplicando el proceso de administración de riesgos desde el principio, el proceso es el siguiente, ver figura 4.2.

FIGURA 4.2 Etapas AS/NZS 4360

El establecer el contexto, es definir los parámetros básicos dentro de los cuales debe administrarse el riesgo, así como el alcance para el resto del proceso de administración de riesgos los puntos clave en esta etapa son:

- Comprender la organización y sus capacidades, así como sus metas, objetivos y las estrategias que están vigentes para lograrlos.
- Definir la estructura bajo la cual se estarán tratando los riesgos: los elementos para identificarlos y analizarlos.
- Desarrollar y decidir los criterios internos y externos contra los cuales se va a evaluar el riesgo.
- Establecerse las metas, objetivos, estrategias, alcance (parte importante es establecer y designar recursos) y parámetros de la actividad a la cual se está aplicando el proceso de administración de riesgos.
- Definir la relación entre la organización y su entorno, identificando las fortalezas, debilidades, oportunidades y amenazas de la organización.

Como **segunda etapa** esta el identificar riesgos: Para identificarlos se responde a las siguientes preguntas:

- ¿qué?
- ¿cómo? y
- ¿por qué?

La tercera etapa consiste en analizar los riesgos de la cual en el capítulo 2 se abordo un tema al respecto, ésta tarea se hace con el fin de separar los riesgos menores aceptables de los riesgos mayores, proveer datos para asistir en la evaluación y tratamiento de los riesgos. Se puede analizar los riesgos desde tres tipos de análisis: cualitativo, semi-cuantitativo y cuantitativo.

- En el **análisis cualitativo** utiliza formatos de palabras (alto, bajo, medio, regular, muy alto, etc.) o escalas descriptivas (como una gráfica de barras por ej.) para describir la magnitud de las consecuencias potenciales y la probabilidad de que esas consecuencias ocurran.

- En el **análisis semi-cuantitativo** a las escalas cualitativas se les asignan valores en cualquier rango para producir un ordenamiento de prioridades más detallado(los valores asignados no tiene que guardar una relación precisa con la magnitud real de las consecuencias o probabilidades) y no sugerir valores realistas tales como los que se hacen en un análisis cualitativo.

- En el **análisis cuantitativo** se utilizan valores numéricos para las consecuencias y probabilidades: Las consecuencias pueden ser estimadas modelando los resultados de un evento o conjunto de eventos, o extrapolando a partir de estudios experimentales o datos del pasado. La probabilidad es expresada generalmente como una probabilidad, una frecuencia, o una combinación de exposición y probabilidad. La forma en que se expresan las probabilidades, las consecuencias y las formas en que las mismas son combinadas para proveer un nivel de riesgo variarán de acuerdo con el tipo de riesgo y el contexto en el cual se va a utilizar el nivel de riesgo.

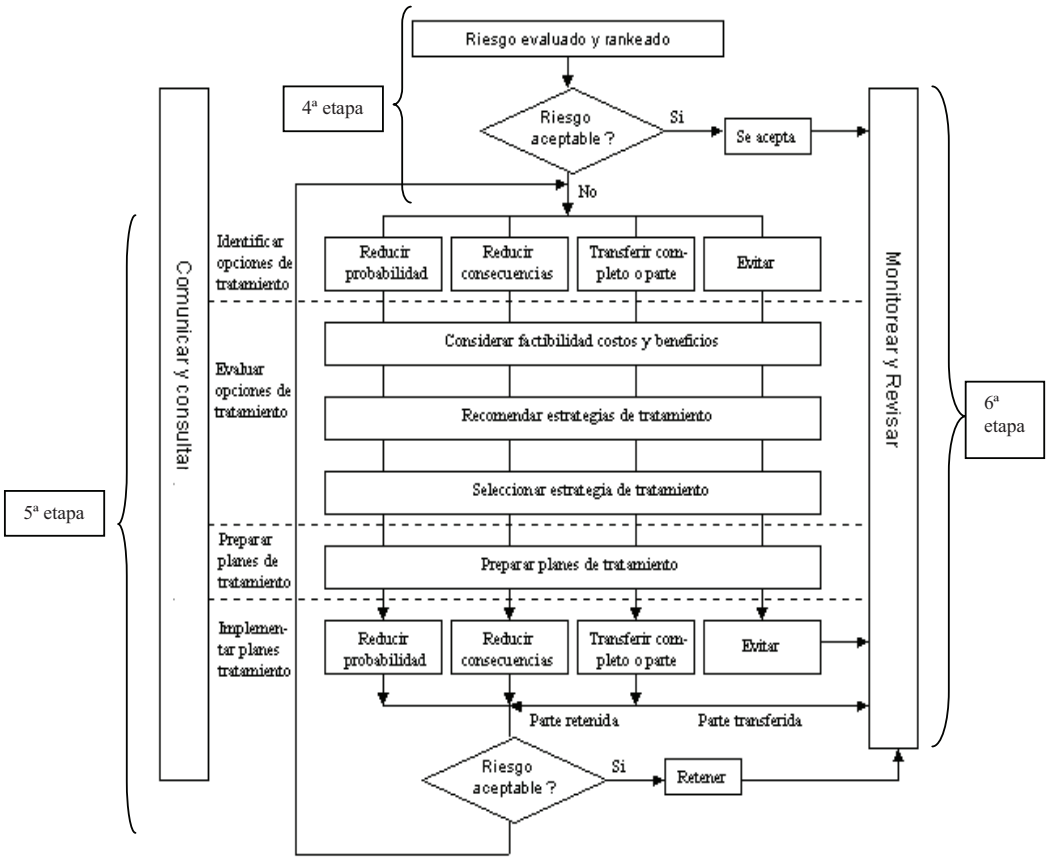


FIGURA 4.3 Etapa de tratamiento de riesgos (tercera, cuarta y quinta etapa)

La cuarta etapa es evaluar los riesgos que se tienen que comparar con los criterios que establecimos y asignamos prioridades a los riesgos.

La quinta etapa después de aceptar los riesgos que se evalúan es darle tratamiento a los mismos para ello se debe formular un propio plan de tratamiento en dónde identificar, evaluar y seleccionar las correctas opciones de tratamiento. En la siguiente figura se ilustra de forma más detallada esta etapa:

La sexta etapa es monitorear y revisar lo hecho en cada etapa para verificar la efectividad del tratamiento de riesgos para que en un caso particular se documenten los pros, así como contras de cada etapa y tratamiento aplicado.

