Universidad Nacional Autónoma de México

Facultad de Estudios Superiores Aragón

Análisis y 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:

María Farah Berdeja Ramírez

DEDICATORIAS

Este trabajo se los dedico a quienes con su dedicación y cariño me han apoyado en las diferentes etapas de mi vida.

Con respeto y gratitud a mis padres por que siempre han estado ahí con su apoyo y consejo:
María del Carmén Ramírez Aguilera
Lic. Sergio Gastón Berdeja Reyes

Con cariño a mi hermano:
Gastón Tariq Berdeja Ramírez

A mis abuelos:
Alicia Yolanda Ramírez Aguilera (q.e.p.d)
Lic. Sergio Berdeja Galeana (q.e.p.d)
Beatriz Reyes Rosales (q.e.p.d)

A mis Familiares:
Rebeca Ramírez Aguilera
Lucila Ramírez Aguilera (q.e.p.d)
Jesús Ramírez Aguilera

Carmen Reyes Rosales(q.e.p.d)

Iván Alejandro Berdeja Reyes
Estela Reyes Rosales

Entre otros.

A mis amigos con los que he compartido muchos años de mi vida, además del placer de conocerlos:
Ignacio Javier González Vargas
Jesús González Melo
Rebeca Figueroa Fernandez
Tania Juarez Olvera
Arturo García Cruz
Jorge Miguel Castillo
Gabriela Rivas
Diana Iridia Trejo
Jorge Alberto Rojas Torres.

AGRADECIMIENTOS:

Al M. en C. Leobardo Hernández Audelo mi gratitud por la dirección del presente trabajo, a quien considero maestro, consejero y amigo.

Además quiero reconocer mi gratitud al:

Dr. Enrique Daltabuit Godas por su apoyo y las oportunidades brindadas.

A la máxima casa de Estudios, la UNAM, y en particular a la Facultad de Estudios Superiores Aragón, por que en sus aulas tuvimos la fortuna de adquirir conocimiento Universal y por los gratos momentos pasados en ellas.

A mis amigos que conocí durante mi estancia en la FES Aragón

Claudia Vázquez, Jorge Cervantes, Jonathan Jolalpan, Miguel Ángel Sánchez, Ricardo Ruiz, Carlos Alberto Fernández, Ricardo Coyote, Baruch Espinosa, entre otros.

Además de mis amigos y compañeros del Laboratorio de Seguridad Informática Centro Tecnológico Aragón:

Eduardo Vega, Alfredo Ramiro Reyes Zuñiga, Omar Antonio y Marco Antonio León, Sergio Mendieta, Jonathan Ponciano, Roberto Hernández, Ramses López, Samuel Marcelo Reyna, Guillermo Tercero, Bruno Bedolla, Alberto Arce, Carlos Hernández, Fernando Alameda, Eder Gilberto Lira, Manuel Alejandro Arteaga, David Campos García, Erick Antonio Rivera Borja, Francisco Javier Ramírez Paredes, José Luis Ramírez, Omar Guzmán, entre otros.

Índice

Índice de Tablas

Índice de Figuras

Figuras Capítulo 5

Figuras Anexo B

Prólogo

La evolución tecnológica que se ha presentado y continúa hasta nuestros días, tiene gran relevancia tanto en nuestras actividades cotidianas e individuales como las del colectivo en empresas y el conglomerado social. Como consecuencia de esta evolución tecnológica, muchas de las actividades que se realizan además del entorno en el que se encuentra inmersa la sociedad humana, es proclive a depender de la tecnología.

La satisfacción de ese balance entre la oferta y la demanda, reflejo de una sociedad globalizada que se relaciona directamente con una centralización y distribución de bienes que cubran las necesidades de una población en constante movimiento, ha traído importantes retos a la inventiva humana y es evidente como se ha dado este constante cambio, a lo largo de la historia, para cimentarse en la realidad de la actualidad.

La mayoría de las actividades que se realizan en nuestros días depende, directa o indirectamente, de las tecnologías de información (TI).Desde antes de la aparición de la escritura el ser humano ha tratado de comunicarse con sus semejantes de alguna forma para transmitir algún tipo de conocimiento o enseñanza, pero no es si no hasta la creación de la escritura que se ha podido transmitir una gran cantidad de información a las generaciones subsecuentes. Esto no ha tenido un impacto tan grande, como lo ha sido hasta nuestros días la creación del Internet, donde, la difusión de la información cada vez es más sencilla por los medios electrónicos a los que tenemos acceso. Por esta razón las tecnologías de información constituyen un elemento cada vez más poderoso.

Las Tecnologías de la Información son el vehículo de muchos de los servicios que se brindan en la sociedad actual y esto puede significar, en las organizaciones y empresas, una ventaja competitiva sobre otras del mismo rubro, incluso como posicionador en los mercados mundiales y también claro, en la difusión y asimilación de las noticias del mundo contemporáneo. Por eso las tecnologías de la Información son necesarias para gestionar o administrar la información. Aunque esto suene redundante hay que considerarle un tratamiento especial, la información como tal puede y debe considerársele en varios estados, los cuales se explicarán más adelante.

La información, como tal, cumple con varias funciones entre las que se encuentran el aumentar el conocimiento de un ente racional (usuario), el proporcionar a quien toma las decisiones la base donde se fundamentará para el desarrollo de soluciones y elecciones, además también, proporcionar una serie de reglas de evaluación y decisión con fines de control donde los datos procesados y aplicados, en alguna situación, proveen el conocimiento para la evaluación y desición en situaciones

afines. Como tal, esta información debe ser elaborada para ser utilizable y reutilizable.

Las Tecnologías de la información actúan como un importante motor de crecimiento, porque sus ventajas económicas en términos de valor añadido , productividad y empleo, se le suman las que se relacionan con su ínter conectividad bidireccional, que permite la transmisión y generalización de ventajas, las experiencias entre diferentes regiones y ambientes, además de proveer de servicios las 24 horas en cualquier rincón del planeta son la parte idílica que traen consigo la proliferación de estas tecnologías y la aceptación social que conlleva. Pero aunado a las ventajas que ésta representa, existe también un riesgo que se le relaciona, y ya que tanto depende de las tecnologías de la información, es menester encontrar un balance y minimizar ese riesgo.

El riesgo puede hacerse presente en cualquier momento, desde un empleado descontento que posiblemente trasgreda o tergiversa la información corporativa, un mal uso de los recursos informáticos, el descuido de un administrador o un usuario, ya sea de forma deliberada o no; por agentes externos o internos; ha traído importantes pérdidas económicas, conflictos bélicos y, en el mejor de los casos, malentendidos políticos. El riesgo se asocia con la probabilidad de que ocurra un suceso no deseado, como los ejemplos mencionados anteriormente, lo que implica preparar y disponer anticipadamente una acción. Analizar este riesgo implica el dimensionar el impacto, en un escenario creíble, es decir, cuanto daño el evento negativo causaría y que tan probable es que se dé este evento.

El impacto, es entonces, el conjunto de posibles efectos negativos sobre el ambiente productivo, en un proceso continuo como consecuencia de la manifestación del riesgo. Existen eventos considerados poco probables, aunque si se suscitaran, tendrían un impacto catastrófico en el ambiente productivo, y para los cuales no existe una medida preventiva disponible, debido a que el riesgo nunca se ha materializado. Aunque no hay una métrica lo suficientemente sólida para considerar el impacto, en el caso anterior, se buscará disminuir la aparición de este evento definiendo los riesgos inherentes, es decir llevar el riesgo a un nivel aceptable.

Una gran cantidad de organizaciones, instituciones, tanto de la iniciativa privada como pública, se han dado a la tarea de realizar manuales o códigos donde se enuncian buenas prácticas que tienen la finalidad de llevar una administración confiable de los recursos con un fin común. Así pues también, múltiples organizaciones han hecho lo propio para enunciar buenas prácticas en el ámbito de la administración de la seguridad de la información y la seguridad informática[1] y esto

[1] La informática es la disciplina que estudia el tratamiento automático de la información utilizando dispositivos electrónicos y sistemas computacionales. Lo que hoy conocemos como informática es la interacción de muchas de las técnicas y de las máquinas que a lo largo de su historia el hombre ha desarrollado para ayudarse y aumentar sus capacidades de memoria, de pensamiento y de comunicación.

ha dado lugar a un gran número de documentos. Es de esperarse que estos documentos sean de carácter general, debido a que las actividades de una empresa no son iguales a las de otra, aunque pertenezcan a un mismo sector y el consenso de estos documentos no debe inclinarse hacia un monopolio o en beneficio de un solo proveedor.

La utilización de controles a implementarse, en cuanto a la seguridad de la información compete, deben permitir la continuidad del negocio y es por esto que deben de ser estimados para cada organización en el balance costo-beneficio.

El propósito del presente trabajo es, proporciona un fundamento para el desarrollo de un programa eficaz de administración de riesgos, conteniendo las definiciones y dirección práctica necesaria para determinar el riesgo y atenuar el impacto dentro de los Sistemas de TI, ya que el desempeño de estos se refleja en los objetivos de los procesos de negocio, que a su vez son parte integral de la misión de una organización.

A continuación se hace mención del contenido temático desarrollado, donde:

En el primer capítulo, se explica como se relacionan las tecnologías de la Información con la seguridad informática, partiendo del entendimiento y conceptualización de los términos inherentes a ambas temáticas (seguridad y tecnología), su importancia e interacción con lo cotidiano y la exposición paulatina de la problemática relacionada con la seguridad de la información, tal es el caso de la falta de información, la modificación de ésta de una forma no deliberada o con dolo, además de algunas recomendaciones realizadas por empresas públicas y privadas de diferentes rubros, que consientes que el tratamiento de la información se realiza de una forma automatizada, llegaron al consenso de que a la información debe proveérsele de ciertas propiedades, mediante una administración confiable. Esto agrupando en manuales, códigos de gestión de la seguridad, gestión de los recursos informáticos, gestión de los servicios, buenas prácticas, entre otros.

Lo inherente a la mitigación, administración y evaluación del riesgo relacionado a la infraestructura informática, la productividad de una empresa, la concientización sobre alguna problemática, el desarrollo de controles, la creación de políticas y la capacitación del personal así como todos los involucrados para llevar acabo una administración confiable y rentable se desarrolla a lo largo del capítulo 2 mediante la delimitación, análisis de los controles existentes, responsabilización. Así como el proceso constante de la administración del riesgo.

Ahora bien, lo relacionado con la prestación de los servicios, entendiendo esto como la adecuada prestación de un servicio respaldado por la infraestructura informática y en base a lo convenido por el prestador y el asimilador de dicho servicio; se desarrolla a lo largo del capítulo 3. Y tiene la finalidad de que, la misión de la organización se asimile, junto con su infraestructura tecnológica, de tal forma que la

falla de alguno de estos elementos pueda interpretarse como el eslabón de una problemática creciente, y/o la afectación de la misión mediante los objetivos relacionados, sí se concreta de esta forma, es inmediata la mitigación, sin llegar a la interrupción del servicio. De tal forma, que si fuese el caso, la disminución, en cuanto a productividad se refiere, se llevará a cabo de una manera aceptable para los intereses de la empresa, pero siempre teniendo en cuenta el impacto en el negocio.

EL capítulo 4 aborda el punto de vista de la gestión de Servicios, la asimilación de nuevas tecnologías, el desarrollo de aplicaciones de una forma enfocada a la prestación de un servicio, y las diferencias de optar por controles para asegurar la disponibilidad y operación del servicio con la premisa de solo ponerlos en marcha, sin tener una visión general y organizada de la empresa y las repercusiones que en productividad, costos y operación que tendrán antes de su aplicación.

En el capítulo 5, el último de este trabajo, se muestran los resultados obtenidos a lo largo de éste, así como también, las conclusiones emanadas de su desarrollo.

Convenciones

Se utilizaron a lo largo de este trabajo las siguientes convenciones:

- Anglicismos: en letras itálicas (*oblicuo, sesgado, inclinado* o *cursivo*) como se muestra a continuación:

(“Service Management”)

- Palabras clave: se encuentran en negritas. Por ejemplo:

memoria

Títulos y subtítulos

Los siguientes tamaños de letra se refieren los títulos y subtítulos (como puede observarse en la estructura del índice).

Formato	Descripción
Título Capítulo	Utilizado para el título del capítulo Arial Black 20 pt
1Título	Utilizado para Títulos en primer nivel ARIAL 16 pt Negritas
1.1Título	Utilizado para subtítulos en segundo nivel ARIAL 14 pt Negritas
1.1.1Título	Utilizado para subtítulos en tercer nivel ARIAL 13 pt Negritas
1.1.1.1Título	Utilizado para subtítulos en cuarto nivel Times New Roman 14 pt Negritas
1.1.1.1.1Título	Utilizado para subtítulos en quinto nivel Times New Roman 13 pt Negritas e Italicás
1.1.1.1.1.1Título	Utilizado para subtítulos en sexto nivel Times New Roman 11 pt Negritas
1.1.1.1.1.1.1Título	Utilizado para subtítulos en septimo nivel Times New Roman 12 pt Normal
Texto en general	Utilizado para el desarrollo de temas y subtemas ARIAL 12 pt. Normal

Pies de página

Pies de página	Descripción
	Utilizando números arábigos, secuenciales por capítulo. Dicha numeración se reinicia en el capítulo subsecuente. Por ejemplo: *gadgets*[2]

Referencias

Referencias	Descripción
	Utilizando números arábigos entre paréntesis cuadrados al superíndice Por ejemplo: Flujo y Retroalimentación de la información [12] (pp. 8)

Referencias Por Capítulo	Descripción
	Al final de cada capítulo se encuentran las referencias donde: El Autor u organismo emisor está con letras itálicas ARIAL 10 pt. El Título, subtítulo referido está entrecomillado y en negritas con letras ARIAL 10pt Por ejemplo: *Mike Friedman, L. Wlosinski.* "**Integrating Security into the Systems Development Life Cycle (SDLC)".** Center for Information Thechnology Officer Mayo 22, 2003 Slide 10.

Hipervinculos

Hipervínculos	Descripción
	Subrayado por ejemplo: plan implementado de protección.

Citas Textuales

Citas Textuales	Descripción
	Utilizando el texto de la cita entrecomillado y en letras itálicas. Por ejemplo: “*En el caso de una org…”*

Tablas y Figuras

Títulos de Tablas y Figuras	Descripción
	Centrados, en negritas Por ejemplo: **Figura 3 Puntos de acción para la mitigación de riesgos**

Texto explicativo en Tablas y Figuras	Descripción
	Inmediatamente debajo del título de la tabla o la figura, según corresponda, en ARIAL 10 pt Por ejemplo: Si el costo del ataque es mayor que la ganancia obtenida e…

Capítulo
1
Las Tecnologías de Información y la Seguridad Informática

Resumen

La Información es una colección de hechos significativos y pertinentes, para el organismo u organización que los percibe, es decir, un conjunto ordenado de datos, los cuales son la representación de hechos, condiciones, situaciones o valores en un código determinado, por lo tanto la asociación de los datos en un determinado contexto es lo que se convierte en información. Este conjunto de datos describen sucesos o identidades.

"*En el caso de una organización, ésta selecciona hechos entre sucesos y entidades particulares, para satisfacer sus necesidades de información*."[1]

Las Tecnologías de Información es un termino, ahora comúnmente utilizado y normalmente referido, a todo aquello relacionado con el procesamiento de la información, utilizando diferentes dispositivos electrónicos, aunque si bien es cierto, el termino tecnología de Información hace referencia también, a las diferentes tecnologías utilizadas, incluso antes de la aparición de la imprenta y sí, de la escritura, y que son igualmente validas para el procesamiento de la información, es decir, "*se entiende como aquellas herramientas y métodos empleados para recabar, retener, manipular o distribuir información y no solamente las relacionadas o asociadas con computadoras*".[2]

En la actualidad es común encontrarnos con una gran cantidad de *gadgets*[1], que han proliferado su uso en los últimos años, tal es el caso de dispositivos de cómputo portátiles: las computadoras llamadas *lap top*, las computadoras de bolsillo (*Pocket PC*) , los asistentes digitales personales (*PDA*) y las computadoras para la palma de la mano (*Palm*). Todas estas herramientas son computadoras con funcionalidad completa, aunque restringida, y con capacidad de almacenar grandes cantidades de datos y programas.

Estos artilugios tecnológicos complican por su portabilidad el protegerlos, debido a que el someterlos a controles de la organización, como lo haría con sus activos dentro de una oficina o inmueble, no es aplicable, ya que estos controles recaen en el usuario final y el someterse a estos causa inconformidad o descontento y pueden ser fácilmente ignorados. También al ser capaces de almacenar grandes cantidades de información e incluso trasmitirla permitiría que fuesen usados maliciosamente, por ejemplo, para extraer información sensible de la organización y divulgarla.

Otras de las problemáticas inherentes al manejo de la información son: los accesos no autorizados que comprometen información vital, de la empresa causando pérdidas

[1] *Gadget* es aquel dispositivo que tiene un propósito y una función específica, generalmente de pequeñas proporciones, práctico y a la vez novedoso. También es el término que se le ha dado a la nueva categoría de mini aplicaciones, diseñada para proveer de información o mejorar una aplicación o servicio de una computadora, o bien cualquier tipo de interacción a través de la Internet, por ejemplo una extensión de alguna aplicación de negocios, que provea información en tiempo real del estatus del negocio u organización.

económicas por fraudes o evidenciando incluso aspectos internos, la modificación y el borrado de información merma la productividad y si la intrusión no es detectada impide tomar alguna acción correctiva, haciendo poco fiable el origen de la información.

---

1 Las Tecnologías de la Información y la Seguridad Informática

1.1 Conceptos de Información

En sentido general, la **información** es un:
"*conjunto organizado de datos, que constituyen un mensaje sobre un determinado ente o fenómeno. De esta manera, si por ejemplo organizamos datos sobre un país (número de habitantes, densidad de población, nombre del presidente, etc.) y escribimos por ejemplo, el capítulo de un libro, podemos decir que ese capítulo constituye información sobre ese país. Cuando tenemos que resolver un determinado problema o tenemos que tomar una decisión, empleamos diversas fuentes de información (como podría ser el capítulo mencionado de este imaginario libro), y construimos lo que en general se denomina conocimiento o información organizada que permite la resolución de problemas o la toma de decisiones*". [3]

La información podemos encontrarla en cuatro estados o procesos[2]: Adquisición, Creación, Almacenamiento y Transmisión, descritos en el apartado, estados de la información.

"*Uno de los elementos clave para una organización y también visto como herramienta competitiva es la mejora del flujo y proceso de la información y que esta información pueda ser accesible de manera rápida e interrelacionada*". [4]

En la actualidad, en los sistemas de información recae el funcionamiento de la empresa y el cumplimiento de sus objetivos y su misión como organización, debido a que ayudan a mejorar procesos, reducir tiempo (horas/hombre) y además de centralizar tareas que agreguen valor. La función principal de estos sistemas es la de tener información fiable e inmediata, es decir, para su aprovechamiento hay que proveer, a la información, de propiedades de **seguridad** las cuales son: confidencialidad, integridad, autenticidad y disponibilidad.

[2] Los procesos son un conjunto de actividades o eventos que se realizan o suceden con un objetivo determinado.

1.1.1 Estados de la Información

La **adquisición** de información la realizamos a través de nuestros órganos sensoriales, cuando interactuamos con el medio, posteriormente el cerebro forma círculos neurales a través de la experiencia adquirida, permitiéndole así conceptualizar, asociar y razonar a posteriori. Se divide en la percepción y la sensación.

La percepción no sólo es la repetición de nuestro entorno, como si se tomará una instantánea, mediante nuestros órganos sensoriales y perceptivos. La sensación es el **proceso** receptivo y la percepción es la que nos permite distinguir o diferenciar un objeto de otro, una cosa de otra, es lo que da la pauta para **conceptualizar** lo que nos rodea.