NOTA IMPORTANTE: Entre cada etapa se debe comunicar y consultar los progresos o retrasos.

4.3.5 ISO 31000

En el 2009 se usaba mayoritariamente el estándar AS/NZS4360 y ahora en 2010 se opta por el nuevo estándar ISO 31000:2009 no es excluyente uno de otro es más aquellas compañías que avanzaron con la metodología australiana se les facilita la implementación de la ISO.

El 13 de Noviembre de 2009 fue publicada una norma oficial sobre la gestión de riesgos: la norma ISO 31000.

Entre las características generales están:

1. Establece los principios y directrices de carácter genérico sobre la gestión de riesgos.
2. Puede ser utilizado por cualquier institución pública, privada o empresa de la comunidad, grupo o individuo. Por lo tanto, la norma no es específica de cualquier industria o sector.
3. Se puede aplicar durante toda la vida de una organización, para una amplia gama de actividades, incluidas las estrategias y las decisiones, operaciones, procesos, funciones, proyectos, productos, servicios y activos.
4. Se puede aplicar a cualquier tipo de riesgo, cualquiera que sea su naturaleza, teniendo consecuencias positivas o negativas.

Aunque la norma ISO 31000:2009 proporciona directrices genéricas, no es la intención de promover la uniformidad de la gestión de riesgo a través de las organizaciones. El diseño, ejecución de planes de gestión del riesgo y los marcos se debe tomar en cuenta las diversas necesidades de una organización, sus objetivos particulares, el contexto, estructura, operaciones, procesos, funciones, proyectos, productos, servicios o activos específicos y las prácticas empleadas.

Se pretende que la norma ISO 31000:2009 se utilizará para armonizar los procesos de gestión de riesgos en las normas existentes y futuras. Proporciona un enfoque común en apoyo de las normas de control de riesgos específicos y/o sectores, y no sustituyen a las normas.

ISO 31000 está diseñado para ayudar a las organizaciones a:

- Aumentar la probabilidad de lograr los objetivos de fomentar una gestión proactiva.
- Ser consciente de la necesidad de identificar y tratar los riesgos en toda la organización.
- Mejorar la identificación de las oportunidades y amenazas.
- Cumplir con las exigencias legales y reglamentarias y las normas internacionales.
- Mejorar los informes financieros.
- Mejorar la capacidad de gobernar o dirigir.
- Mejorar la confianza de los interesados y la confianza.
- Establecer una base confiable para la toma de decisiones y la planificación de mejorar los controles.
- Efectivamente asignar y utilizar recursos para el tratamiento del riesgo.
- Mejorar la eficacia y eficiencia operativa.
- Mejorar la salud, seguridad, así como la protección del medio ambiente.
- Mejorar la prevención de pérdidas y de manejo de incidentes.
- Reducir al mínimo las pérdidas.
- Mejorar el aprendizaje organizacional.
- Mejorar la capacidad de resistencia de la organización.

Al mismo tiempo, la **ISO publica la Guía ISO 73:2009, el vocabulario de gestión de riesgos**, que complementa la norma ISO 31000, proporcionando una colección de términos y definiciones relativas a la gestión del riesgo.

Kevin W. Knight AM, Presidente del grupo de trabajo ISO que ha desarrollado el estándar explica: "ISO 31000 es un documento práctico que pretende ayudar a las organizaciones en el desarrollo de su propio enfoque de la gestión del riesgo".

4.3.6 Formas para el tratamiento de riesgos

4.3.6.1 Externas: Outsourcing

Para disminuir estos riesgos es recomendable considerar bien si realmente es necesario externalizar el servicio, así como, identificarlo, definirlo bien y establecer los objetivos que se quiere obtener como resultado de la contratación de outsourcing. Como sugerencia se debe tener un líder responsable del proceso y establecer criterios de todo el proceso.

El *outsourcing* se intenta traducir por "externalizar" ó "subcontratar" es un negocio con otros para que se ocupen de un servicio en particular que se quiera, las personas en las que se dejan

los activos deben ser altamente especializadas en el tema que compete; de preferencia debe contar con certificaciones reales y precisas del tema en sí, para el tema de gestión de riesgos la certificación que encaja es la de seguridad en sus diversas modalidades.

Algunas razones para las cuales contratar outsourcing:

- Reducción del coste de servicio subcontratado
- Concentración en las actividades principales de la empresa
- Mejora de la calidad de servicio
- Acceso a personal altamente calificado
- Simplificación de los procesos del negocio
- Reducción de los tiempos de llegada de los productos/ servicios de la empresa al mercado
- Reducción de los riesgos indirectos asumidos por la empresa

La mayoría de las consultoras de seguridad ofrecen auditorías, soluciones inmediatas o a nivel intermedio utilizando uno o combinaciones de los diversos modelos mencionados en capítulo 3 no es difícil encontrar el servicio de outsourcing, lo difícil es confiar en personas ajenas al negocio.

Riesgos de contratar un servicio de outsourcing:

- No alcanzar los objetivos marcados
- Pérdida de control del servicio y de pérdida del conocimiento interno
- Dependencia del proveedor
- Conflictos con el proveedor
- Conflictos internos
- Elección del proveedor
- Robo de información

Lo que no se debe dejar en manos de terceros es la realización y verificación de respaldos de información importante (backups*)*, no existe como tal un orden de las cosas que podríamos externalizar, las que no, porque depende de cada compañía y entorno. La externalización de procesos de negocio o servicios es recurrente en las épocas de crisis económica y generalmente se elige el proveedor de más bajo costo.

El creciente uso de las TIC aumenta la situación de subcontratación de puestos de trabajo, y por tanto, reduce el coste de la entrada de firmas. Según las estimaciones de la Asociación de Tecnologías de la Información de América (ITAA) el 2% de 10 millones de empleos en EE.UU. relacionados con la informática, han sido enviados al extranjero y 12% de las empresas de TI han externalizado el trabajo, el 77% de las empresas multinacionales usan outsourcing, el 72% de las empresas europeas lo han hecho mientras que el 71% de las empresas europeas y el 78% en los EE.UU. planea usar estos servicios en los próximos dos años.

En el caso de México, el INEGI muestra en la tabla 4.2 la proporción de las dependencias y entidades de la administración pública por servicios informáticos externos contratados

(outsourcing), según nivel de administración (Central, Paraestatal o Estatal), de los años 1995 a 2000.

Servicios informáticos externos	1995			1996			1998			1999			2000		
	C	P	E	C	P	E	C	P	E	C	P	E	C	P	E
Administración de equipo	2	5	2	1	4	0	7.1	6.3	14.3	0	2.3	13.3	0	2.1	12.5
Asesoría y consultoría informática	4	30	8	2	17	5	50.0	28.8	57.1	58.8	35.6	8	66.7	35.1	75
Capacitación en informática	10	50	10	6	32	5	78.6	65	100	88.2	72.4	86.7	83.3	69.1	93.8
Captura de datos	2	4	0	1	4	0	21.4	10	28.6	17.6	8	26.7	11.1	8.5	0
Desarrollo de sistemas	6	25	9	4	24	6	64.3	35	71.4	64.7	37.9	66.7	66.7	43.6	62.5
Infraestructura y servicios adicionales	5	18	6	3	15	2	21.4	23.8	28.6	47.1	26.4	40.0	38.9	38.3	43.8
Mantenimiento y reparación de equipo	16	76	17	8	59	6	85.7	91.3	71.4	94.1	92	80	100	92.6	81.3
Procesamiento de datos	2	4	0	1	2	0	0.0	5.0	14.3	5.9	3.4	6.7	5.6	4.3	18.8
Servicios de comunicación	8	22	8	6	29	1	64.3	73.8	57.1	58.8	60.9	53.3	5.6	3.2	6.3
Servicios de información	5	18	3	2	4	1	57.1	33.8	28.6	23.5	18.4	33.3	77.8	75.5	68.8
Otros	ND	ND	ND	4	5	ND	7.1	5	0	11.8	3.4	0	38.9	21.3	31.3

TABLA 4.2 Outsourcing contratado por nivel de Administración

NOTA:1995 Información de 16 dependencias, 99 entidades y 21 Estados
1996 Información de 9 dependencias, 84 entidades y 10 Estados
1998 Información de 14 dependencias, 84 entidades y 7 Estados
1999 Información de 17 dependencias, 94 entidades y 15 Estados
2000 Información de 15 dependencias, 59 entidades y 8 Estados
ND No disponible.
Fecha de actualización: Martes 24 de junio de 2003
Iniciales: CPE: Central, Paraestatal y Estatal respectivamente.
FUENTE: **INEGI**. Encuesta Informática de la Administración Pública (varios años).

4.3.6.2 Internas: Matriz de riesgo

La otra forma de gestionar los riesgos es apoyarse del departamento encargado de la seguridad del negocio y formular una guía para la administración del riesgo remitida por dicho departamento u Oficina de Control Interno por ejemplo: el Departamento de Calidad y elaborar una matriz basada en probabilidades y consecuencias como la de la figura 4.4, la matriz de riesgo se abordará en el siguiente capítulo.

PROBABILIDAD DE OCURRENCIA	ALTA			
	MEDIA			
	BAJA			
SEVERIDAD/ IMPACTO DE LAS CONSECUENCIAS		BAJA	MEDIA	ALTA

FIGURA 4.4 Elaboración de Matriz de Riesgo

CAPÍTULO 5

MATRIZ DE RIESGOS

5.1 Definición

Matriz de riesgo: Es una herramienta gráfica que junto con el análisis de riesgo, permite determinar de una manera cuantitativa la verdadera severidad de los riesgos que se identifican.

Se puede realizar una matriz por cada riesgo identificado ó se puede realizar una matriz única dinámica, en la cual se involucren todos los riesgos identificados junto con su probabilidad y su impacto.

PROBABILIDAD DE OCURRENCIA	ALTA			
	MEDIA			
	BAJA			
SEVERIDAD/ IMPACTO DE LAS CONSECUENCIAS		BAJA	MEDIA	ALTA

TABLA 5.1 Esquema general de una matriz de riesgo

5.2 Elaboración

Es muy importante aclarar que se pueden identificar impactos tanto negativos como positivos y ambos deben tomarse en cuenta. La asignación de prioridad depende de la clasificación que se haya hecho de probabilidad vs impacto, de acuerdo con lo expuesto hasta el momento, la estimación de riesgo (ER) más acertada es el producto de la probabilidad de que un determinado peligro produzca un cierto daño (P) por el impacto (I) o por el número de veces que ocurre (frecuencia, F):

ER = P * I

ER = P * F

ER = Estimación de riesgo
P = Daño que produce
I = Impacto que produce
F =Frecuencia

NIVEL PROBABILIDAD P	NIVEL IMPACTO I	NIVEL DE RIESGO (SEVERIDAD) P x I	PRIORIDAD AUDITORIA
Casi Certeza (5)	Catastróficas (5)	EXTREMO (25)	PRIORIDAD ALTA
Casi Certeza (5)	Mayores (4)	EXTREMO (20)	PRIORIDAD ALTA
Casi Certeza (5)	Moderadas (3)	EXTREMO (15)	PRIORIDAD ALTA
Casi Certeza (5)	Menores (2)	ALTO (10)	PRIORIDAD MEDIA ALTA
Casi Certeza (5)	Insignificantes (1)	ALTO (5)	PRIORIDAD MEDIA ALTA
Probable (4)	Catastróficas (5)	EXTREMO (20)	PRIORIDAD ALTA
Probable (4)	Mayores (4)	EXTREMO (16)	PRIORIDAD ALTA
Probable (4)	Moderadas (3)	ALTO (12)	PRIORIDAD MEDIA ALTA
Probable (4)	Menores (2)	ALTO (8)	PRIORIDAD MEDIA ALTA
Probable (4)	Insignificantes (1)	MODERADO (4)	PRIORIDAD MEDIA
Moderado (3)	Catastróficas (5)	EXTREMO (15)	PRIORIDAD ALTA
Moderado (3)	Mayores (4)	EXTREMO (12)	PRIORIDAD ALTA
Moderado (3)	Moderadas (3)	ALTO (9)	PRIORIDAD MEDIA ALTA
Moderado (3)	Menores (2)	MODERADO (6)	PRIORIDAD MEDIA
Moderado (3)	Insignificantes (1)	BAJO (3)	PRIORIDAD BAJA
Improbable (2)	Catastróficas (5)	EXTREMO (10)	PRIORIDAD ALTA
Improbable (2)	Mayores (4)	ALTO (10)	PRIORIDAD MEDIA ALTA
Improbable (2)	Moderadas (3)	MODERADO (6)	PRIORIDAD MEDIA
Improbable (2)	Menores (2)	BAJO (4)	PRIORIDAD BAJA
Improbable (2)	Insignificantes (1)	BAJO (2)	PRIORIDAD BAJA
muy improbable (1)	Catastróficas (5)	ALTO (5)	PRIORIDAD MEDIA ALTA
muy improbable (1)	Mayores (4)	ALTO (4)	PRIORIDAD MEDIA ALTA

Tabla 5.2 Estimación de riesgo

Hasta el momento son 2 las etapas mencionadas: identificación del peligro y estimación el riesgo. Las siguientes etapas son: valorar el riego y por último controlarlo. La organización suele establecer las combinaciones específicas de probabilidad e impacto que llevan a un riesgo ser clasificado como extremo, alto, muy alto, moderado, bajo y las combinaciones que la organización asigne.