La formación del **concepto** está estrechamente ligada al contexto; esto significa que todos los elementos, incluyendo lenguaje y cultura, y la información (**conocimiento**[3] acumulado y retroalimentado en varias iteraciones a lo largo de la vida) percibida por los sentidos que sea accesible al momento en que una persona construye el concepto de algo o alguien, influyen en la **conceptualización** (**creación** de la información). El conocimiento de la experiencia siempre es concreto, tiene una referencia a una cosa, una situación o algo que es único e irrepetible.

La percepción supone una serie de elementos en los que hay que distinguir la existencia del objeto; la combinación de un cierto número de sensaciones; la integración de nuevos estímulos percibidos en experiencias anteriores, a su vez, los cuales son acumulados en la memoria (**almacenamiento**). La selección de ciertos elementos de nuestras sensaciones y la eliminación de otros, por eso el acto perceptivo, no solo es el registro de los datos en nuestro cerebro, si no que también la interpretación de las impresiones de los sentidos, la respuesta a un estímulo es reestructurada, no puede considerársele como una respuesta automática hacia el mismo sentido, es decir, un mismo fenómeno observado y percibido por un grupo de personas, recibirá distintas respuestas, además de, que su interpretación no será la misma para cada una de estas personas.

Las funciones generales del sistema de **memoria** abarcan: la **retención** de información, el apoyo en el aprendizaje de nuevo conocimiento, la comprensión del ambiente en un momento dado, la formulación de metas inmediatas y la resolución de problemas.

En cuanto a la **transmisión** de la información el ser humano mediante el **lenguaje** verbal ha sido capaz de transmitir la información adquirida, creada y almacenada en su cerebro.

[3] Conocimiento es la capacidad de convertir datos e información en acciones efectivas, por lo que el conocimiento puede ser explícito (cuando se puede recoger, manipular y transferir con facilidad) o tácito. Este es el caso del conocimiento heurístico resultado de la experiencia acumulada por individuos.

El Circuito del Habla representa claramente, como se da esta **transmisión,** en donde el receptor, mediante el oído es capaz de percibir ondas sonoras. Estas ondas sonoras viajan a través del medio, el aire, pero como éste no esta, comúnmente aislado, si no, que se encuentra con variaciones de ruido, las cuales pueden despreciarse por el receptor, aunque, si la acumulación de ruido satura el medio el receptor no interpretará la información correctamente, aunado a esto, tanto el emisor como el receptor han convenido o conocen el lenguaje [4]que les permite generar el mensaje (emisor) asegurándose de el entendimiento de éste (receptor).

Ahora bien Albert Einstein decía: "*Si no tienes una buena memoria, hazte una de papel*", está frase hace alusión al olvido, es por eso que utilizamos, también, algún tipo de recipiente de información externo a nuestra corteza cerebral, donde confiamos la información, de la cuál se hará uso posteriormente con algún fin especifico.

Este almacén secundario, donde yace ahora la información, se somete al receptor para su interpretación en el momento oportuno, esto implica que el receptor conoce la **tecnología** para extraer de este almacén secundario la información, es decir, tiene la capacidad de **transformarla** para su comprensión. Entonces, mientras el emisor usa determinada tecnología con el fin de **transmitir** información. El receptor utiliza la tecnología **inversa** con la finalidad de procesar los datos que obtenga de esta transformación.

El hasta ahora receptor de la información puede convertirse en un futuro en emisor y el hasta entonces emisor en receptor dando origen a un flujo de **retroalimentación** (comunicación) entre estos dos entes, donde la información es manipulada. En el siguiente apartado se ahondará sobre esta temática.

1.1.2 Manejo de la Información

En el ejemplo anterior, donde dos personas tratan de compartir información, suponemos que tanto el proceso a nivel cerebral, tanto del emisor y del receptor se realizaron de manera satisfactoria y además de que la transmisión a través del medio fue la idónea, es decir un correcto e ideal manejo de la información.

En la actualidad, la transmisión de la información se realiza mediante la comunicación oral, como lo explica el circuito del habla y por supuesto, también con dispositivos de cómputo cada vez más novedosos y con diferentes funcionalidades. A continuación, Figura 1 Transmisión de Información Sistemas Computacionales, se muestra una comparativa con el circuito del habla, el cual ha sido utilizado desde la creación del

[4] En este caso referido al lenguaje verbal que se caracteriza por emplear signos que transmiten significados y que pueden articularse formando estructuras complejas que adquieren nuevas capacidades de significación en donde se consideran los aspectos anatómicos y neurológicos; los primeros conformados por un aparato fonador donde gracias al diafragma y las cavidades de la cabeza el ser humano puede generar sonidos; los segundos mediante conexiones en la corteza cerebral.

lenguaje verbal, y la comunicación realizada por los dispositivos electrónicos en sistemas computacionales, para satisfacer las necesidades de información.

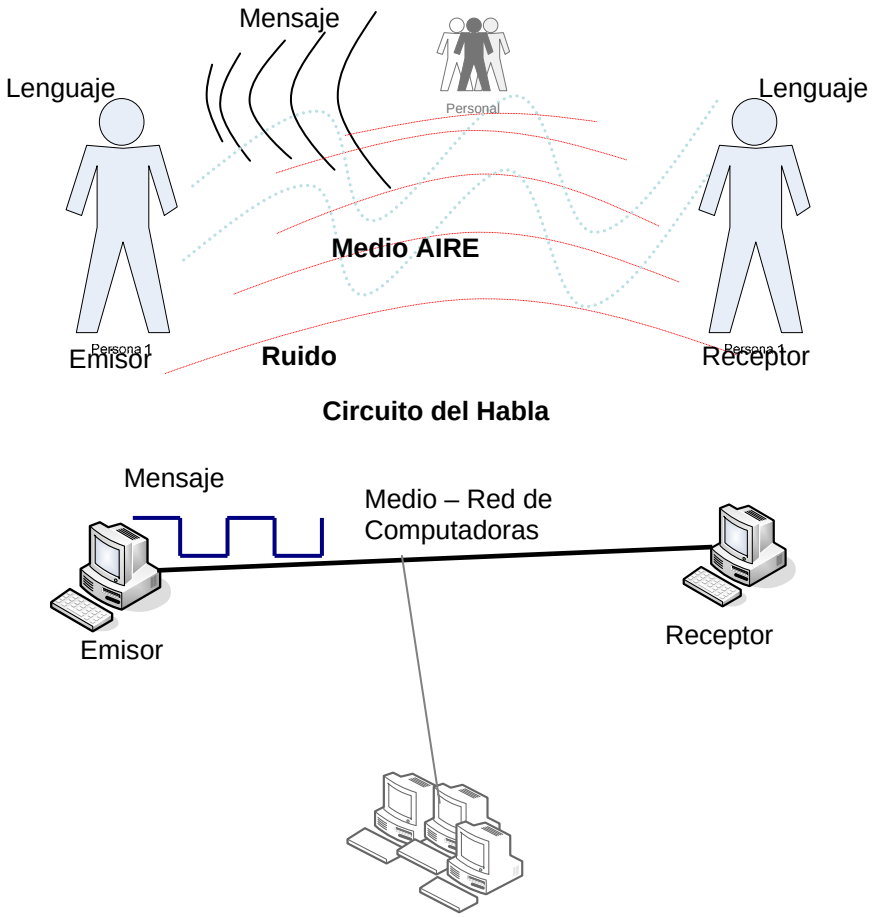

Figura 1 Transmisión de Información Sistemas Computacionales

En el circuito del habla el ruido es un elemento no deseado que impide, en algunos casos la comunicación, ya que comparte el mismo medio que utiliza el emisor para transmitir el mensaje, el aire, este medio no es exclusivo del emisor y del receptor, existen otras personas utilizando el medio, transmitiendo y percibiendo ondas sonoras.

En el caso de la red de computadoras el medio que interconecta los diferentes dispositivos electrónicos, computadoras, para este caso en particular, es el cable de red (cobre), donde se encuentran elementos no deseados entre ellos el ruido[5], este provocado por los mismos dispositivos que están interconectados, y el cual no puede eliminarse, el medio se comparte con otras computadoras o dispositivos electrónicos,

[5] El ruido como tal en el medio ya no es factor tan critico, debido a mecanismos implementados tanto en la elaboración del cableado (cables blindados) y lo protocolos de comunicación utilizados para la comunicación.

como es el Internet o red de redes, donde hay muchas computadoras interconectadas.

El lenguaje verbal, por su parte, en los seres humanos, es la interpretación de los sonidos en base a un conocimiento previo que data desde las primeras interacciones con fonemas a una edad muy temprana y se desarrolla durante la infancia, esto permite generar un mensaje por el emisor, además de que el receptor debe de tener esta base (lenguaje) para procesar los fonemas y comprender el mensaje.

Para una red de computadoras los mensajes que se transmiten, de una computadora a otra, mantienen un mismo código, el cual se caracteriza por diferencias de voltaje que viajan sobre el cable de red y se procesan por la otra computadora al ser captadas.[6]

El ser humano, al igual que otros animales, ha utilizado una tecnología para manipular la información y transmitirla.

El manejo de la información se realiza mediante los sentidos; **órganos sensoriales**[7]; el tacto, la vista el oído, el gusto y el olfato. Posteriormente en el cerebro, humano o animal, se realiza un proceso el cual norma sus acciones.

Algunos científicos realizaron experimentos, los cuales son indicativos del como los animales y los seres humanos norman sus acciones por los estímulos obtenidos del medio. Como puede observarse en el experimento realizado por Iván Pavlov, quién dio origen a lo que hoy se conoce como psicología conductista.

Utilizando perros, a los cuáles, se les acerca alimento y estos instintivamente comenzaban a salivar. Adicionalmente Pavlov expuso a estos animales al sonido de una campana al momento que les presentaba el alimento, esto dio como resultado, que con el sonido de la campana, los perros comenzarán a salivar sin necesidad de que olfatearán el alimento, únicamente con el sonido de la campana.

Posteriormente, John B. Watson y su colaboradora Rosalie Rayner, realizaron experimentos con un niño de 11 meses donde se le expuso a un sonido estridente, haciendo que se sobresaltara, mientras se le presentaba un objeto peludo, el resultado fue que el niño sollozará con la interacción de un objeto peludo, a pesar de haber eliminando el sonido estridente, por ejemplo: una rata, un abrigo, entre otros objetos con esta característica. El niño, antes de realizado este experimento, no había demostrado miedo hacia los objetos con pelo.

---

[6] Véase el Anexo B. Transmisión de mensajes en Red

[7] Los receptores sensoriales son los órganos capaces de captar los estímulos del medio ambiente (órganos de los sentidos) y del medio interno (receptores viscerales) En los receptores sensoriales la energía del estímulo se transforma en el lenguaje informático del organismo, mientras que en los estímulos ambientales de distinto tipo inducen en los receptores sensoriales ubicados en la cabeza y en la piel, la generación de señales eléctricas que viaja por vías específicas hasta centros nerviosos también específicos donde se generan sensaciones particulares. Normalmente tenemos conciencia de este tipo de información.
Del mismo modo, estímulos del medio interno actúan sobre sistemas sensoriales específicos, pero la información que transportan, al actuar sobre los centros que les corresponden, no siempre generan sensaciones. La conciencia que tenemos de este tipo de información es limitada

Los datos que se reciben a través de los órganos sensoriales y asociados con diferentes localidades del **cortex**[8] en el cerebro, son procesados.

En el caso de algunos animales menos primitivos, los datos son organizados, y posteriormente se considera la creación de información haciendo asociación no solo contextual si no también con lo que se denomina "*Memoria Declarativa que es la habilidad para recordar los detalles de los eventos (incluyendo tiempo, lugar y circunstancias) y los conceptos*"[5]

Al recibir estímulos a través de nuestros sentidos estos pueden ser erróneos, produciendo que la interpretación de los datos, proceso de creación de información, no coincida con una representación de la realidad, además puede ocurrir que algunos de los elementos encargados de procesar los estímulos recabados por nuestros sentidos no lo hagan dentro de los parámetros que son considerados normales, estos hechos consideran a la información creada no fidedigna, por lo que al transmitirla mantendrá características no deseadas e impedirá que la representación del hecho, objeto, o situación analizada, desde un inicio, sea desvirtuada.

Algunos ejemplos de recepción errónea del entorno, por medio de nuestros sentidos, son: Las ilusiones ópticas, las auditivas y sensitivas. El termino correcto es el de "*Pareidolia, que es un fenómeno psicológico, consistente en que un estímulo vago y aleatorio (habitualmente una imagen) que es percibido erróneamente como una forma reconocible*[6] ." Describe un fenómeno psicológico que implica la estimulación vaga y aleatoria (a menudo una imagen o un sonido).

Se asocia con la particularidad innata, del ser humano, de reconocer patrones y de la asociación de imágenes conocidas con una forma conocida, uno de los ejemplos claros es el encontrar en las nubes rostros u objetos.

[8] Cortex es el manto de tejido nervioso que cubre la superficie de los hemisferios cerebrales, tales redes neuronales, se distinguen en tres tipos básicos de corteza:
Isocortex (o Neocortex), que es el último en aparecer en la evolución del cerebro, es el encargado de los procesos de raciocinio; paleocortex, comprende el cerebro olfatorio; Arquicortex, constituido por la formación del hipotálamo, esta es la parte "animal" o instintiva, es la parte del cerebro que se encarga de la supervivencia, las reacciones automáticas y los procesos fisiológicos. Dentro del cortex, se pueden distinguir áreas con capacidad de procesar la información, más eficaces, las áreas del neocortex, asiento o soporte principal del Registro de Lo Simbólico. En los lóbulos como el temporal (las neuronas captan cualidades sonoras en la corteza auditiva primaria, además de contener neuronas que se relacionan con la comprensión del lenguaje, memoria y aprendizaje), el frontal (contiene la corteza primaria aquí las neuronas controlan los músculos del cuerpo, se distribuye en la corteza cerebral en función de las partes del cuerpo), el parietal (corteza somato sensorial primaria, compuesta por neuronas relacionadas con el tacto, también se organiza en función de las partes del cuerpo), y el occipital (contiene la corteza visual primaria, localizada en la parte posterior, procesa la información visual que llega de la retina) .

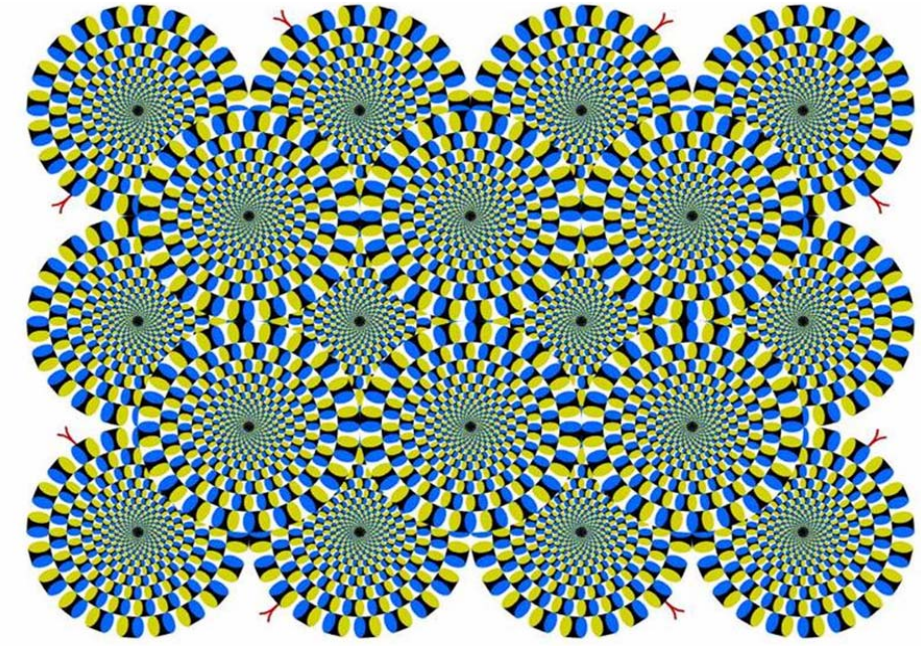

Figura 2 Ilusión óptica de movimiento

Se utiliza un método de psicodiagnóstico, basado en la pareidolia, creado por el psicoanalista Hermann Rorschach, y denominado test de Rorschach, por su autor, que consta de láminas donde se ven manchas de tinta sobre un fondo blanco, las características de estas manchas es que poseen una forma vaga y sugerente, auxiliar para diagnostico de enfermedades como depresión, esquizofrenia y desordenes de ansiedad.

Figura 3 Lámina del test de Rorschach[7]

Las tecnologías de Información son utilizadas para el manejo de la información.

En la actualidad es asociado este término con la computación, sin embargo, las tecnologías de la Información no son exclusivas de nuestra realidad actual.

1.2 Tecnologías de Información

Los **animales,** por su parte, son capaces de **almacenar** y **adquirir** información de su entorno, aunque el **proceso** para **generación** de información no puede compararse con la que ocurre en el cerebro humano. Sin embargo son capaces también, de **transmitirla.** La transmisión de la información en los animales se realiza mediante la tecnología de comunicación animal.

En las investigaciones realizadas por "*Charles Darwin, se destacó la importancia de la comunicación y de la expresión en la supervivencia biológica. Estudios recientes han puesto de relieve toda una gama de formas de comunicación animal. Así, por ejemplo, cuando una abeja descubre una fuente de néctar, vuelve a la colmena para informar sobre su hallazgo. A continuación comunica la distancia a la fuente mediante un baile, la dirección mediante el ángulo que forma el eje del baile y la cantidad de néctar mediante la vigorosidad del mismo.*

Asimismo, los científicos han registrado e identificado diferentes cantos de pájaros para cortejar, aparearse, demostrar hambre, transportar alimentos, marcar un territorio, avisar de un peligro y demostrar tristeza. Las investigaciones sobre el comportamiento de ballenas y delfines han revelado que éstos disponen de señales vocales relativamente elaboradas para comunicarse bajo el agua."[8]

En efecto, el movimiento que realiza una abeja transmite información a los demás miembros del panal, pero para que el proceso de transmisión de la información esté completo es necesario aplicar una tecnología inversa, la cual permitirá la adquisición, por el receptor o receptores, para su posterior proceso.

El ser humano, por su parte ha utilizado diferentes tecnologías, muchos de estos procesos anteriores al cómputo, aunque la utilización y proliferación de las computadoras han permitido que el término tecnología de la información sea más comúnmente asociado a la época actual. Uno de los ejemplos de estas tecnologías para transmisión de información se puede encontrar en cuevas donde existen varias pinturas rupestres y más adelante, en la línea del tiempo, la escultura. Estas pinturas o esculturas mostraban, en algunos casos, la estructura social, las actividades realizadas e incluso las deidades que adoraban (civilizaciones anteriores a la proliferación de las tecnologías de información mediante medios electrónicos), información interpretada y transmitida hacia sus congéneres. La forma de comunicación y el manejo de la información han evolucionado a lo largo de la historia del hombre.

La informática es la unión de "*muchas de las técnicas y de las máquinas que el hombre ha desarrollado a lo largo de la historia para apoyar y potenciar sus capacidades de memoria, de pensamiento y de comunicación.*" [9]

Podemos considerar la invención y evolución de las siguientes tecnologías como los parte aguas:

La creación de la computadora personal, PC, el Internet y podemos considerar también la proliferación de gadgets como las PDAs, PocketPC, entre otros, todos éstos han llevado al tratamiento de la información, a el manejo de la misma hacía cualquier parte del mundo. La información ya no solo radica en espacios delimitados por paredes o en estantes de bibliotecas o incluso en computadoras de grandes dimensiones.

La información puede encontrarse en muchas lugares. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitirla por correo o utilizando medios electrónicos, presentada en imágenes, o expuesta en una conversación. Cualquiera sea la forma que adquiere la información, o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada.

Desde hace mucho tiempo, incluso desde antes del homo erectus, el hombre ha tratado de proteger la información esto podemos verlo incluso en las pinturas rupestres en cuevas donde la información importante que estas pinturas representaba no se situaban en la parte externa de las cuevas, se encontraba en el interior de la misma no visible para todos.