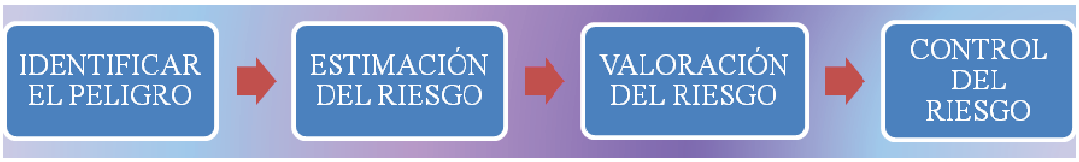


FIGURA 5.1 Etapas para elaborar matriz de riesgo

VALORACIÓN DEL RIESGO

La tabla 5.3 muestra los principales objetivos que se plantean al cubrir un análisis de riesgo.

OBJETIVO DEL PROYECTO	MUY ALTO	ALTO	MODERADO	BAJO	MUY BAJO
Alcance	El elemento terminado del proyecto es efectivamente inservible	Reducción del alcance inaceptable para el patrocinador	Áreas de alcance principales afectadas	Áreas de alcance secundarias afectadas	Disminución del alcance apenas perceptible
Calidad	El elemento terminado del proyecto es efectivamente inservible	Reducción de la calidad inaceptable para el patrocinador	La reducción de la calidad requiere la aprobación del patrocinador	Sólo las aplicaciones muy exigentes se ven afectadas	Degradación de la calidad apenas perceptible
Coste	Aumento del coste mayor al 40%	Aumento del coste del 20-40%	Aumento del coste del 10-20%	Aumento del coste menor al 10%	Aumento del coste insignificante
Tiempo	Aumento del tiempo mayor al 40%	Aumento del tiempo del 20-40%	Aumento del tiempo del 10-20%	Aumento del tiempo menor al 10%	Aumento del tiempo insignificante

TABLA 5.3 Principales objetivos en un análisis de riesgo

Con los principales objetivos definidos en la tabla 5.3 y la tabla 5.4 se hace una valoración del riesgo.

Probabilidad	Consecuencias				
	1 (insignificantes)	2 (menores)	3 (moderadas)	4 (mayores)	5 (catastróficas)
A(Casi segura)	Alto	Alto	Extremo	Extremo	Extremo
B(Probable)	Moderado	Alto	Alto	Extremo	Extremo
C(Posible)	Bajo	Moderado	Alto	Extremo	Extremo
D(Poco probable)	Bajo	Bajo	Moderado	Alto	Extremo
E(Rara)	Bajo	Bajo	Moderado	Alto	Alto

TABLA 5.4 Matriz de análisis cuantitativo de riesgo

CONTROL DEL RIESGO

Los diversos controles o tratamientos que existen para abordar un riesgo son de tipo preventivo, correctivo y detectivo (que actúan antes, durante o al finalizar un proceso respectivamente). Las principales formas de tratamiento o control son las siguientes:

- Mitigar
- Transferir
- Dejar
- Reducir
- Evitar
- Compartir
- Reciclar
- Impulsar
- Comunicar y Otras definidas por cada organización

Durante el tratamiento de un riesgo se verifica si se tienen controles existentes, si los hay es necesario describirlos y aclarar si son preventivo, correctivo o detectivo, ya que ayudaran a atacar más rápido el riesgo y a evaluar de forma rápida, si el control existente sirve o no. Para esto último se debe responder a las siguientes preguntas: ¿Disminuye el nivel de probabilidad de riesgo?, ¿Disminuye el nivel de impacto de riesgo?, ¿Es efectivo para minimizar el riesgo?, ¿Los controles están documentados?, si se responde no a la última pregunta no es seguro aplicar el control existente ya que el resultado que arroje será incierto, en cambio si se responde si a una o a las 4 preguntas si es recomendable usar el control existente.

5.3 Ejemplo

El siguiente ejemplo es un extracto de un trabajo de la materia de depósitos de datos se refiere a la programación de un canal de televisión que transmite programación nacional y de cadenas de Estados Unidos. El canal de televisión es nuevo, así que, los riesgos que aquí se corren involucran mucho dinero porque se transmitirán, series, telenovelas, programas educativos, de concursos y por su puesto comerciales, en el ejemplo como nivel de riesgo alto he puesto la pérdida de un equipo de transmisión o satélite (algo que pareciera fantasioso pero no irrealizable) puesto que no es algo que se pueda controlar tan fácil, causaría una estimación de riesgo inaceptable y por tanto el tratamiento sólo podría ser transferirlo o compartirlo pero jamás reducirlo (sería imposible) o evitarlo debido a que sería catastrófico.

En caso contrario ahora un efecto positivo se tiene aumento de rating en el canal con probabilidad baja y valoración leve (Lo cual es razonable esto porque apenas el público empieza a conocer al canal) entonces la estimación de riesgo es:

$$ER = P * I$$

$$ER = P * F$$

P= 1 e I = 5, por lo tanto, ER = 1 * 5 = 5

Según la clasificación (tabla de clasificación P vs I) se tiene un riesgo bajo (estado verde); es decir, algo que puede que no afecte es aceptable y el control o tratamiento que se le otorgue es asumir el riesgo, dejarlo y compartirlo.