La información como tal puede significar una ventaja en un ambiente competitivo, una salvaguarda en el caso de un atentado, una estrategia para hacerle frente a un enemigo, un procedimiento para el manejo de una sustancia peligrosa, un apoyo para tomar una desición y como tal si está información se vuelve invalida, por que se ha comprometido, perderá el propósito por el que fue creada y los beneficios que de ella se esperaban desaparecerán o se verán disminuidos.

Figura 4"Información confidencial"[10]

Se han encontrado en pergaminos, que datan del siglo XIV, escritos bajo la ahora inscripción, partículas de un material utilizado para la realización de la tinta en los pergaminos, hierro, esto ha permitido realizar una imagen virtualizada del contenido previo de estos pergaminos, debido a que estos pergaminos, hechos de piel animal, eran reutilizados, encontrando partituras musicales que se creía jamás iban a

recuperarse, de un himno a la virgen María, y ahora es posible extraer esa información generando una imagen virtualizada de las partituras musicales además, el contenido final, que ostentan ahora esos manuscritos, no se ha modificado.

Lo anterior ejemplifica la utilización de una tecnología, en este caso un software denominado “Digital Image Archive of Medieval Music (DIAMM” [11] (pp. 18)) que permitió rastrear sobre el pergamino las partituras musicales y digitalizarlas.

El manejo de la información, que se da hasta nuestros días, ha sido provocado principalmente por la retroalimentación de la misma información, como se explicó en el apartado de manejo de información, se utiliza un almacén secundario para la información, mediante alguna tecnología, principalmente enfocado al término de la informática, haciendo referencia a su utilización con la finalidad de ampliar las capacidades mentales del ser humano.

En el ejemplo del circuito del habla, los procesos como Almacenamiento, Organización y Creación de la información se realizan en el cerebro y la Transmisión se realiza mediante algún medio, en este caso el aire, la tecnología utilizada es el lenguaje, tecnología de comunicación, conformada principalmente por un aparato fonador y un código representativo de los fonemas emitidos; la adquisición, por medio de nuestros órganos sensoriales, en este caso es el oído.

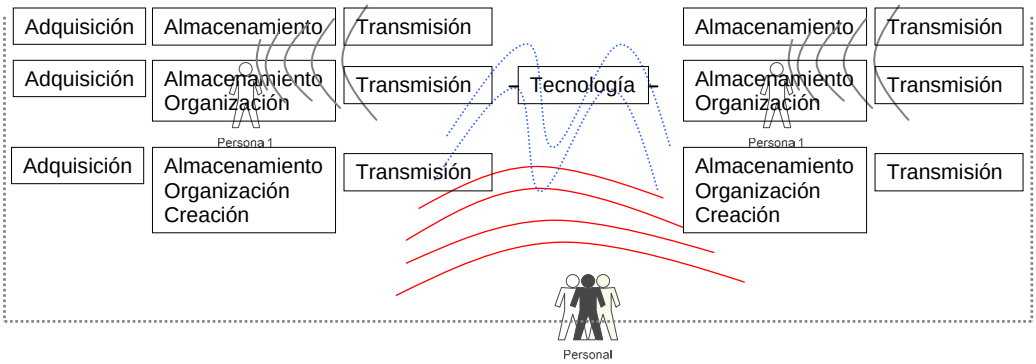

Figura 5 Flujo y Retroalimentación de la información [12] (pp. 8)

La Tecnología de comunicación ocupada, en el Circuito del Habla, es compartida por otras personas, además del medio, el aire, que también es compartido, lo cual trae consigo, que la información sea difundida, sin consentimiento ex profeso de el emisor y el receptor, otro aspecto a considerar, es también, que se puede generar ruido, el cual impide la comunicación, ya sea mediante su propio aparato fonador o algún otro instrumento saturando el medio y los umbrales de percepción auditiva, o incluso imitar el timbre de voz del emisor, intercambiando entre el mensaje real información tergiversada. Puede esto concretarse en un engaño si entre emisor y receptor no hay línea de vista.

Por tal motivo se debe de proveer a la información de características de seguridad como: confidencialidad, disponibilidad, integridad, autenticidad.

Una de las épocas de la historia de la humanidad donde es más notorio el tratamiento que se le da a la información es la denominada Oscurantismo[9], donde solo ciertos grupos podían tener acceso a la información.

1.3 Seguridad de la Información

El ser humano ha tratado de **resguardar** la **información** de muchas maneras y el principal hecho que ha desatado la creación de muchos de los métodos existentes para su resguardo son los **conflictos bélicos**.

La razón primordial para **no difundir** a todos la información se basaba en el **valor** que ésta representa, por ejemplo el hipotético caso de un mapa del tesoro, tiene el objetivo de mostrar como llegar a un tesoro resguardado para disfrute de solo unos cuantos, sí cayera en otras manos podría implicar el **despojo** de aquellos que lo resguardaron originalmente. No siempre se tratará del mapa hacia un tesoro escondido, como es el caso de los planos de una fortaleza donde después de escudriñarlos se descubriría alguna posible falla estructural o el acomodo de cada una de las habitaciones, información muy conveniente para un **terrorista**, para la **contraparte militar** en una guerra o para el **perpetrador** nocturno con deseos de apoderarse de lo que no le pertenece.

La inventiva humana se ha dado a la tarea de evitar comprometer determinada información en su manejo "*La Criptografía que es una de las ciencias donde se integran la Criptología, junto con el Criptoanálisis y la Esteganografía*"[13] (pp. 45), esta última, la **estenografía**, ha acuñado muchos métodos para transmitir la información, se basa en ocultar la información en un mensaje legible. Algunos ejemplos de técnicas de esteganografía que han sido usados en la historia son:

- ✓ Mensajes ocultos en tabletas de cera en la antigua Grecia, la gente escribía mensajes en una tabla de madera y después la cubrían con cera para que pareciera que no había sido usada.
- ✓ Mensajes secretos en papel, escritos con tintas invisibles entre líneas o en las partes en blanco de los mensajes.
- ✓ Durante la segunda guerra mundial, agentes de espionaje usaban micro-puntos para mandar información, los puntos eran extremadamente pequeños comparados con los de una letra de una máquina de escribir por lo que en un punto se podía incluir todo un mensaje.
- ✓ Mensajes escritos en un cinturón enrollado en un bastón, de forma que sólo el diámetro adecuado revela el mensaje.
- ✓ Mensajes escritos en el cuero cabelludo, que tras crecer el pelo de nuevo, oculta el mensaje

[9]Oscurantismo. Oposición sistemática a que se difunda la instrucción en las clases populares.

La **esteganografía** es la ciencia que estudia los procedimientos encaminados a ocultar la existencia de un mensaje; mientras que la **criptografía** pretende que un **intruso** que consigue un mensaje no sea capaz de averiguar su contenido, es decir, busca métodos para asegurar la **integridad** y **confidencialidad** de los mensajes, ejerciendo sobre estos una transformación mediante un **elemento clave**, este elemento clave, es el que permitirá que al ser aplicado por los poseedores de dicho elemento, el mensaje sea des transformado. El **criptoanálisis** tiene como objetivo obtener la información des transformada sin la posesión del elemento clave.

El manejo de la información trae consigo problemáticas inherentes a la seguridad de la información, descritas en los ejemplos citados anteriormente.

En cuanto a la **seguridad en cómputo**, como el **triángulo de oro** representa, es proveer a la información, en un sistema de cómputo, de **integridad**, para evitar que la información sea cambiada, la **disponibilidad** de la información radica en que se pueda deliberar, determinar, mandar lo que ha de hacerse con ella cuando se desee y la **confidencialidad** es el evitar la difusión de la información a un tercero no deseado. Pero cabe **agregar**, el **no repudio** o seguridad en emisiones, que busca acreditar a un sujeto u objeto de manera que las acciones realizadas o los servicios proveídos sean identificados, claramente, como de un proceso o sujeto en cuestión.

El término **Seguridad de la información** cubre una amplia gama de actividades en una organización. Esto incluye tanto los **productos** y **procesos** que previenen **accesos no autorizados** y este aseguramiento de la información; se valdrá del entendimiento del proceso, en cada circunstancia. Por lo que además se debe incluir la **seguridad física** y la **seguridad personal**, esta última, relativa al personal con relación directa o indirecta en el proceso de la información.

En la figura 6, se observa como la información en un sistema computacional, sigue un flujo muy similar al del circuito del habla, en seres humanos.

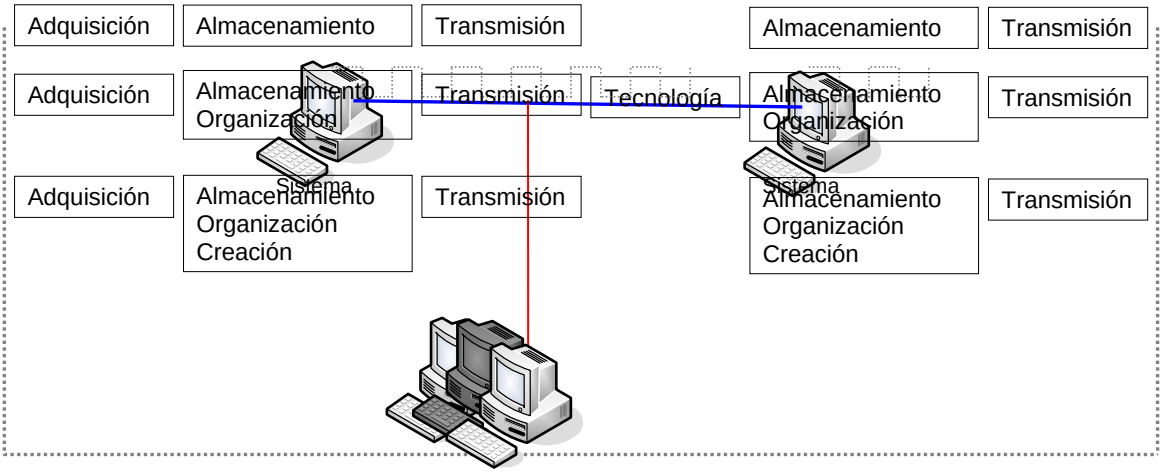

Figura 6 Flujo y Retransmisión de la Información en sistemas computacionales

Aunque el Internet es un claro ejemplo de un medio compartido por muchos usuarios en todo el mundo, no todos estos usuarios tienen un fin común, por lo que no puede considerársele un sistema de cómputo, además de que este medio fue creado con una finalidad divulgativa, escasa en control y por ende también escasa de seguridad, para comunicarse se utilizan tecnologías y protocolos de red (TCP/IP); los cuales han vencido las fallas de comunicación relacionadas con el ruido (retransmisión de paquetes, checksum), interconectando los dispositivos con cables blindados, aunque para las redes inalámbricas y satelitales puede verse afectado el medio por las inclemencias del tiempo y la interferencia en la frecuencia utilizada.

Un sistema de cómputo debe entenderse como un conjunto conformado por la colección de software; "*capaz de procesar y almacenar información de acuerdo a una serie de instrucciones*" [14]; hardware; "*conjunto de elementos electrónicos*" [15]; medios de almacenamiento; datos; información y personas involucradas en el flujo de la información, para satisfacer las necesidades organizacionales.

"*La información es un recurso que, como el resto de los importantes activos comerciales, tiene valor para una organización y por consiguiente debe ser debidamente protegida*". [16] (pp. 9) La seguridad de la información tiene la premisa de **proteger** a ésta de una gran gama de **amenazas**, a fin de garantizar la **continuidad del negocio**, **minimizar el daño** como consecuencia de la concretización de una amenaza o vulnerabilidad y **maximizar el retorno** sobre las inversiones y las oportunidades.

El término **vulnerabilidad** consiste en explotar, para "*causar daño o pérdida a un sistema de cómputo*" [17], una debilidad propia de este sistema, donde la probabilidad de ocurrencia es latente, por ejemplo, debilidades en procedimientos, diseño, o incluso la puesta en práctica de los anteriores, donde se pudo explotar la debilidad para causar pérdida o daño, en un caso hipotético, un sistema particular puede ser

vulnerable a la manipulación desautorizada de datos porque el sistema no verifica la identidad de un usuario antes de permitir el acceso a ellos.

Mientras que a los eventos considerados poco probables, sin embargo si se suscitaran tendrían un impacto catastrófico en nuestro ambiente productivo se les considera una **amenaza**, es decir, *"un conjunto de circunstancias que tienen potencial de causar perdida o daño*" [18], que en el contexto de seguridad de la información incluye tanto actos deliberados o dirigidos, como por ejemplo los realizados por personas mal intencionadas y también aquellos para los cuales no existe una medida preventiva disponible, debido a que el riesgo nunca se ha materializado, es decir, "*sucesos no dirigidos, aleatorios o impredecibles, como un desastre natural*[10]". [19]

El **compromiso**[11]**, otro de los términos relativos a la seguridad de la información,** es la concretización, en cualquier forma posible, de pérdida o daño en un sistema de cómputo por alguna de las características de seguridad en la información deseables para la continuidad de las actividades empresariales que son impedidas o que no se llevan a cabo.

El **Internet** es un medio sumamamente utilizado por la mayoría de las empresas y mediante el cual se brindan muchos servicios de gran importancia a los clientes de una determinada organización, ya sea con fines de lucro, el groso de los casos, o carente de este fin. En la siguiente figura, Principales tipos de amenazas a los sistemas de información, se representan las **amenzas** sobre los sistemas de información que no solo se dan en su interconectividad en la red de redes, si no también, pueden darse en un ambiente delimitado como lo es la intranet corporativa y en todos los posibles ambientes donde se de el flujo de información.

[10] Un desastre natural tal es el caso de un movimiento sísmico, un huracán o cualquier otro fenómeno extremo de la naturaleza que se convierte en desastre o catástrofe cuando ocasiona pérdidas humanas o económicas. Es decir, se denomina desastre natural sólo cuando el problema social o económico es detonado por un fenómeno de la naturaleza. Loe Golden dice "un peligro latente se convierte en desastre si ocurre donde vive gente".

[11] Compromiso es exponer o poner a riesgo a alguien o algo en una acción o caso aventurado.

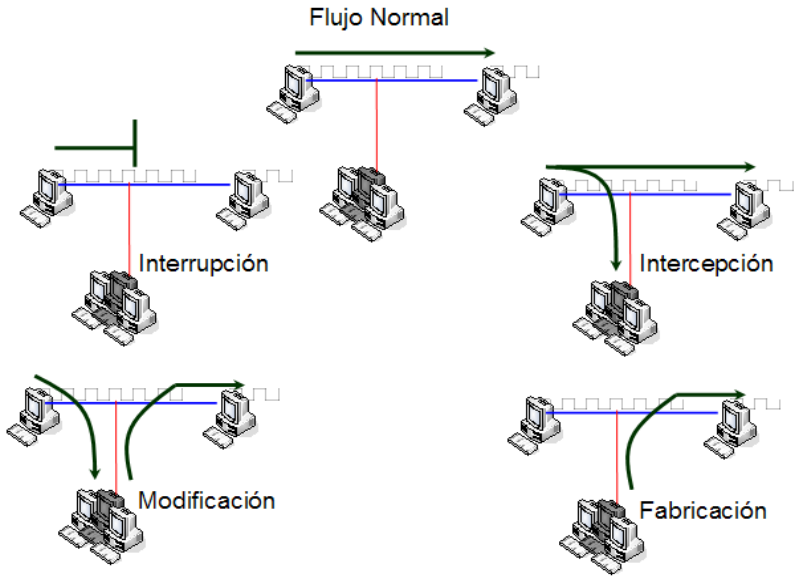

Figura 7 Principales tipos de amenazas a los sistemas de información

El flujo normal, en una comunicación en red, siempre va tener uno o varios sistemas compartiendo el medio (Internet o intranet corporativa, por ejemplo), aunque no necesariamente esto implica una actividad maliciosa sobre este flujo, pero una **vulnerabilidad** sobre los protocolos de información en donde se puede **materializar** alguna de las **amenazas** ilustradas anteriormente.

La **interrupción**, para fines de este ejemplo, puede hacerse presente en la ruptura del medio, (trozar el cable), y que se relaciona, estrechamente, con la seguridad física y la disposición, el cuidado del cableado, etc. en una determinada organización, la descompostura de los dispositivos de interconexión impidiendo la **disponibilidad** del sistema y los recursos que este provee, como consecuencia de una mala configuración del equipo de interconexión, actualizaciones de software, no llevadas a cabo, sobre estos dispositivos y su exposición a temperaturas inapropiadas para su buen funcionamiento o medios con humedad, fuego, etc. que evidencian un resguardo equivocado o una puesta en marcha con un análisis deficiente, otro ejemplo podría implicar, la destrucción o extravío de la información dentro del sistema. La intercepción implica la obtención de la información, pérdida de la confidencialidad, por un tercero no deseado, él cual puede divulgarla.

La **modificación**, otra de las amenazas, implica la alteración de la información, ya sea intencional o no intencional, perdiendo su **integridad**, un claro ejemplo es la alteración de la base de datos corporativa, donde se encuentra la nomina, omitiendo el pago de prima vacacional, por ejemplo. La **fabricación** consiste en la generación de datos falsos, no teniendo información base que sufriría cambios, como es el caso de la modificación, es más bien la realización de está, por el intruso

Un ejemplo más claro para diferenciar la **modificación** de la **creación** o fabricación, puede ser eliminar intencionalmente de un mensaje los signos de puntuación, el

significado de él mensaje será diferente al original (con signos de puntuación) y habrá sufrido una **modificación** (se trata de perdida de la **integridad** del mensaje), incluso las modificaciones realizadas por el ruido, inherentes al medio donde se trasmiten los datos, aunque en este caso no se trate de una acción realizada por un ente malicioso, si no por la naturaleza del medio, sin intención de arremeter con dolo, por otra parte el elaborar una nota de auxilio **ficticia** y enviarla a una estación policial implicando el despliegue de los elementos policíacos hacia el lugar del "supuesto"(**autenticidad**) siniestro, es un ejemplo claro de crear información..

Un **ataque**, término comúnmente ocupado, "*consiste en cualquier acción que explota una vulnerabilidad.*" [20] Es decir, acometer de forma maliciosa para explotar una vulnerabilidad, por ende podemos considerar ataques **pasivos** y **activos**. Los primeros son antesala a los ataques activos ya que analizan la información que obtienen, lo que muestra la pérdida de la confidencialidad, es decir observar el comportamiento sin perturbar "*el estado del sistema o de la información."* [21] (pp. 48)

"*Los ataques activos alteran el estado de la información o el sistema*" [22] (pp. 48) por lo que se ve afectada la integridad y autencidad de la información, en el caso de un ataque activo y como éste tiene como precedente un ataque pasivo, que atenta también la confidencialidad, utilizando la información obtenida del análisis, ataque pasivo, el atacante acomete con ánimo de causar daño, sin embargo, también dentro de los posibles atacantes se encuentran procesos o programas, no solo personas, con la capacidad de interceptar, leer, retener, engañar suplantando a las partes legítimas en una comunicación.

Los posibles ataques se presentan sobre los activos, un activo es el recurso del sistema de información o los relacionados con éste, necesario para que la organización funcione en base a los objetivos de la misión de la organización. De los activos, que trabajan con un fin común, característica propia de un sistema.

1.3.1 Características de los Sistemas

Sistema es un conjunto o combinación de objetos o partes que forman una unidad compleja, es decir es un todo organizado y complejo, otra definición es la siguiente: "*Un sistema es un conjunto de elementos dinámicamente relacionados formando una actividad para alcanzar un objetivo, operando sobre datos/energía/materia, para proveer información/energía/materia*" [23]. De la cual podemos conceptualizar un sistema de información como: un conjunto de elementos dinámicamente relacionados, que operando con datos, para proveer información; los datos y la información, forman actividades, estas conformadas en procedimientos, para alcanzar un objetivo, relacionado estrechamente, con la misión de la organización, mientras que cada procedimiento tendrá, por supuesto, un objetivo, que contribuye en un todo con la misión de la organización.

Los límites o fronteras entre el sistema y su ambiente admiten cierta arbitrariedad.

La organización se comprende entonces como un sistema, subsistema, o un súper sistema dependiendo del enfoque. Mientras que la totalidad del sistema esta representado por todos los componentes y relaciones necesarias para la realización de un objetivo, con ciertas restricciones. Los sistemas operan, tanto en serie como en paralelo en cuanto a las actividades que realizan.