Matriz de riesgo a emplear y escala de colores a usar

Probabilidad	alta	3	15	30	60
	media	2	10	20	40
	baja	1	5	10	20
	Valoración		5	10	20
			leve	moderada	catastrófico
			Impacto		

Tabla 5.5 Ejemplo de clasificación P vs I

Combinaciones						
Probabilidad	Impacto	Producto	Nivel de riesgo	Resultado	Tratamiento	
1	5	5	8%	Bajo	Aceptable	Asumir el riesgo. Permite a la Entidad asumirlo, es decir, el riesgo se encuentra en un nivel que puede aceptarlo sin necesidad de tomar otras medidas de control diferentes a las que se poseen.
1	10	10	17%	Bajo	Tolerable 1	Asumir o reducir el riesgo. Se deben tomar medidas para llevar los Riesgos a la Zona Aceptable o Tolerable, en lo posible.
2	5	10	17%	Bajo	Tolerable 2	Asumir o reducir el riesgo. Se deben tomar medidas para llevar los Riesgos a la Zona Aceptable o Tolerable, en lo posible. Cuando la Probabilidad del riesgo es media y su Impacto leve, se debe realizar un análisis del costo beneficio con el que se pueda decidir entre reducir el riesgo, asumirlo o compartirlo.
3	5	15	25%	Medio	Moderado 1	Evitar el riesgo, se deben tomar medidas para llevar los Riesgos a la Zona Aceptable o Tolerable, en lo posible, los Riesgos de Impacto leve y Probabilidad alta se previenen.

2	10	20	33%	Medio	Moderado 2	Reducir, Evitar, Compartir o transferir el riesgo. Se deben tomar medidas para llevar los Riesgos a la Zona Aceptable o Tolerable, en lo posible. También es viable combinar estas medidas con evitar el riesgo cuando éste presenta una Probabilidad alta y media, y el Impacto es moderado o catastrófico. Los Riesgos con Impacto moderado y Probabilidad media, se reducen o se comparte el riesgo, si es posible.
1	20	20	33%	Medio	Moderado 3	Reducir, Compartir o transferir el riesgo. Cuando el riesgo tiene una Probabilidad baja e Impacto catastrófico se debe tratar de compartir el riesgo y evitar la entidad en caso de que éste se presente. Siempre que el riesgo es calificado con Impacto catastrófico la Entidad debe diseñar planes de contingencia, para protegerse en caso de su ocurrencia.
3	10	30	50%	Alto	Importante 1	Reducir, Evitar, Compartir o transferir el riesgo. Se deben tomar medidas para llevar los Riesgos a la Zona Aceptable o Tolerable, en lo posible. También es viable combinar estas medidas con evitar el riesgo cuando éste presenta una Probabilidad alta y media, y el Impacto es moderado o catastrófico.
2	20	40	67%	Alto	Importante 2	Reducir, Evitar, Compartir o transferir el riesgo. Se deben tomar medidas para llevar los Riesgos a la Zona Aceptable o Tolerable, en lo posible. También es viable combinar estas medidas con evitar el riesgo cuando éste presenta una Probabilidad alta y media, y el Impacto es moderado o catastrófico. Siempre que el riesgo es calificado con Impacto catastrófico la Entidad debe diseñar planes de contingencia, para protegerse en caso de su ocurrencia.
3	20	60	100%	Alto	Inaceptable	Evitar, Reducir, Compartir o transferir el riesgo. Es aconsejable eliminar la actividad que genera el riesgo en la medida que sea posible, de lo contrario se deben implementar controles de prevención para evitar la Probabilidad del riesgo, de Protección para disminuir el Impacto o compartir o transferir el riesgo si es posible a través de pólizas de seguros u otras opciones que estén disponibles. Siempre que el riesgo sea calificado con Impacto catastrófico la Entidad debe diseñar planes de contingencia, para protegerse en caso de su ocurrencia.

Tabla 5.6 Control de riesgo

Nº	Descripción del riesgo	Controles existentes	Riesgo	Opciones manejo
1	Dejar de registrar el nombre de un programa en la lista de inscritos o en la base de datos	Entregar por parte de la Secretaria de Administración, mediante relación las solicitudes de inscripción (ver procedimiento para la elaboración de listas para candidatos)	Medio	Reducir, Compartir o transferir el riesgo. Cuando el riesgo tiene una Probabilidad baja e Impacto catastrófico se debe tratar de compartir el riesgo y evitar la entidad en caso de que éste se presente. Siempre que el riesgo es calificado con Impacto cata
6	Pérdida inaceptable de audiencia	1.Sondeo de gustos del público 2.Publicidad 3 (regalar artículos pre promocionales)	Medio	Reducir, Evitar, Compartir o transferir el riesgo. Se deben tomar medidas para llevar los Riesgos a la Zona Aceptable o Tolerable, en lo posible. También es viable combinar estas medidas con evitar el riesgo cuando éste presenta una Probabilidad alta y media, y el Impacto es moderado o catastrófico. Los Riesgos con Impacto moderado y Probabilidad media, se reducen o se comparte el riesgo, si es posible.
8	Catástrofe natural:(Inundación, Huracán y/o Temblor)	Poner a funcionar lo servidores distribuidos y los respaldos de cualquiera de los 2 países (MÉXICO Y/O USA)2.Transmitir desde el lugar del incidente	Bajo	Asumir o reducir el riesgo. Se deben tomar medidas para llevar los Riesgos a la Zona Aceptable o Tolerable, en lo posible.

TABLA 5.7 Extracto del mapa de riesgos

Nº	Descripción del riesgo	Probabilidad (%)	Controles existentes	¿Disminuye el nivel de probabi-lidad del riesgo?	¿Disminuye el nivel de impacto del riesgo?	Fuente	Valoración riesgo
1	Dejar de registrar el nombre de un programa en la lista de inscritos o en la base de datos	11	Revisar todas las solicitudes de inscripción	no	no	errores	Moderado
2	Que algún candidato no cumpla con la totalidad de los requisitos establecidos	5	No contratar y /o promoverle otra entrevista	no	no	fallas	Moderado
3	Dejar de transmitir noticieros de origen estadounidense	20	1.Pérdida de credibilidad del público estadounidense y habla hispana en E.U.A.	no	no	incumplimiento	Moderado
4	Pérdida de satélite y/o equipo de transmisión	0,2	Entregar informe urgente de pérdida de equipo invaluable y presentar reporte de inventario con carácter urgente	no	no	externa	fuerte
5	Huelga de trabajadores	0,3	1.Tomar control de asistentes 2.Contratar gente nueva 3.Escuchar peticiones	si	si	abuso	Moderado
6	Pérdida inaceptable de audiencia	41	1.Sondeo de gustos del público	si	si	planeación	fuerte