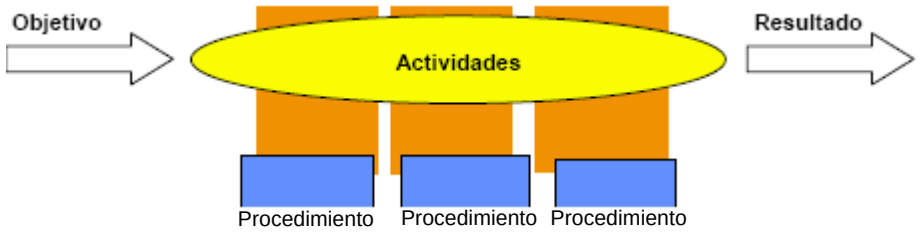

Figura 8 Flujo de las actividades[24]

"*Según Bertalanffy, sistema es un conjunto de unidades recíprocamente relacionadas. De ahí se deducen dos conceptos: propósito (u objetivo) y globalismo (o totalidad).*" [25]

Todo sistema tiene uno o varios propósitos. Los elementos (u objetos), como también las relaciones, definen una distribución que pretende alcanzar un objetivo; mientras que el Globalismo o totalidad se definen como un cambio en las unidades del sistema, con la probabilidad de que produzca cambios en las otras unidades. Existe una relación de causa/efecto, es decir, el efecto presenta un ajuste a todo el sistema, de aquí se derivan dos fenómenos la entropía y hemostasia.

"*La Entropía como el proceso mediante el cual un sistema tiende a consumirse, desorganizarse, morir*". [26] Además se establece que la entropía siempre es creciente en sistemas aislados. La entropía está relacionada con la tendencia natural de los objetos a caer en un estado de desorden. Está tendencia de los sistemas a desgastarse, a desintegrarse, como consecuencia, el relajamiento de los estándares y un aumento de la aleatoriedad, es decir, buscan un nivel más estable que tiende a ser lo más caótico. *"Aunque la entropía ejerce principalmente su acción en sistemas cerrados y aislados, afecta también a los sistemas abiertos; éstos últimos tienen la capacidad de combatirla a partir de la importación y exportación de flujos desde y hacia el ambiente, con este proceso generan neguentropía (entropía negativa)*." [27].

La entropía aumenta con el correr del tiempo. Si aumenta la información, disminuye la entropía, pues la información es la base de la configuración y del orden. De aquí nace la negentropía[12], o sea, la información como medio o instrumento de ordenación del sistema.

[12] La neguentropía, la podemos definir como la fuerza opuesta al segundo principio de la termodinámica, es una fuerza que tiende a producir mayores niveles de orden en los sistemas

"*El concepto de entropía fue introducido por primera vez por R. J. Clausius a mediados del siglo XIX. Clausius, ingeniero francés, también formuló un principio para la Segunda ley: "No es posible proceso alguno cuyo único resultado sea la transferencia de calor desde un cuerpo frío a otro más caliente". En base a este principio, Clausius introdujo el concepto de entropía, la cual es una medición de la cantidad de restricciones que existen para que un proceso se lleve a cabo y nos determina también la dirección de dicho proceso.*" [28]

Homeostasis es el equilibrio dinámico entre las partes del sistema. Los sistemas tienen una tendencia a adaptarse con el fin de alcanzar un equilibrio interno frente a los cambios externos del entorno.

El término Sistema de TI se refiere a un sistema de carácter general por ejemplo una mainframe, red de área local, o una aplicación mayor que puede funcionar sobre un sistema de soporte general y el cual utiliza recursos para satisfacer las necesidades de información de los usuarios.

"*Un sistema de TI es identificado definiendo límites alrededor de un conjunto de procesos, comunicaciones, almacenamiento y recursos relacionados (arquitectura). No necesariamente todos los componentes de un sistema deben estar conectados físicamente*" [29] (pp. 4), los ejemplos son: un grupo de computadoras personales (PCs) independientes en una oficina; un grupo de PCs situadas en los hogares de los empleados bajo un programa definido de reglas para el trabajo a distancia; un grupo de laptops (PCs portátiles) proporcionadas a los empleados que requieren la capacidad del computo móvil para desempeñar su trabajo; y un sistema con muchas configuraciones idénticas que son instaladas en localidades con el mismo ambiente y con los mismos controles físicos. Por ser parte de un sistema, tiene las características antes mencionadas, con un objetivo definido que sustenta a la misión de la organización, deberá mantener ciertos aspectos, relativos a la seguridad de la información, descritos en los servicios de seguridad.

---

abiertos, y la podemos relacionar con la conservación de la Energía, que predice que ésta ni disminuye ni aumenta, simplemente se transforma constantemente, y, en el caso de sistemas abiertos, con cualidad negantrópica, aumentando su nivel de organización. En tal sentido se puede considerar la neguentropía como un mecanismo auto-regulador con capacidad de sustentar, es decir con una capacidad y un poder inherente de la energía de manifestarse de incontables formas y maneras. La neguentropía favorece la subsistencia del sistema, usando mecanismos que ordenan, equilibran, o controlan el caos. Mecanismo por el cual el sistema pretende subsistir y busca estabilizarse ante una situación caótica.

1.4 Servicios de Seguridad

La seguridad de la información es proveer de características como *confidencialidad, integridad y autenticidad*[13] a la información en cada uno de los estados que se encuentre, es decir, prevenir durante estos procesos que la información se comprometa y además que sea accesible cuando se requiera por los entes legítimos, es decir que sea disponible. Estas características de seguridad se proveerán en base a la importancia que tenga la información en el proceso organizacional y evaluando cual o cuales de estas características tendrá mayor significancia o importancia en cada proceso, mediante el estudio y análisis comparativo de las circunstancias de una situación de riesgo, la probabilidad de ocurrencia, además de los factores que intervienen en un determinado proceso, para tratar de prever su evolución. "*Los objetivos en seguridad pueden traslaparse o pueden ser mutuamente exclusivos. Por ejemplo, requerimientos fuertes de confidencialidad pueden restringir severamente la disponibilidad*." [30] (pp. 55) .El equilibrio de la implantación de controles con la productividad.

Además de otros aspectos que influyen, como son los costos inherentes de someterse a un determinado control, parte fundamental de la integración de servicios de seguridad en una organización.

La confidencialidad, característica de la seguridad de la información, se comprende como el permitir o denegar el acceso a determinada información, es decir sobre cuales activos del sistema se otorgan o conceder accesos y sobre quién o qué recaerá la facultad de autorizar o no el acceso. El concepto integridad, otro de los servicios de seguridad, según el contexto, puede tener diferentes significados como: precisión, exactitud, inalterabilidad, en el caso de modificación en los procedimientos aceptables y por los entes y/o procesos autorizados."*Es común reconocer tres aspectos de la integridad: acciones autorizadas, separación y protección de recursos, y detección y corrección de errores*" [31] (pp. 55).

La disponibilidad, característica de seguridad de la información, se aplica a datos y recursos como son: la presencia de datos y recursos en forma usable, la capacidad de responder a necesidades, la respuesta en tiempo además de "*asignación justa, tolerancia a fallas, utilidad o usabilidad, concurrencia controlada*" [32] (pp. 55).

Por lo cual un servicio de seguridad es una característica que debe tener un sistema para satisfacer una política de seguridad, parte importante en el cumplimiento de los objetivos que sustentan la misión de la organización. En donde se destaca la utilización de un terminado mecanismo de seguridad es un procedimiento concreto utilizado para implementar el servicio de seguridad. En otras palabras, un servicio de seguridad identifica lo que es requerido; mientras que el mecanismo describe cómo lograrlo.

[13] En la Publicación Especial del NITS sp 800-26 "Computer Security".Considera que en la Integridad están incluidos los servicios de Autenticidad y No Repudio, considerados también pero de manera separada en el ISO 7498-2. Además de la Responsabilización.

En la arquitectura de seguridad **OSI**, Estándares **ISO 7498-2** y **ITU-T X.800**, identifica cinco clases de servicios de seguridad: confidencialidad, autenticación, integridad, control de acceso, y no repudio, que a continuación se describen.

1.4.1 Confidencialidad

El servicio de confidencialidad como tal puede darse en los siguientes tipos:

- ✓ Confidencialidad orientada a conexión.
- ✓ Confidencialidad no orientada a conexión.
- ✓ Confidencialidad selectiva.
- ✓ Confidencialidad aplicada al análisis de tráfico.

Confidencialidad orientada a conexión: Consiste en la protección de todos los datos de usuario en una comunicación orientada a conexión de nivel *N*.

Confidencialidad no orientada a conexión: Consiste en la protección de todos los datos de usuario contenidos en una sola unidad de datos del servicio (UDS) en una comunicación no orientada a conexión de nivel *N*.

Confidencialidad selectiva: Consiste en la protección de campos específicos de todas las unidades de datos de usuario de una comunicación orientada a conexión de nivel *N* o de una sola unidad de datos del servicio (UDS) en una comunicación no orientada a conexión de nivel *N*.

Confidencialidad aplicada al análisis del tráfico: Este servicio sirve para la protección de los datos frente a un análisis del tráfico originado por una comunicación entre entidades pares. Así un intruso podría analizar las direcciones origen y destino de las unidades de datos intercambiadas, la cantidad de datos transmitidos y la frecuencia con que tiene lugar la comunicación entre entidades pares.

1.4.2 Autenticación

Existen dos tipos de autenticación: **autenticación de identidad** o **identificación**, y **autenticación de origen de datos**. Este último tipo de autenticación se refiere a la certeza, de una manera in controversial y demostrable, el origen de los datos, es decir, extinguir la posibilidad de haber suplantado el origen. El servicio de autenticación está estrechamente relacionado al de control de acceso.

Autenticación del origen de los datos: Este servicio se aplica a comunicaciones no orientadas a conexión donde las unidades de datos son independientes y por lo tanto en esté caso lo más que se puede garantizar es que el origen de cada unidad de datos corresponde con la indicada en su cabecera (*header*). Este servicio puede ofrecerse en aplicaciones como el correo electrónico, donde no hay una comunicación previa entre entidades finales. (Este servicio esta asociado con el

servicio de integridad de datos no orientado a conexión; no parece muy útil asegurar la identidad del origen de los datos si no se puede garantizar su integridad).

Autenticación de entidades pares: Este servicio se aplica a comunicaciones orientadas a conexión. Al establecerse la conexión de nivel (N) este servicio asegura la identidad de las dos entidades que se comunican, es decir, se asegura que cada una es quién dice ser. Posteriormente en la fase de transferencia debe garantizar que un intruso no pueda suplantar a cualquiera de las dos entidades legítimas, un ataque común es el denominado de hombre en medio, que se comunican a efectos de transmisiones o recepciones no autorizadas.

La **autenticación**, entendida como proceso de **identificación** se clasifica en tres tipos, de acuerdo a la naturaleza de los elementos en que se basa su implementación: **En algo que se sabe**, **En algo que se tiene, En algo que se es.**
Para el caso de En algo que se sabe, la autenticación puede basarse en algo que se aprende o memoriza, tal como una contraseña, denominado también como *password*. Al ser revelado al receptor ante el cual se desea identificarse, se demuestra ser quien se dice ser.

Cuando se trata de **algo que se tiene**, la autenticación se basa en un objeto tangible tal como una moneda, una llave física (metal), o cualquier otro objeto con esta finalidad, identificación del poseedor.

En el tercer caso, **En algo que se es**; también denominada autenticación biométrica; la identidad se demuestra comparando patrones relacionados a alguna característica inherente a la naturaleza de la entidad que se identifica, que denota exclusividad. Una característica inherente a su naturaleza podría ser sus huellas digitales, su voz, etc., en el caso de una persona.

La autenticación también puede ser **directa** o **indirecta**. Es directa "*si en el proceso de autenticación sólo intervienen las partes interesadas o que se van a autenticar*" [33] (pp. 64). Es decir, no interviene ninguna tercera parte actuando como juez. Es indirecta "*si en el proceso interviene una tercera parte confiable que actúa como autoridad o juez que avala la identidad de las partes*" [34] (pp. 64).

También la autenticación puede ser **unidireccional** o **mutua**. Es unidireccional si con que una de las partes que se autentique ante la otra basta. Es mutua cuando se requiere que ambas partes se autentiquen entre sí.

1.4.3 Integridad

El servicio de Integridad como tal identifica los siguientes servicios

- ✓ Integridad con conexión con recuperación.
- ✓ Integridad con conexión sin recuperación.
- ✓ Integridad con conexión selectiva a campos.
- ✓ Integridad sin conexión.
- ✓ Integridad sin conexión selectiva a campos.

Integridad orientada a conexión con mecanismos de recuperación: Proporciona la integridad de todos las unidades de datos de usuario de una comunicación orientada a conexión de nivel *N* y detecta cualquier modificación, inserción, borrado o retransmisión de cualquier unidad de datos dentro de una secuencia entera de unidad de datos del servicio (SDU[14]) haciendo uso de mecanismos de recuperación de la integridad si fuera necesario. El uso de este servicio junto con el servicio de autenticación de entidad par proporciona un alto grado de protección frente a la mayoría de ataques activos.

Integridad orientada a conexión sin mecanismos de recuperación: Este servicio es semejante al anterior con la diferencia de que en este caso sólo se detecta las violaciones en la integridad de los datos pero no se articulan mecanismos de recuperación de la integridad.

Integridad orientada a conexión sobre campos selectivos: Este servicio asegura la integridad de campos específicos dentro de las unidades de datos de usuario de nivel N en una comunicación orientada a una conexión y toma una determinación de si los campos seleccionados han sido modificados, insertados, borrados o retransmitidos.

Integridad no orientada a conexión: Este servicio asegura la integridad de una sola unidad de datos del servicio (SDU) en comunicaciones no orientadas a conexión, teniendo alguna forma de detección de la modificación de una SDU. Adicionalmente también pueden existir algunos mecanismos que garanticen la detección de retransmisiones.

Integridad no orientada a conexión sobre campos selectivos: Este servicio asegura la integridad de campos específicos dentro de una sola unidad de datos del servicio (SDU) en comunicaciones no orientadas a conexión. Este servicio toma alguna determinación si los campos seleccionados han sido modificados.

[14] La unidad de datos de servicio, SDU por sus sigla es inglés *Service Data Unit* es un sistema de datos que son enviados por un usuario de los servicios de una capa dada, y se transmite a un usuario de servicio del par semántico sin cambiar. El SDU es básicamente los datos que cierta capa pasará hacia una capa inferior. A diferencia de la PDU (*protocol data unit*) que especifica los datos que serán enviados a la capa del protocolo par en el extremo de recepción.

La manera en que este servicio de seguridad se implementa normalmente es a través de la utilización de funciones hash o funciones de dispersión, un tipo de criptografía que no utiliza llaves.

1.4.4 El Control de Acceso

El **control de acceso** protege a los activos del sistema contra accesos y uso no autorizados. Éste es de los servicios que normalmente no utilizan técnicas criptográficas para su implementación; en cambio, existe un gran número de técnicas propias y tipos de control de acceso, así como también modelos específicos para su implementación. Este servicio está cercanamente relacionado al de autenticación ya que un usuario debe ser autenticado antes de tener acceso a los activos del sistema. Por esta razón, su estudio detallado se integra con el de autenticación, en algunas de sus partes. (Administración de identidades).

1.4.5 El No Repudio

El no repudio proporciona protección contra la posibilidad de que alguna de las partes involucradas en una comunicación niegue haber enviado o recibido un mensaje, u originado o haber sido el destinatario de una acción. Los servicios de no repudio identificados son:

- ✓ No repudio con prueba de origen. Este servicio proporciona los mecanismos necesarios para asegurar que el mensaje fue enviado por la entidad especificada.
- ✓ No repudio con prueba de entrega. Este servicio proporciona los mecanismos necesarios para asegurar que el mensaje fue recibido por la entidad especificada.

Para implementar este servicio se utilizan esquemas de **llave pública** tales como las **firmas digitales**, pero no se restringe a ellas; también se pueden utilizar técnicas de cifrado de llave secreta y de llave pública pero, en esta última, siempre que se utilice una **tercera parte confiable** (Autoridad Certificadora).
Los servicios de seguridad son características deseables en un sistema de información, en cuanto el procedimiento concreto para la implementación del servicio de seguridad, es decir el cómo, se denomina mecanismo.

1.5 Mecanismos de Seguridad

Los servicios de seguridad son implementados mediante mecanismos de seguridad. Un servicio de seguridad puede utilizar uno o varios mecanismos de seguridad.

Los mecanismos de seguridad se agrupan en dos categorías: los específicos y los penetrantes (filtros).

En los mecanismos específicos se encuentran el "*cifrado, la firma digital, el control de acceso, la integridad, la autenticación, protección contra el análisis de tráfico (Traffic Padding), Control de Ruteo y Notarización*" [35] (pp. 62, 63) descritos a continuación.

1.5.1 Cifrado

El **cifrado** puede proporcionar la confidencialidad de la información de datos o del flujo de tráfico y puede desempeñar una función en varios otros mecanismos de seguridad o complementarlos, según se describe en los puntos siguientes:
Los algoritmos de cifrado pueden ser **reversibles o irreversibles**.
Los algoritmos de cifrado **reversibles** pueden ser de dos tipos:

- ✓ **El cifrado simétrico** (es decir, con llave secreta), en el cual el conocimiento de la llave del cifrado implica el conocimiento de la llave de descifrado y viceversa.
- ✓ **El cifrado asimétrico** (por ejemplo, con clave pública), en el cual el conocimiento de la clave del cifrado no implica el conocimiento de la clave de descifrado, o viceversa. Algunas veces las dos claves de este sistema se denominan: llave pública y llave privada.

Los **algoritmos de cifrado irreversibles** pueden utilizar o no una llave. Cuando utilizan una llave, ésta puede ser pública o secreta.
La existencia de un mecanismo de cifrado implica el uso de un mecanismo de administración de llaves, salvo en el caso de algunos algoritmos de cifrado irreversibles.

1.5.2 Firma Digital

Estos mecanismos definen dos procedimientos:

- ✓ **firma de una unidad de datos**; y
- ✓ **verificación de una unidad de datos firmada**.

El primer proceso utiliza información que es privada (es decir, única y confidencial) del firmante. El segundo proceso utiliza procedimientos de información que están

disponibles públicamente, pero a partir de los cuales no puede deducirse cuál es la información privada del firmante.

El proceso de **firma** conlleva un cifrado de la unidad de datos o la producción de un valor de control criptográfico de la unidad de datos, utilizando la información privada del firmante como una llave privada.

El proceso de **verificación** conlleva la utilización de los procedimientos e información públicos para determinar si la firma se produjo con la información privada del firmante.

La característica esencial del mecanismo de firma es, que la firma sólo puede producirse utilizando la información privada del firmante. De este modo, cuando se verifica la firma, puede probarse subsiguientemente a una **tercera parte** (por ejemplo, a un juez o árbitro), en cualquier momento, que sólo el poseedor único de la información privada pudo haber producido la firma.

Estos mecanismos pueden utilizar la identidad **autenticada** de una entidad o información sobre la entidad (tal como la lista de miembros de un conjunto conocido de entidades) o capacidades de la entidad, para determinar y aplicar los **derechos de acceso** de la entidad. Si la entidad intenta utilizar un recurso no autorizado, o un recurso autorizado con un tipo impropio de acceso, la función de control de acceso rechazará la tentativa y puede informar además el incidente a los efectos de generar una alarma y/o anotarlo en el registro de auditoria de seguridad. La notificación al expedidor del rechazo de acceso para una transmisión de datos en modo sin conexión puede proporcionarse solamente como resultado de controles de accesos impuestos en el origen.