			2.Publicidad nivel 3 (regalar artículos pre promocionales)				
7	Fallas en suministro eléctrico	9	1.Comprar plantas generadores de electricidad	si	si	fallas	Moderado
8	Catástrofe natural:(Inundación, Huracán y/o Temblor)	22	Poner a funcionar lo servidores distribuidos y los respaldos de cualquiera de los 2 países (MÉXICO Y/O USA)2.Transmitir desde el lugar del incidente	si	si	natural-externa	significante

TABLA 5.8 Mapa de riesgos completo

5.4 Ventajas y desventajas de la matriz de riesgo

5.4.1 Ventajas

- Colabora en decisiones referentes a la gestión de diversos acontecimientos que interfieren en el cumplimiento de los objetivos.
- Por ser técnicas cuantitativas para calificar los riesgos tiene gran importancia cuando se reporta responsabilidades en términos financieros.
- Rápido y relativamente fácil de usar. Si la evaluación ha sido debidamente estructurada, los eventos riesgosos pueden ser considerados por turnos, por probabilidad y consecuencias generales identificadas.
- Los usuarios ganan generalmente un conocimiento general de la comparación de los riesgos en eventos riesgosos.
- La matriz puede ser empleada para separar los eventos riesgosos en clases de riesgos.

5.4.2 Desventajas

- En casos complicados, es bastante difícil asignar probabilidades a las incertidumbres.
- A medida que se consideran eventos más complejos, la intuición se hace cada vez menos confiable.
- Impreciso. Los eventos riesgosos los cuales caen bajo la misma clase pueden representar sustancialmente diferentes niveles de riesgo.
- Dificulta la comparación de eventos dentro de la misma base.
- La comparación entre clases de riesgos puede conducir a inconsistencias.
- No existe una clara justificación del proceso empleado para calificar la severidad de las consecuencias.

CONCLUSIONES

Actualmente un sistema de información junto con una buena administración nos permite manejar nuestros recursos de una manera eficiente, organizada y confiable. Una buena administración nos asegura calidad en nuestros procesos y la satisfacción del cliente (el cual es el elemento principal para los encargados de Tecnologías de la Información), los principios de administración de Fayol son una buena guía para administrar correctamente a las empresas.

México está tomando fuerza en el campo de las TI especialmente en la parte de educación, la capacitación para el uso y desarrollo de las tecnologías, considero será un tema muy importante que se tiene que tratar en un futuro no muy lejano y tal vez algún día las certificaciones en esta rama ya no serán un adicional, sino una necesidad.

La ventaja del análisis de riesgo radica en que es posible no ser experto en el tema para conocer el ¿qué?, ¿cómo? y ¿cuándo? alguna amenaza nos tome por sorpresa. Si seguimos el esquema básico de análisis de riesgo se tiene la seguridad que no se olvidará considerar alguna oportunidad o en el caso negativo, alguna amenaza negativa.

El análisis de riesgo no es una tarea sencilla, pero debido su carácter retroactivo, si no se consideró alguna oportunidad u amenaza, se puede integrar al proceso del análisis desde la etapa de identificación de riesgos y continuar con las demás etapas, hasta llegar a la etapa final: la de comunicación. Si se administran los riesgos gozamos de un ambiente de competitividad mundial, estamos preparados para los cambios tecnológicos, sociales y se puede tomar la decisión de qué escenarios aceptar y cuáles no.

De los métodos que mencioné actualmente los más usados son: ITIL, COBIT, CRAMM Y MAGERIT éste último sigue en apogeo desde la década de los 90's. Los métodos conllevan a que las etapas o fases son similares; dichas fases son: identificar riesgos, clasificarlos, evaluar su impacto y por último el tratamiento de los mismos, sólo que unos métodos traen consigo manuales, hojas informativas, software con complementos necesarios, hojas de registro, tablas de referencia y más o de lo contrario no funcionan al 100%. De los métodos, el método COBIT consta de un software integral, contiene en primer lugar una serie de preguntas las cuales deben ser contestadas de manera afirmativa o negativa hasta concluir con las 7 etapas.

Para la identificación de las áreas más críticas usa colores para diferenciar el estado deseado del estado obtenido; mientras MOSLER Y MAGERIT emplean símbolos o mezclas de renglones junto con viñetas diferentes. Otra ventaja de COBIT sobre todos los otros métodos, es la capacidad de representar simultáneamente estados diferentes que se obtienen de introducir factores y riesgos a lo largo del análisis que se hace durante las 7 etapas; esto es muy útil en el caso de necesitar comparar que nos conviene más: Si seguir el plan de seguridad lanzado primero o mejor aplicar el arrojado bajo otros factores o propiamente dicho el obtenido en las otras gráficas. No está de más mencionar que la documentación es poca pero sustancial y clara. Recomiendo mucho este método.

El método MOSLER sólo es recomendable usar cuando en realidad no sabemos el nivel de magnitud que tendrán nuestros riesgos; es decir, desde muy bajo, normal hasta un nivel elevado, es un método meramente operacional, dónde cada cálculo modifica en mucho al posterior cálculo(me refiero a los cálculos que se tienen que hacer con los 6 criterios), si no se tiene cuidado se obtienen resultados erróneos de 80% por ello recomiendo que el encargado de

esta tarea no sea el líder de grupo o proyecto, sino una persona que se dedique exclusivamente al desarrollo del análisis del riesgo (como debería ser el caso), por la cantidad de tiempo y precisión que se debe de llevar a cabo. Como punto final quiero destacar que este método es el ideal para novatos o principiantes en el análisis de riesgos, porque así se asegura que no harán planes y recomendaciones intuitivamente ni de manera superficial.

El método MAGERIT dejo elementos a considerar tanto buenos como malos; como punto bueno lleva más de 10 años en implementación, eso nos dice que es un buen método, por otra parte el punto malo los que no conocen una notación XML, él cual es el identificador único de la posición jerárquica dentro del proceso de identificación de activos, que sirve como base para manipular las siguientes etapas, resulta monótono estar consultando el "Catálogo de Elementos de MAGERIT versión 2", en mi caso desde la primera etapa tuve el inconveniente de consultar dicho catálogo para poder ejemplificar de forma general, como se desempeña cada etapa; tome los activos raíz, por ejemplo, del activo Servicios con código [S], entre sus "servicios hijos" por llamarlos de una manera tiene a [www] world wide web junto con otros 16 "servicios hijos" más, pero repito, para no introducir tanta nomenclatura sólo utilice los activos raíz o padre, para conocer los otros "hijos" de activos sugiero ver el documento mencionado ya anteriormente.