1.5.3 Control de Acceso

Los **mecanismos de control de acceso** pueden basarse, por ejemplo, en la utilización de uno o más de los elementos siguientes:

a. Bases de información de control de acceso, donde se mantienen los derechos de acceso de entidades pares. Esta información debe ser mantenida por centros de autorización o por la entidad a la que se accede, y puede tener la forma de una lista de control de acceso o de una matriz de estructura jerárquica o distribuida. Esto presupone que se ha asegurado la autenticación de la entidad par.
b. Información de autenticación como contraseñas, cuya posesión y presentación anterior son la prueba de la autorización de la entidad que efectúa el acceso.
c. Capacidades, cuya posesión y presentación anterior son la prueba del derecho a acceder a la entidad o recurso definido por la capacidad.

Cabe mencionar que una capacidad debe ser in usurpable y debe transmitirse de una manera fiable.

d. Etiquetas de seguridad, que cuando están asociadas con una entidad, pueden utilizarse para conceder o negar el acceso, en general de acuerdo con una política de seguridad.
e. Hora del intento de acceso.
f. Ruta del intento de acceso, y
g. Duración del acceso.

Pueden aplicarse mecanismos de control de acceso en cualquiera de los dos extremos de una asociación de comunicaciones y/o cualquier punto intermedio.
Los controles de acceso aplicados en el origen con cualquier punto intermedio se utilizan para determinar si el emisor está autorizado a comunicar con el destinatario (receptor) y/o a utilizar los recursos de comunicaciones requeridos.

En una transmisión de datos en modo sin conexión, los requisitos de los mecanismos de control de acceso de la entidad par en el destino, deben conocerse con prioridad en el origen, y deben registrarse en la base de informaciones de gestión de seguridad

1.5.4 Integridad de los Datos

La integridad de los datos tiene dos aspectos: la integridad de una sola unidad de datos o de un sólo campo, y la integridad de un tren de unidades de datos o de campos de unidad de datos. En general, se utilizan diferentes mecanismos para proporcionar estos dos tipos de servicios de integridad, aunque no es práctica la provisión del segundo sin el primero.

La determinación de la **integridad** de una sola unidad de datos entraña dos procesos, uno en la entidad **emisora** y otro en la entidad **receptora**. La entidad emisora **añade** a una unidad de datos una cantidad que es una función de los propios datos. Esta cantidad puede ser una información suplementaria, tal como un **código de control de bloque** o un **valor de control criptográfico**, y puede estar cifrada. La entidad **receptora** genera una cantidad correspondiente y la **compara** con la cantidad, la cual está en función de los propios datos, recibida para determinar si los datos han sido modificados en tránsito. Este mecanismo por sí solo no ofrecerá protección contra la reproducción de una sola unidad de datos. En las capas apropiadas de la arquitectura, la detección de una manipulación puede conducir a una acción de recuperación (por ejemplo, una retransmisión o una corrección de error) en esa capa o en otra superior.

Para la **transferencia** de datos en modo con conexión, la protección de la **integridad** de una secuencia de unidades de datos (es decir, la protección contra errores de secuenciación, pérdida, reproducción, inserción o modificación de datos) requiere además alguna forma de ordenación explícita, como la numeración de secuencias, el estampado de la hora (*time stamping*) o el encadenamiento criptográfico.

Para la transmisión de datos en modo sin conexión, el estampado de la hora puede utilizarse para proporcionar una forma limitada de protección contra la reproducción de unidades de datos individuales.

1.5.5 Intercambio de Autenticación

Algunas de las técnicas que pueden aplicarse a los intercambios de autenticación son:

a. utilización de información de autenticación, como contraseñas, suministradas por una entidad emisora
b. y verificadas, por la entidad receptora;
c. técnicas criptográficas; y
d. uso de características y/o propiedades de la entidad.

Los mecanismos pueden incorporarse en la capa (N) para proporcionar autenticación de la entidad par. Si el mecanismo no logra autenticar la entidad, el resultado será el **rechazo o la terminación de la conexión** y puede causar también una anotación en el registro de **auditoria de seguridad** y/o un informe a un centro de **gestión de seguridad**.

Cuando se utilizan técnicas criptográficas, éstas pueden combinarse con protocolos de toma de contacto: como protección contra la repetición (es decir, asegurar el funcionamiento en tiempo real). Mediante el estampado de la hora y relojes sincronizados (GPS);

a. dos o tres tomas de contacto (para autenticación unilateral y mutua respectivamente); y
b. servicios de no repudio, mediante firma digital y mecanismos de notarización.

El estampado de la hora al igual que la sincronización de relojes en los protocolos para autenticación podrían tornarse demasiado engorrosos, la utilización de números pseudoaleatorios en el protocolo es otra opción por lo que es necesario analizar, para éste último caso, la utilización de un generador de números pseudoaleatorios, debido a que sí no se elije un generador de números pseudoaleatorios con el suficiente tiento podría significar una vulnerabilidad, utilizando repetición de los datos enviados por una entidad legítima a otro tiempo pero ahora enviados por una entidad ilegitima, para el protocolo de autenticación.

1.5.6 Relleno de Tráfico (Traffic Padding)

Pueden utilizarse mecanismos de relleno de tráfico para proporcionar diversos niveles de protección contra análisis del tráfico. Este mecanismo puede ser eficaz solamente si el relleno de tráfico está protegido por un servicio de confidencialidad.

1.5.7 Control de Enrutamiento

Las rutas pueden elegirse dinámicamente o por acuerdo previo con el fin de utilizar sólo subredes, relevadores o enlaces físicamente seguros.
Al detectar ataques de manipulación persistentes, los sistemas extremos pueden dar instrucciones al proveedor del servicio de red que establezca una conexión por una ruta diferente.

La política de seguridad puede prohibir que los datos que transportan ciertas etiquetas de seguridad pasen a través de ciertas subredes (MPLS por ejemplo), relevadores o enlaces. Asimismo, el iniciador de una conexión (o el expedidor de una unidad de datos en modo sin conexión) puede especificar prohibiciones de encaminamiento en las que se indica que se eviten determinadas subredes, enlaces o relevadores.

1.5.8 Notarización

Pueden garantizarse las propiedades sobre los datos comunicados entre dos o más entidades, tales como su integridad, origen, fecha y destino, mediante la provisión de un mecanismo de notarización. La seguridad es proporcionada por una tercera parte que actúa como notario, en el que las entidades comunicantes tienen confianza y que mantiene la información necesaria para proporcionar la garantía requerida de una manera verificable. Cada instancia de comunicación puede utilizar la firma digital, el cifrado y los mecanismos de integridad, según sea apropiado, para el servicio que es proporcionado por el notario. Cuando se invoca este mecanismo de notarización, los datos se comunican entre las entidades comunicantes por las instancias de comunicación protegidas y el notario.

1.6 Implantación de Mecanismos de Seguridad

Para la implantación de mecanismos de seguridad se debe de desarrollar cuidadosamente, objetivos para cada caso de negocio[15], las necesidades de servicios de seguridad en las TI deben basarse en las necesidades del negocio, es decir, en las necesidades de la organización. Un caso de negocio contiene un análisis de la solución propuesta, el costo estimado, los beneficios analizados, un proyecto de análisis de riesgos y una evaluación de otras alternativas consideradas. Debe proveer suficiente documentación para describir y sustentar esas necesidades.

i. Desarrollo concreto de los acuerdos de servicio, que definen las expectativas del funcionamiento para cada control de seguridad requerido, además de describir resultados mesurables, e identificar las soluciones y respuestas para cualquier instancia identificada de incumplimiento.

[15] Veáse el anexo C; se muestra un formato para caso de negocio

ii. Utilizar métricas a través del ciclo de vida de la seguridad de las TI. Las métricas proporcionaran los datos objetivos para evaluar el *baseline*[16] de los niveles de servicio, en la fase de evaluación, para determinar el rendimiento del proveedor de servicio, en la fase operacional. Las métricas, en lo posible, deberán ser seleccionadas para indicar progreso con objeto de lograr o mantener una condición de seguridad que resuelva una necesidad de seguridad subyacente.

iii. Desarrollar procesos y procedimientos que pueden seguir con eficacia los acuerdos de servicio y las métricas que serán aplicadas a través del ciclo de vida de muchos y diferentes servicios de seguridad en las TI dentro de una organización.

iv. Asegurarse que haya un apropiado periodo de transición (internamente) es una posición entre un proveedor de servicio o una capacidad existente y un nuevo proveedor de servicio.

v. Mantener el nivel técnico necesario para entender y manejar el o los servicios de seguridad que son proporcionados y para proteger los datos críticos enfocados en la misión de la organización.

vi. Poner especial atención a las seis áreas en cuestión: estrategia/misión, presupuestos/financiamiento, tecnología/arquitectura, organización, personal, políticas/procesos.

vii. La evolución tecnológica y las necesidades de la organización tienen que relacionarse directamente, por lo cual se tiene en cuenta como administrar controles efectivos durante el Ciclo de Vida del Desarrollo de un sistema.

1.6.1 Ciclo de Vida del Desarrollo de un Sistema-SDLC (System Developement Lice Cycle)

"*Como otros aspectos de los sistemas de procesamiento de información, la seguridad es más efectiva y eficiente si se planea y administra a través del ciclo de vida de los sistemas computacionales. Desde la planeación inicial, pasando por el diseño, implementación y operación a disposición*" [36] (pp. 73). El Ciclo de Vida del Desarrollo de un Sistema (SDLC) se refiere al alcance completo de las actividades conducidas por los propietarios del sistema que se asocian a este durante el periodo de vida del sistema. Muchos de los eventos y análisis de seguridad relevantes ocurren durante la vida del sistema.

Una organización tendrá típicamente muchos planes de la seguridad en cómputo. Sin embargo, no es necesario que exista un plan separado y distinto para cada sistema físico (por ejemplo, PC). Los planes pueden englobar, por ejemplo, los recursos

[16] Baseline es una línea o un estándar imaginario por el cual las cosas son medidas o comparadas. Especificaciones iniciales establecidas.

informáticos dentro de un elemento operacional, de un uso importante, o perteneciente a un grupo de sistemas similares (cualquiera tecnológico o funcional).

El SDLC consta de varias fases descritas en el siguiente apartado.

1.6.1.1 Fases del SDLC

Varios “ciclos de vida” son asociados con los sistemas informáticos o de cómputo, incluyendo el desarrollo de sistemas adquisición y ciclo de vida de la información. Hay muchos modelos para el ciclo de vida del sistema informático pero la mayoría contiene cinco fases básicas

i. Iniciación. Durante la fase de la iniciación, la necesidad de un determinado sistema se expresa y el propósito del mismo se documenta.

ii. Desarrollo/adquisición. Durante esta fase el sistema es diseñado, comprado, programado, desarrollado, o de lo contrario construido. Esta fase consiste en otros ciclos definidos, tales como el ciclo de desarrollo del sistema o el ciclo de adquisición.

iii. Implementación. Después de probar el sistema inicial el sistema es instalado o presentado.

iv. Operación/Mantenimiento. Durante esta fase el sistema efectúa su trabajo. El sistema es modificado la mayoría de las veces por la adición de hardware y software y por otros numerosos eventos.

v. Disposición. El sistema informático es dispuesto una vez que la transición a un nuevo sistema informático se termina.

El objetivo primario del SDLC es asegurar que el sistema es: desarrollado de acuerdo con los requerimientos indicados, trabaja efectivamente, tiene un costo real[17] y es sostenible. La inclusión de controles de seguridad y métricas durante el proceso ayuda asegurar que: salvaguardas[18] como parte del diseño, los costos de desarrollo y/o adquisición incluirán seguridad y el progreso se puede alcanzar.

La figura siguiente, Fases del SDLC, muestra las cinco fases enlazadas entre sí y que conforman el ciclo de vida del desarrollo de un sistema.

[17] Costo Real costos históricos que se han incurrido en un periodo anterior.
[18] Salvaguarda cosa que asegura o protege contra algún riesgo o necesidad también se refiere a un control con la finalidad de asegurar o proteger contra algún riesgo o necesidad.

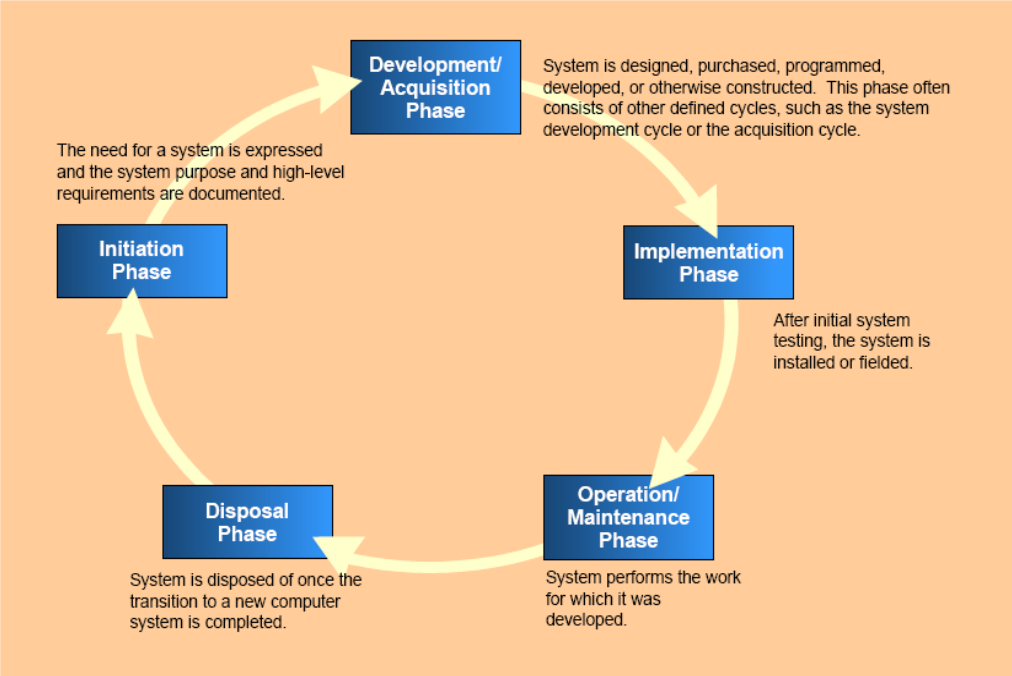

Figura 9 Fases del SDLC [37] (pp.12)

En adición, los siguientes siete pasos progresivos se diseñan para ser integrados en cada etapa del ciclo de vida del desarrollo del sistema.

1) Desarrollar el enunciado de la política del plan de contingencia. Una política formal del departamento o el organismo que proporcionan la autoridad y guía necesaria para desarrollar un plan de contingencia eficaz.
2) Conducir el Análisis de impacto al negocio que en sus siglas en ingles se le denomina BIA (Business Impact Analysis). El BIA ayuda a identificar y priorizar los sistemas y componentes críticos de TI. Una plantilla del BIA es desarrollada para proporcionar asistencia del usuario.
3) Identificar los controles preventivos. Las medidas tomadas para reducir los efectos de las interrupciones del sistema pueden incrementar la disponibilidad del mismo y reducir costos del ciclo de vida de la contingencia
4) Desarrollar estrategias de recuperación. A través de la estrategia de recuperación y asegurar que el sistema pueda ser recuperado rápida y efectivamente después de una interrupción.
5) Desarrollar el plan de contingencias de TI. El plan de contingencia debe contener una guía detallada y procedimientos para restablecer un sistema dañado.
6) El plan de pruebas, capacitación y ejercicios. El plan de pruebas identifica huecos en la planeación, mientras que la capacitación en la recuperación,

prepara al personal para el plan de activación; ambas actividades proporcionan eficiencia al plan y la disposición total de la organización.

7) Mantenimiento del Plan. El plan debe ser un documento subsistente que se pone al día cada día regularmente para seguir siendo actual con las mejoras del sistema.

Como parte de la evolución de las especificaciones iníciales establecidas, *baseline,* y su conformación con los niveles de servicio, tanto en la fase operacional como en la fase de evaluación, mediante la utilización de métricas proporcionadas por el ciclo de vida de la seguridad de las TI que a continuación se describe.

1.6.2 Ciclo de Vida de la Seguridad (Security Life Cycle)

Muchas empresas se basan en procesos cíclicos, tales son los casos de: el ciclo de comprar y vender, el ciclo de desarrollo de aplicaciones y el Ciclo de vida de la Seguridad (SLC). En el ámbito de la seguridad en las TI, el ciclo de vida de la seguridad puede orientar de forma efectiva ocupándose de las etapas fundamentales en el éxito de garantizar el éxito de las operaciones y de los negocios, a continuación se analizará éste ciclo.

Las **Políticas, estándares y directrices** (*guidelines*) son el fundamento que rigen las cuatro fases del ciclo de vida de la Seguridad.

Las políticas se aseguraran que varias áreas importantes como son controles, el área jurídica y la clasificación de la información estén cubiertos cabalmente; en cuanto a las normas se refiere, éstas deben garantizar un control adecuado sobre las configuraciones de los diversos componentes y el software en cuestión, por su parte las directrices prácticas (*guidelines*), garantizan la ejecución de las tareas en forma ordenada y previsible.
En la siguiente figura se muestran las fases del SDLC.

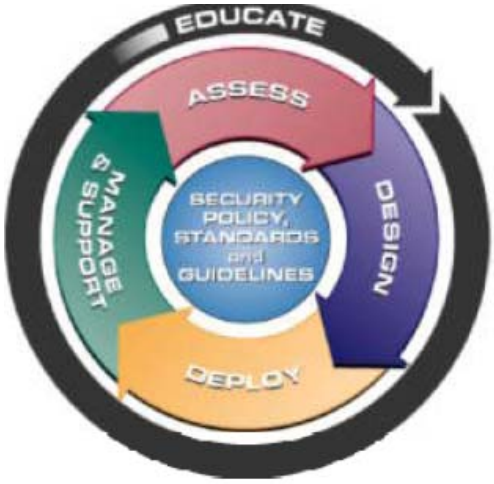

Figura 10 Ciclo de vida de la Seguridad[38] (pp. 1)

A continuación se muestra el ciclo de vida de la seguridad conformado por las cuatro fases fundamentadas en las políticas, los estándares y las directrices (*guidelines*), englobando un entrenamiento continuo en todas las fases.

La primera fase es la evaluación considerada como un acontecimiento crucial, que determina el proyecto de ley en seguridad, que determina, a su vez, la salud de cualquier sistema.

Actividades como son auditorias, **pruebas de penetración**[19] (pen Test) y revisiones se llevarán a cabo periódicamente, o cuando surjan necesidades, tal es el caso de un cambio importante. Normalmente la evaluación de riegos se calcula a partir de los datos recabados.

El **diseño** es la segunda fase del SLC se basa en la organización y las normas de la industria, es una etapa importante ya que provee una adecuada configuración de seguridad, el diseño comprende actividades como la formulación y el proceso de mejora con respecto al diseño en sí.

La **implementación** es la tercera fase y consiste en desplegar el diseño elaborado en la etapa o fase anterior, los especialistas y el personal calificado que tiene que ser empleado para estas actividades.

Por último la **administración** y el monitoreo son fundamentales para asegurar que el sistema sea funcional y ayuda de manera proactiva como un mecanismo de detección de problemas.

Es necesario contar con **capacitación continua** en todo el ciclo de vida en los diferentes niveles organizacionales, las aptitudes y conocimiento se plantearán dentro de este proceso.

[19] Las Pruebas de Penetración o Pen Test están diseñadas para detectar vulnerabilidades y brechas de seguridad que puedan ser utilizadas por personas malintencionadas para atacar y penetrar en la red interna de una organización.

Las políticas, estándares y directrices, como se menciono anteriormente, son la base que rige el SLC, y por lo cual muchos organismos se han dado a la tarea de recabar e incorporar, de forma evolucionada, en diferentes organizaciones, con el objetivo de beneficiarse de la aplicación de las políticas, estándares y directrices.
En el siguiente apartado se ahondara en esta temática.

1.7 Buenas Prácticas y Estándares

Las organizaciones frecuentemente deben evaluar y elegir entre una gran variedad de tecnologías de información que proveen servicios de seguridad que mantengan y mejoren la totalidad de los servicios que la organización ofrece. Estos servicios dependen, en menor o gran medida, de la infraestructura tecnológica, además deben cubrir los objetivos plasmados en la misión de la organización. Esto mediante un programa de seguridad conformado por el reconocimiento y la concordancia de todas las áreas involucradas.

"*Como cualquier otra actividad colectiva humana se requieren políticas, normas y vigilancia de las mismas para mejorar su desempeño. Cualquier actividad que se trata de llevar a cabo en forma caótica, sin reglas aceptadas por todos los participantes, tiende a fallar o a funcionar en forma torpe y hasta dañina*". [39] (pp. 5)

Teniendo como premisa el llevar a cabo una buena administración, varios organismos se han dado a la tarea de recabar recomendaciones y buenas prácticas, que han sido adoptadas por organizaciones de diferentes rubros con la finalidad de incrementar productividad, mantener el orden y cumplir con los objetivos que sustentan la misión de cada organización.

El mantener niveles aceptables de operación mediante los servicios de seguridad, que se proveen, se plasman explícitamente en las políticas de seguridad, al igual que los mecanismos utilizados, los cuales marcan el alcance y nivel de responsabilización de los involucrados, entre otros aspectos. La puesta en marcha de controles tiene la finalidad de reducir el riesgo, es decir, mitigar el impacto a consecuencia de la materialización de una amenaza mediante una práctica, procedimiento o mecanismo, para cumplir cabalmente con los objetivos.

En consecuencia, se explicarán, la fundamentación de la administración en la Seguridad de la Información y la de los servicios de TI.

1.7.1 Gestión de la Seguridad de la Información

La gestión de la seguridad consiste en la realización de las tareas necesarias para garantizar los niveles de seguridad exigibles en una organización, por lo que se debe considerar que los riesgos no se eliminan si no que se gestionan con el objetivo de minimizar el impacto sobre los activos y garantizar la continuidad del negocio, además de que los problemas de seguridad no son únicamente de índole

tecnológico, si no que también abarcan un gran abanico de posibles amenazas incluso las nunca materializadas y para las cuales no se cuenta con un plan, por lo que la seguridad no debe pensarse como un producto, si no como un proceso *ad hoc* para cada organización.

Un Sistema de Gestión de la Seguridad de la Información (SGSI) comprende la política, la estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de la seguridad de la información.
Además de que cubre aspectos organizativos, lógicos, físicos, legales y es también independiente de plataformas tecnológicas y mecanismos concretos.

Las organizaciones pueden beneficiarse cuando las opciones entre servicios y los proveedores de servicios estimulen la competencia y traigan la innovación al mercado. Sin embargo, es difícil determinar las capacidades del proveedor de servicio, medir confiabilidad del servicio y guiar sobre las complejidades implicadas en acuerdos de servicios de seguridad. Los individuos que son responsables de seleccionar, de poner, y de conducir la ejecución de los servicios de seguridad para una organización deben evaluar cuidadosamente sus opciones, antes de seleccionar los recursos que serán confiados para resolver las particularidades de las TI, en base a los requisitos del programa de la seguridad.

Los factores que deben considerarse cuando se seleccionan, implementan y gestionan o administran los servicios de seguridad de las TI incluyen: el tipo de acuerdo de servicio; las calificaciones del proveedor de servicio, los requisitos y capacidades operacionales, la experiencia, y la viabilidad; formalidad de los empleados del proveedor de servicio; y la capacidad del proveedor de servicio para entregar la protección adecuada para los sistemas, los usos, y la información de la organización. Estas consideraciones se aplicarán (en los niveles correspondientes) a cada servicio dependiendo del tamaño, del tipo, de la complejidad, del coste, y de la criticidad de los servicios que son considerados, además de las necesidades específicas de la organización que se ponen en ejecución o que se contraen de los servicios.

Como parte del gran abanico de posibilidades entre los proveedores de servicio, algunas empresas como Gartner Inc., aporta información concisa que guiará a la toma de decisiones, debe de tomarse en cuenta que los estudios realizados por Gartner Inc. o alguna otra de similar perfil, realiza pruebas en localidades especificas y dependiendo de la región geográfica, donde se pretende implementar un control utilizando infraestructura tecnológica, por lo tanto la presencia del proveedor tecnológico no es la misma en los Estados Unidos que en Chile, por ejemplo, si trata de aplicaciones criticas y la base tecnológica no cuenta con un soporte del proveedor que cubra las necesidades de la organización, a pesar de ser un excelente producto, podría significar grandes tiempos de espera en una contingencia, vitales en la toma de decisiones y recuperación del sistema. La realización de pruebas de concepto es una opción que permitirá evaluar la alternativa tecnológica de un determinado proveedor y éstas deben hacerse en un ambiente de pruebas propio de la organización, no es recomendable realizarlo en un ambiente productivo por las

implicaciones en cuanto la estabilidad de la herramienta en un ambiente productivo podría presentarse y los riesgos que a éste se relacionan.

En cuanto a tecnología se refiere, que en conjunto con las necesidades de la organización, permitirá una evolución en los servicios que dependen de la infraestructura tecnológica. A continuación la información relativa a la Gestión o Administración de Servicios de TI.

1.7.2 Gestión de Servicios de TI

El concepto de gestión de servicios de TI, aunque relacionado con ITIL, no es idéntico a ITIL, ya que este último contiene una sección específicamente denominada Gestión de Servicios de Tecnologías de Información. La Gestión de Servicio ITIL está actualmente integrada en el estándar ISO 20000

La Gestión de servicios de TI tiene como objetivos el alinear los servicios de TI, con las cambiantes necesidades del negocio, mejorar la calidad de estos servicios y reducir los costos de largo plazo en la entrega de los servicios de TI. Por lo que la gestión de servicios debe entenderse como la entrega de servicios de TI centralizada hacia aquellos que utilizan con asiduidad los servicios, utilizando una perspectiva orientada a procesos.

Los procesos como tal son la serie de acciones, actividades, cambios conectados entre si y realizados por agentes con el fin de satisfacer un propósito o conseguir una meta, a nivel organización, comprende las actividades realizadas por varios departamentos con un objetivo común y siguen una serie de procedimientos para la obtención de un resultado, estos procedimientos dictaminaran el conjunto de responsabilidades, actividades y autorizaciones que recae en cada tarea, es decir los roles, y delimitará claramente los preceptos que recaerán sobre cada tarea.

La serie ISO/IEC 20000 - Service Management normalizada y publicada por las organizaciones ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission) el 14 de Diciembre de 2005, es el estándar reconocido internacionalmente en gestión de servicios de TI (Tecnologías de la Información). La serie 20000 proviene de la adopción de la serie BS 15000 desarrollada por la entidad de normalización y certificación británica BSI - British Standard Institute. Organizado en dos partes, la primera de las cuales define los requerimientos necesarios para realizar una entrega de servicios de TI alineados con las necesidades del negocio, con calidad y valor añadido para los clientes, asegurando una optimización de los costes y garantizando la seguridad de la entrega en todo momento. El cumplimiento de esta parte, garantiza además, que se está realizando un ciclo de mejora continuo de la gestión de servicios de TI. La segunda parte representa el conjunto de mejores prácticas adoptadas y aceptadas por la industria en materia de Gestión de Servicio TI. Está basada en ITIL y sirve como guía y soporte en el establecimiento de acciones de mejora en el servicio o preparación de auditorias contra el estándar ISO/IEC 20000-1:2005

En los años 80 la calidad del servicio de TI proporcionado por el gobierno Británico era tal que el CCTA (*Central Computer and Telecommunications Agency. Ahora Office of Government Commerce*, OGC) fue comisionado para desarrollar un enfoque del uso eficiente y rentable de los recursos de TI del sector público. Numerosas organizaciones comenzaron a colaborar, con el fin de proporcionar un enfoque independiente de cualquier proveedor. Esto dio lugar a *Information Technology Infrastructure Library*™ (ITIL®). ITIL® creció hasta llegar a ser una colección de las mejores prácticas observadas en la industria de servicios de TI.

Aunque se desarrolló en los años ochentas, ITIL no fue implementada hasta mediados de los 90, se considera a menudo junto con otros marcos de trabajo de mejores prácticas como *Information Services Procurent Library* (ISP, "Biblioteca de adquisición de servicios de información"), la *Application Services Library* (ASL,"Biblioteca de Servicios Aplicativos"), el método de desarrollo de sistemas dinámicos (DSDM, Dynamic Systems Developer Method), el modelo de Capacidad y Madurez[20] (CMM/CMMI) y a menudo se relaciona con la gobernanza de tecnologías de la Información mediante COBIT (Control Objectives for Information and related Technology)[21].

A continuación se introduce sobre los aspectos que considera el BS7799, que se estandarizó como ISO 17799, estándar de seguridad, y como éste ha ido evolucionando: ISO 27001 y 27002.

1.7.3 Estándar de Seguridad de la ISO 17799 - BS 7799

ISO17799, es un estándar detallado de la seguridad. Se ordena en diez secciones o dominios importantes (año 2000), cada una cubre un diverso asunto o área:

i. Hojas de operación (planning) de la Continuidad del Negocio

Los objetivos de esta sección son:

- ✓ Evitar interrupciones a las actividades económicas y a los procesos críticos del negocio, evaluando los efectos de incidentes o de desastres importantes.

[20] El Modelo de Capacidad y Madurez o CMM (Capability Maturity Model), es un modelo de evaluación de los procesos de una organización. Fue desarrollado inicialmente para los procesos relativos al software por la Universidad Carnegie-Mellon para el SEI (Software Engineering Institute)

[21] Control Objectives for Information and related Technology, COBIT, es un conjunto de mejores prácticas para el manejo de información creado por Information System Audit and Control Association, ISACA y IT Governance Institute, ITGI, en 1992.

ii. Control de Acceso del Sistema

Los objetivos de esta sección son:

- ✓ Controlar el acceso a la información
- ✓ Prevenir el acceso desautorizado a los sistemas de información
- ✓ Asegurar la protección de servicios network
- ✓ Prevenir el acceso desautorizado a los computadores.
- ✓ Detectar actividades no autorizadas.
- ✓ Asegurar la información al usar recursos móviles, el computador y servicios de telecomunicaciones de una red

iii. Desarrollo y Mantenimiento del Sistema

Los objetivos de esta sección son:

- ✓ Asegurar la construcción de sistemas operacionales.
- ✓ Prevenir la pérdida, modificación o el uso erróneo de los datos en sistemas o aplicaciones.
- ✓ Proteger el secreto, la autenticidad y la integridad de la información;
- ✓ Asegurar que proyectos y actividades de ayuda se conduzcan de una manera correcta.
- ✓ Mantener la seguridad del software del sistema y de los datos de la aplicación.

iv. Seguridad física y ambiental

Los objetivos de esta sección son:

- ✓ Prevenir el acceso a personas no autorizadas a la información, que pudieran ocasionar daños o interferencia.
- ✓ Prevenir la pérdida o daño en los activos y causaran interrupción a las actividades económicas.
- ✓ Prevenir el hurto recursos con información y un mal tratamiento de ellos.

v. Cumplimiento

Los objetivos de esta sección son:

- ✓ Evitar la ambigüedad de cualquier obligación criminal o civil, estatutos reguladores o contractuales que tengan relación con cualquier requisito de seguridad.
- ✓ Asegurar la conformidad entre sistemas de seguridad y políticas o estándares de la organización. (Como se muestra en la figura 11, debe existir una convergencia de los elementos que se normarán y las

normativas que son aplicables internamente, así como las recomendaciones y mejores prácticas, claro dentro del contexto)

- ✓ Maximizar la eficacia y reducir al mínimo la interferencia externa a los procesos o sistemas.

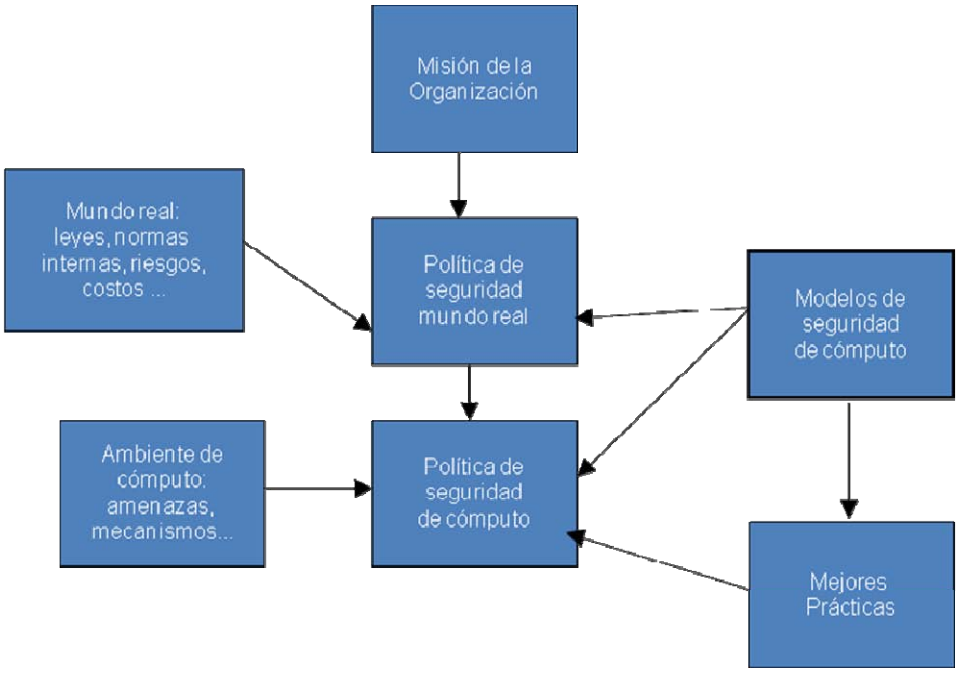

Figura 11 Administración de la seguridad Convergencia Normatividad Mundo Real, Cómputo

Alguno de los controles que ejemplifican claramente este dominio son:

- Los requerimientos regulatorios y contractuales, y el acercamiento de las organizaciones para conocer estos requerimientos deben ser definidos claramente, documentados y mantenerse actualizados para cada sistema de información.
- Se debe disuadir a los usuarios del uso no autorizado de las instalaciones.
- Los requerimientos de auditoría y las actividades de revisión a los sistemas deben ser cuidadosamente planeados, así como minimizar el riesgo de posibles interrupciones en los procesos de negocio.
- El acceso a las herramientas de auditoría de los sistemas de información deben ser protegidos para prevenir cualquier abuso.
- Los gerentes deben asegurarse que todos los procedimientos de seguridad dentro de su área de responsabilidad se llevan acabo correctamente, para lograr el cumplimiento de las políticas y estándares de seguridad.
- Los sistemas de información deben ser revisados periódicamente para el cumplimiento de los estándares de seguridad.

vi. Seguridad del Personal

Los objetivos de esta sección son:

- ✓ Reducir riesgos de error, hurto, fraude o el uso erróneo por parte del recurso humano.
- ✓ Asegurarse de que los operadores estén enterados de amenazas y se preocupen de la seguridad de la información, y que estén equipados para utilizar la política corporativa de seguridad en el curso de su trabajo normal;
- ✓ Reducir al mínimo el daño de incidentes y de mal funcionamiento de la seguridad y aprender de tales incidentes.

vii. Organización de la Seguridad

Los objetivos de esta sección son:

- ✓ Manejar seguridad de la información dentro de la compañía;
- ✓ Mantener la seguridad de los recursos de la organización, del tratamiento de la información y de los activos de la información alcanzados por terceros.
- ✓ Mantener la seguridad de la información cuando el tratamiento de la información ha sido responsabilidad de un outsourcing (organización externa).

viii. . Administración del Procesador y de la Red (Conectividad)

Los objetivos de esta sección son:

- ✓ Asegurar la operación correcta y segura de los recursos que realizan tratamiento de información.
- ✓ Reducir al mínimo el riesgo de fallas de los sistemas;
- ✓ Proteger la integridad lógica del software y de la información;
- ✓ Mantener la integridad, disponibilidad del tratamiento y de la comunicación de la información;
- ✓ Asegurar y salvaguardar la información en redes y la protección de la infraestructura que se utiliza.
- ✓ Prevenir las interrupciones de las actividades económicas y daños a los activos.
- ✓ Prevenir la pérdida, modificación o el uso erróneo de la información intercambiada entre las organizaciones.

ix. Clasificación y control del activo

Los objetivos de esta sección son:

- ✓ Mantener la protección apropiada de activos corporativos y asegurarse de que los activos de la información reciben un nivel apropiado de protección.

x. Política De la Seguridad

Los objetivos de esta sección son:

- ✓ Proporcionar a la dirección o gerencia la ayuda para la seguridad de la información.

1.7.4 PDCA (Plan-Do-Check-Act)

La segunda parte del BS7799 fue publicada en 1999, se conoce como BS 7799 Parte 2, titulada “Sistemas de Administración en la Seguridad de la Información”, enfocada a como implementar Sistemas de Administración en la Seguridad de la Información, ISMS, refiriéndose a la estructura de la administración de la seguridad de la información y a los controles identificados, la más reciente revisión fue en Junio del 2005 y fue base del ISO 27002 en Julio de 2007. Introduciendo el *Plan-Do-Check-Act* (PCDA), esta segunda parte fue adoptada en ISO 27001 en Noviembre del 2005.

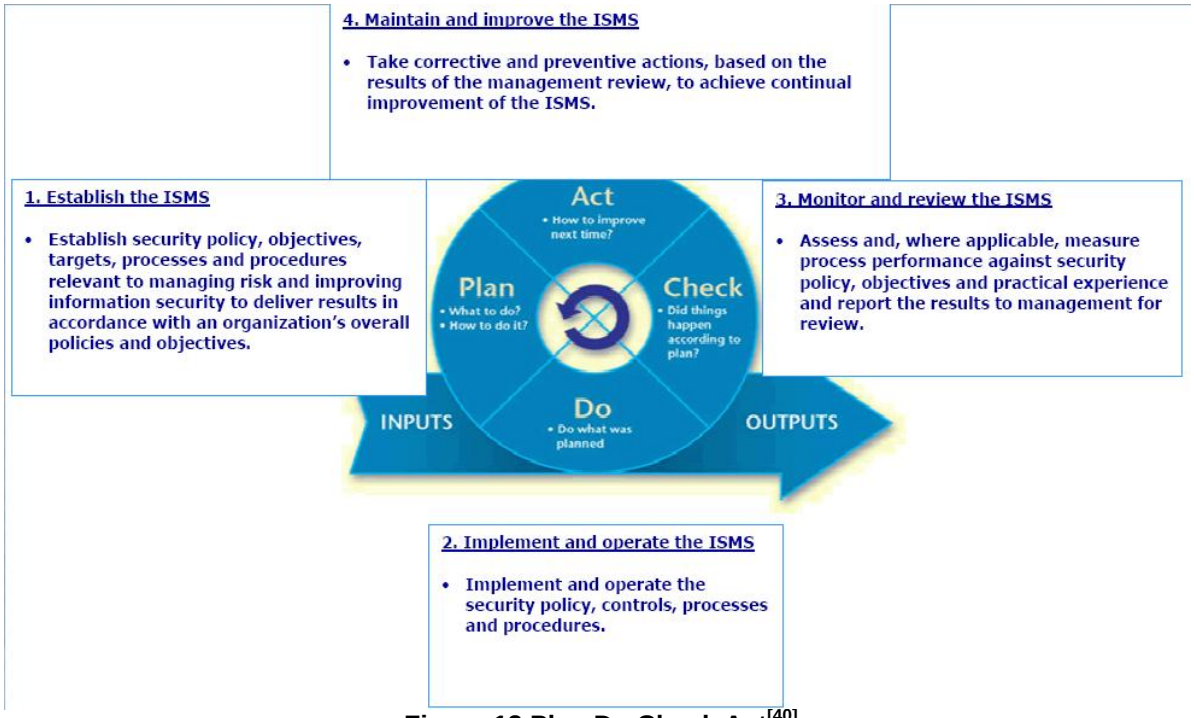

Figura 12 Plan Do Check Act[40]

PDCA (*Plan-Do-Check-Act*) es un proceso iterativo de cuatro pasos para la resolución de problemas, típicamente utilizado en control de calidad. Significa, como se muestra en la figura 11 *Plan Do Check Act*, primeramente, el establecimiento de objetivos y procesos necesarios para la entrega de resultados de acuerdo con las especificaciones.

i. Establecer el ISMS, Sistemas de Administración de la Seguridad de la Información: Establecer las políticas de seguridad, objetivos, metas, procesos y procedimientos relevantes para la administración de riesgos y proporcionando seguridad a la información para la entrega de resultados de acuerdo con las políticas y objetivos globales de la organización.

    a. Define el alcance del ISMS
    b. Define las políticas del ISMS
    c. Define la aproximación sistemática para la valoración del riesgo.
    d. Identifica y valora el riesgo
    e. Identifica y estima las opciones para tratar los riesgos
    f. Prepara el comunicado de aplicabilidad

Posteriormente se lleva a cabo la Implementación de los procesos

ii. Implementación y operación del ISMS, Sistemas de Administración de la Seguridad de la Información: Implementar y llevar a cabo las políticas de seguridad, controles procesos y procedimientos.

    a. Formula el plan para tratar el riesgo
    b. Implementa el plan para tratar el riesgo
    c. Implementa controles
    d. Implementa capacitación y concientización
    e. Controla las operaciones
    f. Controla los recursos
    g. Implementa de una forma reactiva y de detección los controles para los incidentes de seguridad

El tercer paso es la Revisión y evaluación de los procesos y resultados contra los objetivos y especificaciones e informar los resultados

iii. Monitoreo y revisión del ISMS, Sistemas de Administración de la Seguridad de la Información: Los activos y, donde es aplicable, las medidas de rendimiento en los procesos contra las políticas de seguridad, los objetivos y experiencias practicas y los resultados de la revisión a la administración.

    a. Formaliza monitoreando procedimientos y controles

b. Emprende revisiones regulares del ISMS
c. Revisa los riesgos residuales y los riesgos aceptables

El cuarto paso es la aplicación de acciones hacia los resultados para las mejoras necesarias

iv. Mantenimiento y mejora del ISMS, Sistemas de Administración de la Seguridad de la Información: Tomar y prevenir mediante acciones correctivas, basadas en los resultados de la revisión de la administración, a fin de proveer al ISMS de mejoras continuas.

a. Implementa la identificación de mejoras en el ISMS
b. Retroalimentación continua y mejoras
c. Comunicación con las partes interesadas
d. Asegura mejoras a alcanzar concentradas en los resultados

Los requerimientos genéricos a través del PDCA son:

1. La documentación de los requerimientos
2. Administración de las Responsabilidades
3. Administración de las revisiones sobre el ISMS
4. Mejoras en el ISMS

La Segunda Parte del BS7799, ISO27001, contiene 11 secciones o dominios que se describen en el siguiente apartado.