Del software Cramm versión express no me parece que se tenga que solicitar vía email, la razón es por la que piden los datos personales y sólo se da una pequeña demostración online, la cual no es suficiente para conocer el software a fondo y decidirse si evolucionar a la versión expert o seguir usando esa. CRAMM versión expert nos lleva a un registro en línea, el cual solo proporciona una pequeña demostración en línea. Otra forma de conocer la demostración es hablar por teléfono ó dejar datos vía email ó ir personalmente a la oficina de Siemens Enterprise Communications Ltd en Inglaterra, dónde supongo también se proporciona la misma demostración pero un poco más formal. Al ser un software actualmente usado por varios gobiernos como el de Inglaterra (principalmente), ejércitos (el de Holanda) y OTAN comprendo que sea tan restringida la información, demostraciones y datasheets para personas como: estudiantes, profesores e incluso si eres Gerente de TI.

MARION, el método francés surgido en 1985 es concreto y preciso (la fórmula del método es responder un cuestionario y al final muestra una gráfica donde se interpreta contramedidas, estado actual y factores a tomar en cuenta), pero ya no hay ligas de descarga ni información en la que solía ser su página oficial: http://www.clusif.asso.fr/; el cuestionario, no se encontro en internet o en libros. La información que existe de este método es muy poca e incluso la mayoría se encuentra en francés.

La idea general del método la obtuve de la poca información que se encontró, en la página de la CLUSIF se hace notar mucho la metodología MEHARI (sucesora de MARION Y MELISA) de ella si hay al alcance información en formato pdf; en español sólo está la introducción (13 páginas) al método, mientras que en inglés, francés e italiano está la documentación completa. Ésta metodología es recomendable ya que se tiene al alcance todos los documentos necesarios.

MELISA tuvo origen militar, se dice que fue comprado por Telindus, empresa de servicios y soluciones en TIC con presencia en 14 países de Europa (http://www.telindus.be), lo que se sabe de la metodología es que fue abandonada por sus compradores, por tanto, ya no es usada a

pesar de su implementación ampliamente en la década de los 80´s y mediados de los 90's en su país natal Francia.

ITIL no es precisamente una metodología para analizar y gestionar riesgos, pero lo hace, se desarrollo a finales de 1980 pero es hasta ahora en el siglo XXI que se está convirtiendo en el estándar de uso para la gestión de servicios de TI, en el caso de México, es una de las metodologías más usadas ITIL maneja la Gestión de incidencias y problemas, controlando estos dos es más fácil gestionar los demás servicios de TI. Para las empresas que se dedican exclusivamente a servicios ITIL es la mejor metodología a usar, está conformado de manera íntegra de forma que al ejecutar bien un proceso automáticamente te permite tener la seguridad de que el proceso subsecuente también funcionará correctamente.

Las políticas, normas y procedimientos sirven para regular y apoyar actividades dentro de un campo determinado, para México las NOM (Norma Oficial Mexicana) ya poseen un carácter de obligatoriedad; todas se refieren a la seguridad tanto exterior como interior (de edificios y de trabajadores), la ventaja más importante de contar con NOM se debe a que representa el elemento fundamental para sistematizar la seguridad. La STPS (Secretaria de Trabajo y Previsión y Social), es la encargada de desarrollar estas normas y verificar el cumplimiento de las mismas. Voy a destacar que mencione en este capítulo algunas normas con las que se debería contar; esto no significa que son las únicas hay muchas más, cada norma se conforma de complementos, actualizaciones, apartados y/o modificaciones.

La matriz de riesgos tiene muchas variantes una de ellas es el Análisis de Retorno de Inversiones (ROI) la diferencia varía que en este se coloca el costo de las consecuencias, por ejemplo, si hay huelga de trabajadores el costo correspondiente es el debido a liquidaciones y pérdida de clientes por desprestigio.

La matriz de riesgo es una herramienta poderosa y sencilla de aplicar me inclino por ella en vez de utilizar servicios de outsourcing, por la razón que es de uso interno y se corre menor riesgo de robo de información y conflictos con dichos proveedores, además, nadie más conoce más la empresa, organismo o institución que los mismos empleados que la conforman, de esta forma se asegura que la estimación de impacto, nivel de severidad y las veces que ocurre el riesgo son datos reales y útiles, más no infundados o inventados, porque se basan en experiencias pasadas o el conocimiento mismo del lugar y la situación a través de los años.

GLOSARIO

Amenaza: Fenómeno, evento o situación causada de forma natural o por acto humano que podrían generar pérdidas, heridas o peligro.

Anquilostomiasis: Enfermedad parasitaria producida por anquilostomas que provoca anemia y hemorragias intestinales crónicas.

Carbunco: o Antrax enfermedad que afecta principalmente al ganado vacuno y a otros mamíferos herbívoros, pero también puede afectar a personas que hayan estado en contacto con animales infectados.

Diagrama de causa y efecto: Véase Diagrama de Ishikawa.

Diagrama de espina de pescado: Véase Diagrama de Ishikawa.

Diagrama de Ishikawa: Herramienta creada por el ingeniero japonés Dr.Kaoru Ishikawa en el año 1943, método gráfico compuesto por una flecha mayor horizontal que apunta hacia la derecha señalando el problema objetivo a estudiar y con flechas menores alternantes que apuntan al cuerpo de la flecha horizontal, reflejando la relación entre una característica de calidad (variación) y los factores que contribuyeron a su existencia (variables 6 m's);es decir, es un gráfico que relaciona un problema con sus causas potenciales. En este gráfico del lado derecho de la flecha mayor horizontal se anota el problema y del lado izquierdo se especifican todas sus causas potenciales de tal manera que se agrupan y se colocan en orden prioritario según su importancia de acuerdo a su similitud en ramas o subramas en las flechas menores alternantes.

Dominio: Es el nombre que identifica un sitio web. Cada dominio tiene que ser único en Internet. Un solo servidor web puede servir múltiples páginas web de múltiples dominios, pero un dominio sólo puede apuntar a un servidor.

DoS(Denial of Service): Denegación del Servicio es un incidente en el que se priva a un usuario u organización de los servicios de un recurso que normalmente se esperaría tener.