1.7.5 BS7799-2 ISO 27001

El estándar ISO 27001 fue publicado en Octubre del 2005, esencialmente remplaza el viejo estándar BS7799-2. Es la especificación para un ISMS, un Sistemas de Administración en Seguridad de la Información. BS7799 por si mismo fue desde hace mucho tiempo un estándar, primeramente publicado en los noventas como un código de práctica. Como este maduró, una segunda parte surgió para cubrir la administración de sistemas.

El ISO 27001 realza el contenido del BS7799-2 y armoniza junto con otros estándares. El contenido del estándar en si mismo es proveer un modelo estableciendo, implementando, operando, monitoreando, revisando, manteniendo y mejorando el Sistema de Administración en Seguridad de la Información. Considerando lo anterior, esto debe ser una decisión estratégica. Más lejos, el diseño e implementación del ISMS de una organización esta influenciado por aquellas necesidades y objetivos, requerimientos de seguridad, el proceso empleado y el tamaño y estructura de la organización.

El estándar define su enfoque de proceso como la aplicación de un sistema de procesos con una organización, junto con la identificación e interacción de estos procesos, y su administración.

ISO 27001 define mejores prácticas para la administración de la seguridad de la información, la administración debe administrarse en un balance físico, técnico, procedimental y del personal de seguridad. Se divide en 11 dominios:

Política de la Seguridad, encargada de la documentación de políticas, revisión y evaluación. **Organización de la Seguridad de la Información**, encargada de la infraestructura de seguridad de la información y seguridad de los accesos por terceras partes. **Administración de Activos**, se encarga de la responsabilidad de los activos y clasificación de la información. **Seguridad de los Recursos Humanos**, se encarga de la definición de la seguridad en el trabajo, capacitación de los usuarios, respuesta a incidentes y malos funcionamientos. **Seguridad Física y Ambiental**, se encarga de asegurar las áreas, del equipamiento en seguridad y controles generales. **Administración de las Comunicaciones y Operaciones**, se encarga de los procedimientos operacionales, de la planeación y aprobación de sistemas, la protección contra software malicioso, la administración de la red, el manejo de medios y el intercambio de información y software. **Control de Acceso**, en base a los requerimientos del negocio, además de encargarse de la administración de los accesos de los usuarios, responsabilidad de estos, control de acceso a la red, control de acceso en los sistemas operativos, la aplicación de los controles de acceso, el monitoreo de los sistemas de acceso y del equipo de cómputo móvil. **Adquisición, desarrollo y mantenimiento de los Sistemas de Información**, se enfoca en los requerimientos de seguridad, la seguridad en las aplicaciones, controles criptográficos, seguridad de los sistemas de archivos, seguridad en el desarrollo y soporte de los procesos. **Administración de la Continuidad del Negocio,** mediante el análisis y la administración de riesgos para garantizar que una organización pueda continuar operando a un nivel mínimo predeterminado. La gestión de la continuidad del negocio (BCM) reduce riesgos y desarrolla planes para restaurar las actividades del negocio si son interrumpidas por un desastre. **Conformidad**, en base a los requerimientos legales, revisión de políticas de seguridad y conformidad en las tecnologías, además de las consideraciones de los sistemas de auditoria. **Administración de Incidentes en los sistemas de Información**, mediante la elaboración de reportes de incidentes y vulnerabilidades, administración de incidentes y mejoras.

Este capítulo se concreto en introducir los conceptos relacionados a la seguridad de la información, la problemática relacionada al tratamiento de la información asociada a las TI en la actualidad, así como también, las tecnologías utilizadas para transformar datos, no necesariamente relacionadas con computadoras, y que no excluye a las demás tecnologías, como las desarrolladas por animales.

La evolución tecnológica ha incrementado la problemática en seguridad, debido a esto, se han desarrollado, buenas prácticas, estándares, marcos de referencia, etc. para la Administración de la Seguridad y de las Tecnologías de Información.

En el siguiente capítulo se desarrolla una metodología para analizar y administrar los riesgos inherentes al tratamiento de la información mediante la utilización de la infraestructura tecnológica y de la cual dependen los servicios que brindan las organizaciones, con la finalidad de cumplir los objetivos que sustentan la misión de la organización.

Referencias Capítulo 1

[1] *D'Ambrosio Sergio*."**El concepto de Datos I.U.P"**. -Santiago Mariño-. Puerto Ordaz. Disponible en: http://www.monografias.com/trabajos14/datos/datos.shtml leído el 25 Agosto 2007.

[2] *L.I. Genny E. Góngora Cuevas*, *M.A*. **"Tecnología de la información como herramienta para aumentar la productividad de una empresa.¿qué es la Tecnología de la información?"** Disponible en: http://www.tuobra.unam.mx/publicadas/040702105342-__191_Qu.html leído el 25 Agosto 2007.

[3]*Wikipedia La Enciclopedía libre*. "**Información"**. Disponible en: http://es.wikipedia.org/wiki/Informaci%C3%B3n leído el 25 de Agosto 2007.

[4]*L.I. Genny E. Góngora Cuevas, M.A.* **"Tecnología de la información como herramienta para aumentar la productividad de una empresa.¿qué es la Técnología de la información?"** Disponible en: http://www.tuobra.unam.mx/publicadas/040702105342-__191_Qu.html leído el 25 Agosto 2007.

[5]*Passig Villanueva.* "**Los Sistemas de memoria"**. Revista de Psicología – Vol. V Años 1994-1995, p.27. Depto. Fisiología y Biofísica, Facultad de Medicina, Universidad de Chile. Disponible en: http://csociales.uchile.cl/publicaciones/psicologia/docs/Los_sistemas_de_memoria.pdf Leido el 30 Agosto 2007.

[6]*Wikipedia la Enciclopedía libre*. **"Pareidolia"**. Disponible en: http://es.wikipedia.org/wiki/Pareidolia Leído el 31 Agosto 2007.

[7]*Encyclopedia of Mental Disorders :: Py-Z*. **"Rorschach technique"**. Imágen disponible en: http://www.minddisorders.com/images/gemd_02_img0090.jpg Leído el 31 Agosto 2007.

[8] *"profelegui" Adrian*. "**Tecnología de la información y la comunicación. Breve Historia de la Comunicación en Tecnología de la información y la comunicación."** Disponible en: http://www.geomundos.com/tecnologia/profelegui/breve-historia-de-la-comunicacion_doc_7096.html Leído el 26 Agosto 2007.

[9]*Wikipedia la Enciclopedía libre.* "**Informática"**. Disponible en: http://es.wikipedia.org/wiki/Inform%C3%A1tica Leído el 31 Agosto 2007.

[10]*Mike Friedman, L. Wlosinski.* "**Integrating Security into the Systems Development Life Cycle (SDLC)".** Center for Information Thechnology Officer Mayo 22, 2003 Slide 10.

[11]*Revista Muy Interesnate*. "**Éxitos medievales"** p.18 Septiembre 2007.

[12]*Hernández Leobardo y E. Daltabuit* 2006. "**Manejo de la Información"** p.8 En el módulo 4: Seguridad Informática, del Diplomado de Tecnologías de Información, Centro Educativo Multidisciplinario Polanco, México, D.F. 30 Junio-14 Julio 2006. centro Educativo Multidisciplinario Polanco, México, D.F.

[13]*Hernández Leobardo y E. Daltabuit* 2006. "**Servicios y Mecanismos de Seguridad"** p. 45 En el módulo 4: Seguridad Informática, del Diplomado de Tecnologías de Información, Centro Educativo Multidisciplinario Polanco, México, D.F 30 Junio-14 Julio 2006. Centro Educativo Multidisciplinario Polanco, México, D.F.

[14]*IPCITEC- Instituto Politécnico de Ciencia y Tecnología*. "**Sistemas de cómputo ¿Qué es un sistema de cómputo?"** .Disponible en: http://www.ipcitec.freeservers.com/sistemas.html Leído el 6 Septiembre 2007.

[15]*IPCITEC- Instituto Politécnico de Ciencia y Tecnología*. **"Sistemas de cómputo ¿Qué es un sistema de cómputo?"** .Disponible en: http://www.ipcitec.freeservers.com/sistemas.html Leído el 6 Septiembre 2007.

[16]*Airala, Altmark, Bel, Pérez, Seguel, Tiscornia, Masoero, Nunes, Passarello. Instituto Argentino de Normalización*. **"Esquema 1 de Norma IRAM-ISO IEC 17799. Tecnología de la Información. Código de práctica para la administración de la seguridad de la Información"**. p 9. Año 2002

[17] *Charles P. Pfleeger, Shari Lawrence Pfleeger*. **"Security in Computing. Third Edition in the Chapter 1. Is There a Security Problem in Computing? Section 1.2 Attacks"**. Electronic Book. Printed in the United States of America Pub. December 02, 2002. Prentice Hall.

[18] *Charles P. Pfleeger, Shari Lawrence Pfleeger*. **"Security in Computing. Third Edition in the Chapter 1. Is There a Security Problem in Computing? Section 1.2 Attacks"**. Electronic Book. Printed in the United States of America Pub. December 02, 2002. Prentice Hall.

[19] *Wikipedia Enciclopedia libre.* "**Riesgo. Riesgo vs. Amenaza"** Disponible en: http://es.wikipedia.org/wiki/Riesgo Leído el 8 Septiembre 2007.
"Los Desastres naturales". Disponible en: Portal Planeta Sedna http://www.portalplanetasedna.com.ar/desastres01.htm Leído el 8 Septiembre 2007.

[20] *Charles P. Pfleeger, Shari Lawrence Pfleeger*. **"Security in Computing. Third Edition in the Chapter 1. Is There a Security Problem in Computing? Section 1.2 Attacks"**. Electronic Book. Printed in the United States of America Pub. December 02, 2002. Prentice Hall.

[21] *Hernández Leobardo y e. Daltabuit* 2004. **"Introducción a la Seguridad de la Información"** p 48. En el módulo 1: **"Problemática y Definición de la Seguridad Informática"**, del Diplomado de Seguridad Informática, Centro Educativo Multidisciplinario Polanco, México, D.F. 4-13 de octubre 2004. Centro Educativo Multidisciplinario Polanco, México, D.F.

[22] *Hernández Leobardo y e. Daltabuit* 2004. **"Introducción a la Seguridad de la Información"** p 48. En el módulo 1: **"Problemática y Definición de la Seguridad Informática"**, del Diplomado de Seguridad Informática, Centro Educativo Multidisciplinario Polanco, México, D.F. 4-13 de octubre 2004. Centro Educativo Multidisciplinario Polanco, México, D.F.

[23] *Solano Ronald*. **"Teoría de Sistemas. Características de los sistemas."** Disponible en: http://www.monografias.com/trabajos11/teosis/teosis.shtml Leído el 7 Septiembre 2007.

[24]*Quint Wellington Redwood Academy 0202C1. BMC Software.* Imagen tomada de: **"Gestión de Servicios Fundamentos"**. Slide 12. 2002.

[25]*Solano Ronald.* **"Teoría de Sistemas. Características de los sistemas".** Disponible en: http://www.monografias.com/trabajos11/teosis/teosis.shtml Leído el 7 Septiembre 2007.

[26] *Wikipedia La Enciclopedía libre*. **"Teoría de Sistemas. Entropía y neguentropía"**. Disponible en: http://es.wikipedia.org/wiki/Teor%C3%ADa_de_sistemas Leído el 31 Agosto 2007.

[27]*Wikipedia La Enciclopedía libre.* **"Teoría de Sistemas. Entropia y neguentropía"**. Disponible en: http://es.wikipedia.org/wiki/Entrop%C3%ADa_(termodin%C3%A1mica) Leído el 31 Agosto 2007.

[28]*Martínez Bustamante Sandra.* **"La termodinamica y el concepto de entropía".** La Segunda Ley. Disponible en: http://www.monografias.com/trabajos/termoyentropia/termoyentropia.shtml?interlink Leído el 7 Septiembre 2007.

[29]*Mariane Swanson, Amy Whol, Lucinda Pope, Tim Grance, Johan Hash, Ray Thomas.* **"NIST Special publication 800-34.Contingency Planning Guide for Information technology Systems"** p4. Recommendations of the National Institute of standars and Technology . Technology Administration U.S. Departament of Commerce June 2002. Printed in Washington, DC20402-0001

[30]*Hernández Leobardo y E. Daltabuit* 2004. "**Introducción a la Seguridad de la Información"** p 55. En el módulo 1: **"Problemática y Definición de la Seguridad Informática"**, del Diplomado de Seguridad Informática, Centro Educativo Multidisciplinario Polanco, México, D.F. 4-13 de octubre 2004. Centro Educativo Multidisciplinario Polanco, México, D.F.

[31]*Hernández Leobardo y E. Daltabuit* 2004. "**Introducción a la Seguridad de la Información"** p 55. En el módulo 1: **"Problemática y Definición de la Seguridad Informática"**, del Diplomado de Seguridad Informática, Centro Educativo Multidisciplinario Polanco, México, D.F. 4-13 de octubre 2004. Centro Educativo Multidisciplinario Polanco, México, D.F.

[32]*Hernández Leobardo y E. Daltabuit* 2004. "**Introducción a la Seguridad de la Información"** p 55. En el módulo 1: **"Problemática y Definición de la Seguridad Informática"**, del Diplomado de Seguridad Informática, Centro Educativo Multidisciplinario Polanco, México, D.F. 4-13 de octubre 2004. Centro Educativo Multidisciplinario Polanco, México, D.F.

[33]*Hernández Leobardo y E. Daltabuit* 2004. **"Introducción a la Seguridad de la Información"**, p.64. En el módulo 1: **"Problemática y Definición de la Seguridad Informática"**, del Diplomado de Seguridad Informática, Centro Educativo Multidisciplinario Polanco, México, D.F. 4-13 de octubre 2004. Centro Educativo Multidisciplinario Polanco, México, D.F.

[34]*Hernández Leobardo y E. Daltabuit* 2004. **"Introducción a la Seguridad de la Información"**, p.64. En el módulo 1: **"Problemática y Definición de la Seguridad Informática"**, del Diplomado de Seguridad Informática, Centro Educativo Multidisciplinario Polanco, México, D.F. 4-13 de octubre 2004. Centro Educativo Multidisciplinario Polanco, México, D.F.

[35]*Hernández Leobardo y E. Daltabuit* 2004. **"Introducción a la Seguridad de la Información"**, p.62-63. En el módulo 1: **"Problemática y Definición de la Seguridad Informática"**, del Diplomado de Seguridad Informática, Centro Educativo Multidisciplinario Polanco, México, D.F. 4-13 de octubre 2004. Centro Educativo Multidisciplinario Polanco, México, D.F.

[36]*An introduction to Computer Security: The NIST Handbook.* **"Special Publication 800-12"** p.73 National Institute of Standards and Technology Administration U.S Departament Commerce.

[37]*Mariane Swanson, Amy Wohl, Lucinda Pope, Tim Grance, Joan Hash, Ray Thomas.* **"Contingency Planning Guide for Information Technology Systems Recommendations for the National Institude of Standards and Technology"** p.12 Image of the **"System Developed Life Cycle"**.

[38]*Wan Lee*. **"Security Life Cycle- 1.DIY Assesment"** Noviembre 13, 2001 p. 1 SANS Institute Image of Security Life Cycle.

[39]*Hernández Leobardo y E. Daltabuit* 2004. **"Introducción a la Seguridad de la Información"**, p.5. En el módulo 1: **"Problemática y Definición de la Seguridad Informática"**, del Diplomado de

Seguridad Informática, Centro Educativo Multidisciplinario Polanco, México, D.F. 4-13 de octubre 2004. Centro Educativo Multidisciplinario Polanco, México, D.F.

Capítulo
2
Análisis y Administración de Riesgos

Resumen

Un proceso efectivo de la administración de Riesgos es un importante componente para el éxito del programa de seguridad en TI. El objetivo principal del proceso de administración de Riesgos de una organización debe ser proteger a la misma y la capacidad de ésta para llevar a cabo la misión de la organización no sólo enfocada en los activos de TI. Por lo tanto el proceso de administración de Riesgos no debe ser tratado, primeramente, como una función técnica encargada al o los expertos que operan y administran los sistemas de TI, sino como un componente esencial de las funciones de la administración de la organización.

El riesgo es el impacto negativo neto del ejercicio de una vulnerabilidad, en vista de ambos; la probabilidad y el impacto de ocurrencia. La administración de riesgos es el proceso de identificar, determinar y tomar medidas para reducir el riesgo a un nivel aceptable.

El impacto es la consecuencia que se da sobre un activo, proceso de negocio, en cuanto a la disminución de los objetivos y la entrega de los servicios por la materialización de una amenaza.

La Administración de riesgos es el proceso que permite que los encargados de las TI balanceen los costos operacionales y económicos de medidas protectoras, para alcanzar aumentos en las capacidades de la misión mediante la protección de los sistemas de TI y los datos que soportan, para la realización de la misión de la organización. Este proceso, de administración de riesgos, no es único al ambiente de las TI influyen profundamente sobre la toma de decisiones en todas las áreas, es claro que la administración de riesgos se encuentra en la vida cotidiana. Por ejemplo el caso de la seguridad casera.

Mucha gente decide adquirir sistemas de seguridad casera instalados por un proveedor de servicios que mantiene una revisión para otorgar protección mediante un pago mensual al proveedor. La decisión se basó, probablemente, en la necesidad de asegurar, por los dueños de una casa, las mercancías de la misma y fundamentalmente el bienestar de su familia; sopesándolo contra el costo de instalación del sistema de seguridad y la inspección que se realiza, la decisión se fundamento en las necesidades a cubrir para lograr su objetivo, es decir, la misión.