Enrutador: Dispositivo para la interconexión de redes informáticas que permite asegurar el camino de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos.

Espiroquetosis: Enfermedad que se contagia por medio de los roedores, los síntomas de un humano infectado son: escalofríos, dolor de cabeza, dolores musculares, vómitos y alta temperatura.

FAQ: Frequently Asked Questions, Preguntas más frecuentes es una lista de preguntas y respuestas de uso común en la web para proporcionar la misma información para muchos usuarios.

Frecuencia: Cantidad de veces que se repite un determinado valor de cierta variable.

Hacking: Arte informático de construir y solucionar problemas que atenten contra la vulnerabilidad de un sistema o aplicación.

Host: Es una computadora que funciona como el punto de inicio y final de las transferencias de datos.

ISO 27001: Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información.

Método Delphi: Método para obtener el conocimiento de los expertos respecto a un tema concreto que consiste en: preguntar a unos expertos sobre este tema; reunir las aportaciones en un documento y volverlo a pasar a todos los expertos.

Muermo: Enfermedad infecciosa típica de los equinos

PHA: Process Hazard Analysis:Proceso de análisis de peligros o análisis de riesgos

Probabilidad: Es la relación entre el número de veces en que un evento se produce y el total posible de casos.

Protocolo ICMP: Protocolo de Mensajes de Control de Internet: ICMP es utilizado por los protocolos IP y superiores para enviar y recibir informes de estado sobre la información que se está transmitiendo. Los routers suelen utilizar ICMP para controlar el flujo, o velocidad, de datos entre ellos. Los dos tipos básicos de mensajes ICMP son el de informar de errores y el de enviar preguntas.

Protocolo TCP: Protocolo de Control de Transmisión: Es un protocolo orientado a la conexión y establece una conexión (también conocida como una sesión, circuito virtual o enlace) entre dos máquinas antes de transferir ningún dato. Para establecer una conexión fiable, TCP establece el número de puerto y los números de secuencia de inicio desde ambos lados de la transmisión.

Protocolo UDP: Protocolo de Datagramas de Usuario: Es un protocolo no orientado a la conexión y es el responsable de la comunicación de datos extremo a extremo; UDP no establece una conexión. Intenta enviar los datos e intenta comprobar que el host de destino recibe los datos. Se utiliza para enviar pequeñas cantidades de datos que no necesitan una entrega garantizada.

Rating: Cifra que indica el porcentaje de hogares o espectadores que están viendo un programa de televisión.

Router: Véase Enrutador.

Sistema de Información: Conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su posterior uso, generados para cubrir una necesidad (objetivo).

Stress: Reacción fisiológica del organismo, que provoca en los humanos cambios de estado de ánimo y reacciones como frustación, presión, cansancio, etc.

TCP/IP: Protocolo de Control de Transmisión/Protocolo de Internet: Es un sistema de protocolos que hacen posibles servicios Telnet, FTP, E-mail, y otros entre equipos que no pertenecen a la misma red.

Virus: Pequeño software que, al igual que un virus biológico, infecta a una computadora y se propaga en ella con diversos propósitos como daño, robo de información, molestia, etc.

Wizard: Asistente que te guía en la configuración de software.

Zombies: Equipos utilizados por los hackers para lanzar ataques de DoS (Denial of Service), es una computadora que ha sido implantado con un demonio que lo pone bajo el control de un malintencionado pirata informático sin el conocimiento del dueño de la computadora.

BIBLIOGRAFÍA Y MESOGRAFÍA

Bibliografía

Anderson, David R. **Métodos cuantitativos para los negocios**. International Thompson Learning, séptima edición, New York, NY, 1999, 822 páginas.

Berumen Arellano, Sergio Alejandro. **Evolución y desarrollo de las TIC en la economía del conocimiento.** ECOBOOK, 2008,286 páginas.

Cortés Díaz, José María. **Técnicas de prevención de riesgos laborales: seguridad e higiene**. Tebar, novena edición, Madrid, España, 842 páginas.

Del Peso Navarro, Emilio. **Manual de outsourcing informático: (análisis y contratación)**. Díaz de Santos, España, segunda edición, 2003, 237 páginas.

Gestión de servicios ti basado en ITIL Versión 3: Guía de bolsillo Spanish. Van Haren Publishing, 2008, 100 páginas.

Harbhajan Kehal, Varinder P. Singh. **Outsourcing and offshoring in the 21st century: a socio-economic perspective**. LinkHershey, Pennsylvania : Idea Group, 2001, 482 páginas.

López, Victor Raúl. **Gestión eficaz de los procesos productivos.** Especial Directivos, 2008,283 páginas.

Office of Government Commerce. **Estrategia del servicio**. Stationery Office, 2010, 298 páginas.

Ponce de León, Jesús. **Introducción al análisis de riesgos**. LIMUSA Noriega Editores, México, 2002, 217 páginas.

Richard L. Daft, Dorothy Marcic. **Introducción a la administración**. International Thompson Learning, cuarta edición, México, 2006, 614 páginas.

Mesografía

http://definicion.de

http://elabc.blogspot.com/2007/01/definir-los-hitos-del-proyecto-es.html

http://en.wikipedia.org/wiki/BS7799

http://support.microsoft.com/kb/77791/es

http://www.amipci.gob.mx

http://www.biografiasyvidas.com/biografia/f/fayol.htm

http://www.bsi-global.com/British_Standards/index.xalter

http://www.channelplanet.com/index.php?idcategoria=13932

http://www.cinstrum.unam.mx/secciones/depar/sub4/tein.html

http://www.clusif.asso.fr/

http://www.cramm.com/

http://www.csi.map.es/csi/pg5m20.htm

http://www.enterate.unam.mx

http://www.iso.org

http://www.itil.co.uk

http://www.itsmf.comes.it-processmaps.com/itil/

http://www.microsoft.com/spain/technet/recursos/articulos/ipsecapd.mspx#E4D

http://www.piramidedigital.com/Documentos/ICT/pdictsegurindadinformaticariesgos.pdf

http://www.rediris.es/cert/doc/unixsec/node31.html

http://www.sistemasdecalidad.com/index.php?option=com_content&view=article&id=116&Itemid=60normas

http://www.webopedia.com/zombie.html

www.31000.net/

www.inegi.org.mx

www.isaca.org/cobit/

www.stps.gob.mx/marcojuridico/noms.htm