La administración de Riesgos abarca tres procesos: cálculo del riesgo, mitigación del riesgo y; evaluación y valoración.

La cabeza de una unidad organizacional debe asegurarse de que la organización tenga las capacidades necesarias para lograr su misión. Los propietarios de la misión deben determinar las capacidades de seguridad que sus sistemas de TI deben tener para proveer niveles deseados que sustenten la misión frente a las amenazas del mundo real. La mayoría de las organizaciones tienen un presupuesto justo, en cuanto a la seguridad de las TI se refiere; el gasto en seguridad de las TI debe ser revisado a fondo, de la misma forma que las otras decisiones administrativas. Una metodología

bien estructurada de la administración de riesgos, cuando es utilizada efectivamente, puede ayudar a la gestión en la identificación de controles apropiados para otorgar las capacidades en seguridad esenciales para llevar acabo la misión.

2 Análisis y Administración de Riesgos

Cabe mencionar que existe un gran número de metodologías para la realización, primeramente, del análisis de riesgos, mediante un análisis cuantitativo que esta enfocado a determinar valores numéricos (generalmente monetarios) a los componentes objeto de análisis, así también como el establecimiento de valores numéricos de las posibles pérdidas los resultados obtenidos de dicho análisis son objetivos y están basados en métricas generadas igualmente de forma objetiva. Éstos se expresan en porcentajes de probabilidades de ocurrencia de amenazas, pesos, entre otros, la utilización de este tipo de análisis permite mostrar de una manera más sencilla, a la alta dirección los costos, reflejo de la aplicación de los controles necesarios para lograr las metas en la mitigación del riesgo, debido a su expresión basada en un enfoque costo-beneficio y no en términos técnicos. La desventaja de la utilización de este tipo de análisis resulta ser compleja y el trabajo previo al análisis requiere una inversión considerable en tiempo y esfuerzo.

Por otra parte, el análisis cualitativo, no requiere determinar valores numéricos a los componentes objeto de análisis, así también los niveles de posibles pérdidas son expresados de forma cualitativa, metodología expuesta a lo largo de este capítulo. La ventaja de este análisis es que no es necesario contar con la frecuencia de la ocurrencia de cada de una de las amenazas[1], aunque los resultados son subjetivos, los cálculos son más sencillos y llevar acabo este análisis toma un menor tiempo y esfuerzo, la calidad del análisis en comparación con el cuantitativo va en función del grupo de trabajo que se conforme debido a que la obtención de la información que sustentará el análisis se basará en la información recabada como se explica a lo largo de este capítulo y esta se realiza mediante la interacción con los expertos de cada una de las áreas.

Entiéndase por expertos como todos aquellos que nutrirán el análisis mediante la experiencia adquirida de una herramienta, de un proceso, etc. todos éstos con un objetivo común sustentar la misión de la organización.

En la aplicación de un análisis de Riegos es importante conocer la historia de los hechos que tuvieron cierto impacto sobre la organización aunque puede ocurrir que no haya un antecedente en el cual se puedan basar los analistas de riesgos, para este caso es necesario entonces recurrir a información de otros organismos que se encargan de mostrar las perdidas monetarias y los ataques, vulnerabilidades o amenazas ocurridas, uno de estos organismos es Computer Crime and Security

[1] Las definiciones de amenaza, ataque, riesgo, entre otros se explican de manera escueta en el glosario de términos y de una forma más especifica en el capítulo 1 en el apartado Seguridad de la Información

Survey que cada año realiza un informe, del dominio público. En la siguiente figura se muestra una de las gráficas que ostenta información sobre los tipos de ataques detectados a lo largo de 12 meses, correspondientes al año 2007.

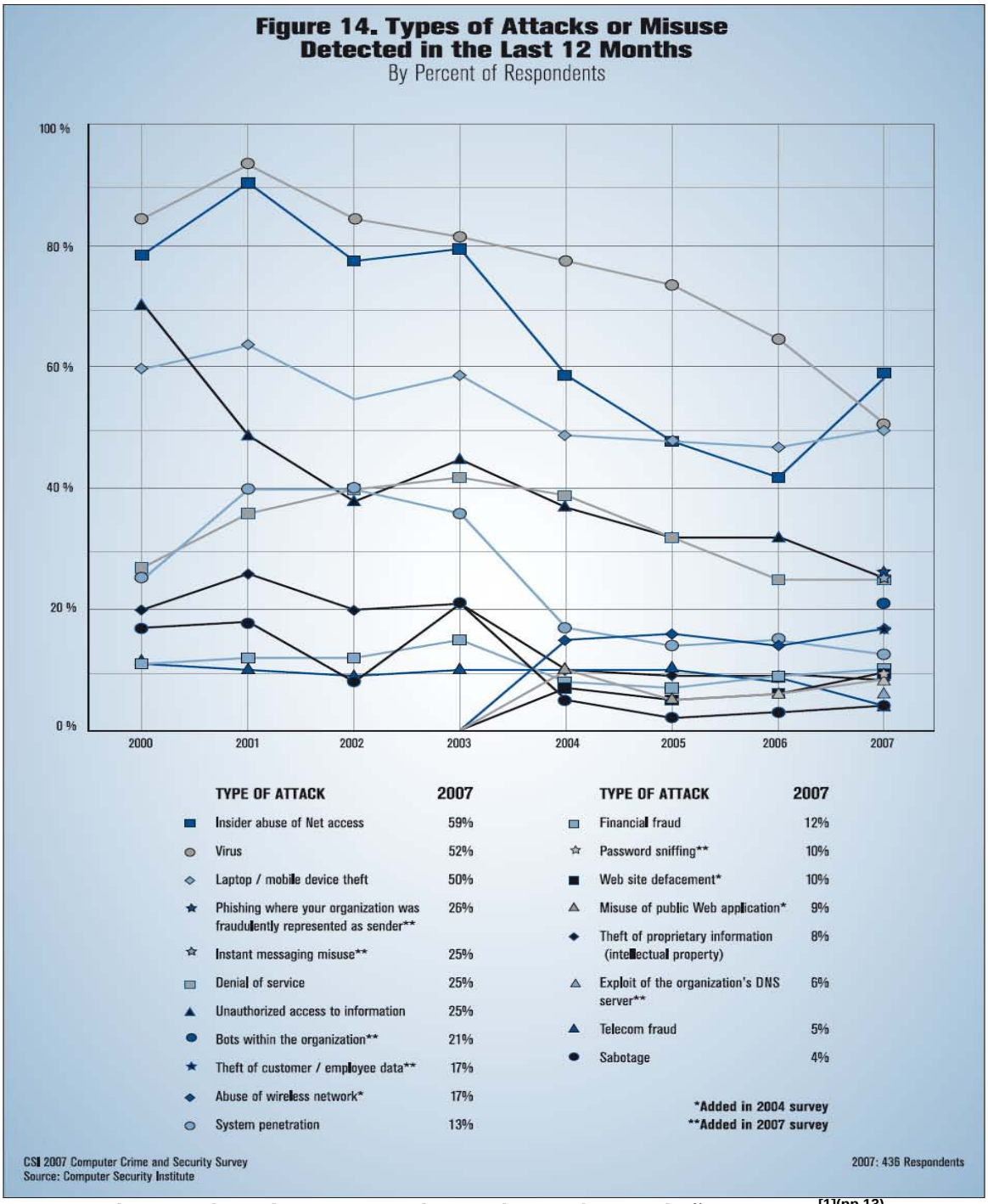

Figura 1 Tipos de ataques o abusos detectados en el año 2007 CSI[1](pp.13)

Otro de los aspectos significativos de los datos reportados por el CSI es la gráfica de costos, en la siguiente figura, Costo de los ataques CSI 2007, se muestran a los dolores que asciende cada tipo de ataque.

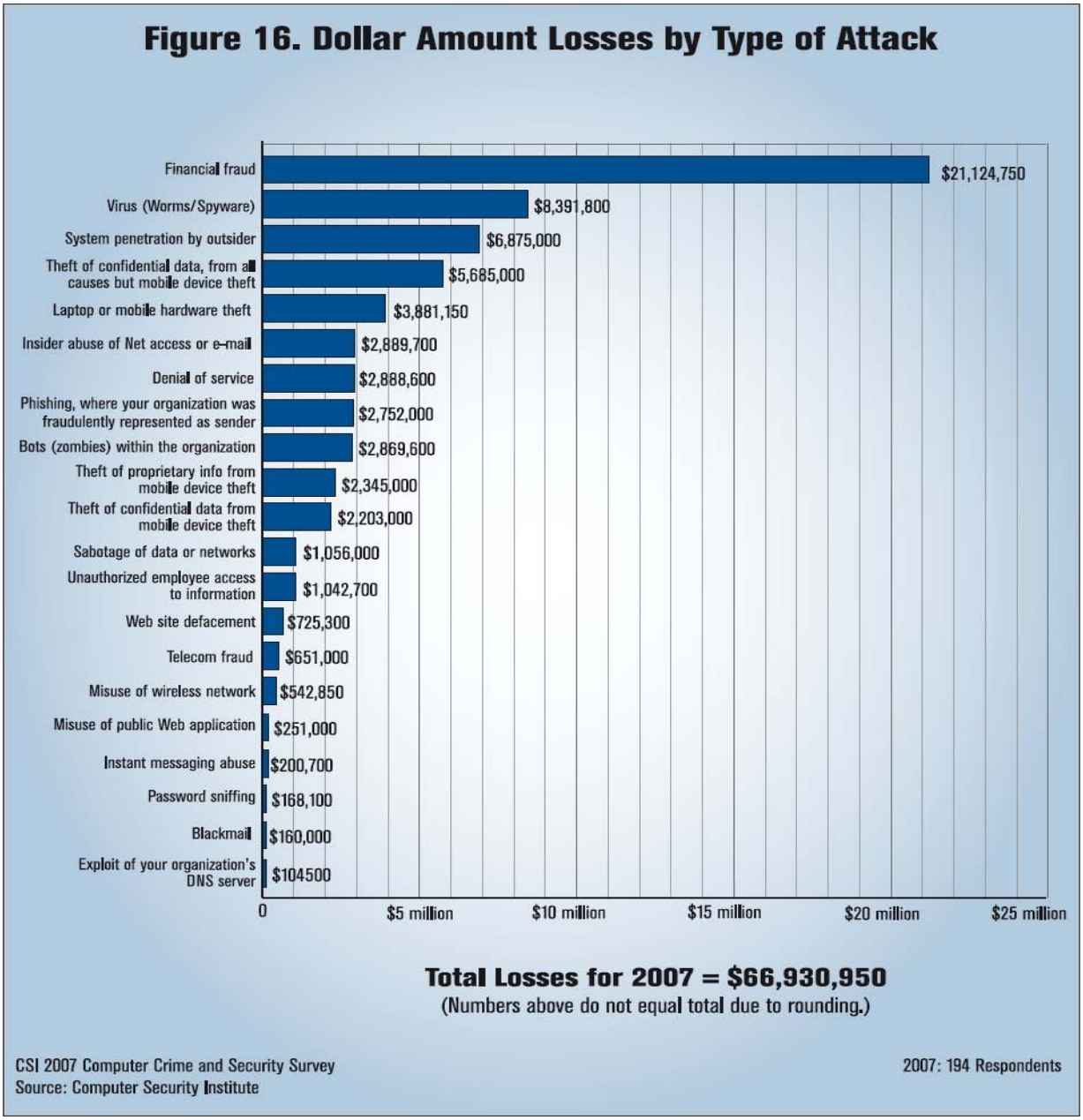

Figura 2 Costos de los Ataques CSI 2007[2](pp.15)

A continuación se explica como se integra el análisis de Riesgos dentro del SDLC (Ciclo de vida del Desarrollo de un Sistema) visto en el capítulo anterior[2], y como se

[2] Véase el apartado Ciclo de Vida del Desarrollo de un Sistema-SDLC (System Developement Life Cycle), en el capítulo 1

relaciona con la metodología de Análisis y Administración de riesgos, que debe de llevarse acabo en el interior de una organización para cubrir las necesidades de seguridad sin entorpecer la misión de la organización, si no otorgándole valor a la misma.

2.1. Integración del Análisis de Riesgos Dentro del SDLC

Minimizando el impacto negativo en la organización y la necesidad de una sólida base en la toma de decisiones son las razones primordiales de las organizaciones para implementar el proceso de administración de riesgos, para sus sistemas de TI. Una efectiva administración de Riesgos debe ser totalmente integrada dentro del SDLC.

El SDLC de un sistema de TI tiene cinco fases, como se explicó con anterioridad, son: inicio, desarrollo o adquisición, implementación, operación o mantenimiento, y disposición. En algunos casos, un sistema de TI puede ocupar varias de estas fases al mismo tiempo. Sin embargo, la metodología de análisis de riesgos es la misma, independientemente de la fase del SDLC por la cual la evaluación se está llevando acabo. La Administración de Riesgos es un proceso iterativo que puede realizarse durante cada una de las principales fases del SDLC.

Fases del SDLC	Características	El apoyo de las actividades del Análisis de Riesgos
Fase 1 Inicio	Las necesidades para un sistema de TI es expresado y el propósito y alcance del sistema de TI es documentado	Identificados los riesgos ,son usados para apoyar el desarrollo de los requerimientos del sistema, incluyendo requerimientos de seguridad, y un concepto de la seguridad de las operaciones (estrategia)
Fase 2 Desarrollo o Adquisición	El sistema de TI es diseñado, comprado, programado, desarrollado, o construido de alguna otra forma.	El riesgo identificado, durante esta fase, puede ser usado para apoyar el análisis de seguridad de el sistema de TI, que puede guiar hacia una arquitectura y diseño equilibrados durante el desarrollo del sistema
Fase 3 Implementación	Las características de seguridad del sistema deben configurarse, habilitarse, probarse y verificarse.	El proceso de Administración de riesgos apoya la evaluación en la implementación del sistema, basándose en sus requerimientos y dentro del ambiente de modelado operacional. Las decisiones de los riesgos identificados deben ser hechas previa la operación del sistema.
Fase 4 Operación y Mantenimiento	El sistema lleva a cabo las funciones. Típicamente el sistema se esta modificando en forma permanente a través de la incorporación de *hardware, software*, y por los cambios en los procesos organizacionales, políticas y procedimientos	Las actividades de la administración de Riesgos son realizadas por reautorizaciones periódicas en el sistema (o reacreaditación) o cuando se hacen cambios importantes a un sistema de TI en su funcionamiento, ambiente productivo (por ejemplo un nuevos sistema de interfaces)

Fases del SDLC	Características	El apoyo de las actividades del Análisis de Riesgos
Fase 5 Disposición	Esta fase puede involucrar la disposición de información, *hardware* y *software*. Las actividades pueden incluir el descarte y destrucción de información, así como el movimiento y el archivo de la misma.	Las actividades de administración de riesgos son realizadas sobre los componentes del sistema que serán dispuestos o remplazados para asegurar que el *hardware* y el *software* son dispuestos apropiadamente, que los datos residuales son correctamente manejados, y que la migración de un sistema se conducirá en una manera segura y sistemática.
Tabla 1 Las Fases del SDLC y su relación con el análisis de Riesgos		

2.2. Planes de Contingencia

Los sistemas de TI son vulnerables a una gran variedad de interrupciones, desde las poco severas (por ejemplo, interrupción de la energía, falla en el disco duro) a severas (por ejemplo destrucción del equipo, fuego), de una gran variedad de fuentes tales como desastres naturales hasta acciones terroristas.

Mientras que muchas de las vulnerabilidades pueden ser reducidas al mínimo o eliminadas con técnicas, gestión, o soluciones operacionales como parte del esfuerzo de la administración de riesgos, es virtualmente imposible eliminar totalmente todos los riesgos. En muchos casos los recursos críticos pueden residir fuera del control de la organización (tal como la energía eléctrica o telecomunicaciones), y la organización puede no asegurar su disponibilidad. De esta manera el plan de contingencia efectivo, en cuanto a su ejecución y prueba, son esenciales para atenuar el riesgo de perder la disponibilidad del sistema y el servicio. Por consiguiente para que el plan de contingencias tenga éxito debe asegurar lo siguiente:

i. Entender el proceso del Plan de Contingencia en las TI y el lugar dentro de la continuidad del plan de operaciones, y del plan de continuidad del Negocio

ii. Desarrollar o reexaminar la política de contingencias y la planeación de procesos, además de la aplicación de los elementos del ciclo de planeación, que incluye un planteamiento preliminar, análisis de impacto al negocio, selección del sitio alterno y la estrategia de recuperación.

iii. Desarrollar o re examinar las políticas propias de los planes de contingencia con énfasis en mantener, capacitar y ejercitar el plan de contingencia.

La administración de riesgos abarca una gran gama de actividades, para identificar, controlar y atenuar riesgos en los sistemas de TI. Las actividades de la administración de riesgos hacia la perspectiva de un **plan de contingencia** en las TI tienen dos funciones primarias.

En primer lugar, la administración de riesgos debe identificar amenazas y vulnerabilidades para poder establecer controles adecuados, previniendo que los

incidentes sucedan o limitando los efectos del mismo. Estos controles de seguridad protegen a los sistemas de TI contra tres clasificaciones de amenazas.

Las Naturales como huracanes, las humanas (respuesta a ataques informáticos, como denegación de servicios, virus, entre otros; que involucran actividades fuera del alcance del plan de contingencia de las TI, como las actividades asociadas con la preservación de evidencia, mediante el análisis del computo forense siguiendo una intrusión ilegal, un ataque de denegación de servicios o otro delito informático) y las ambientales como falla del equipo, errores de *software* y fallas de energía eléctrica.

En segundo lugar, la administración de riesgos debe identificar riesgos residuales para los cuales los planes de contingencia se deben aplicar. Un plan de contingencia, por lo tanto, se vincula estrechamente a los resultados del cálculo del riesgo y del proceso de mitigación. La relación entre identificar y poner controles de seguridad en ejecución, desarrollar y mantener el plan de contingencia, y poner el plan de contingencia en ejecución una vez que haya ocurrido el acontecimiento, son los elementos del proceso de administración de riesgos y los planes de contingencia.

Como los riesgos pueden variar en un cierto plazo y los nuevos riesgos pueden sustituir a los antiguos mientras se desarrolla un sistema, el proceso de la gestión de riesgos debe ser progresivo y dinámico. La persona responsable de los planes de contingencia en las TI debe estar al tanto de los riesgos hacia el sistema y reconocer si el plan de contingencia actual puede tratar totalmente los riesgos residuales y la eficacia de este plan.

2.3. Evaluación de Riesgos

La evaluación de riesgos es el primer proceso en la metodología de la Administración de Riesgos. Las Organizaciones usan la evaluación de riesgos para determinar el alcance potencial de la amenaza y el riesgo asociado con los sistemas de TI durante todo el SDLC (*System Developer Life Cycle*). El resultado de este proceso ayudará a identificar controles de manera apropiada, para la reducción o eliminación del riesgo durante el proceso de mitigación.

"*El Riesgo es una función de la probabilidad de origen de una amenaza determinada ejerciendo un potencial especifico de la vulnerabilidad y las repercusiones resultantes de este acontecimiento adverso en la organización*" [3] (pp. 8)

Para determinar la probabilidad de un evento adverso futuro, las amenazas para un sistema de TI deben ser examinadas en conjunto con las vulnerabilidades potenciales y los controles internos para los sistemas de TI. El impacto se refiere a la magnitud del daño por el ejercicio de una amenaza, que puede ser provocado por una vulnerabilidad. El nivel del impacto es regido por los impactos posibles a la misión y a su vez produce una relativa valoración para los activos de TI y los recursos afectados (por ejemplo la criticidad y sensitividad de los componentes de un sistema de TI y los datos). La metodología de evaluación de riesgos abarca nueve pasos: Determinación de los atributos peculiares del sistema, Identificación de Amenazas y

Vulnerabilidades, Análisis de los Métodos de Control, Determinación de la probabilidad, Análisis del Impacto, Determinación del riesgo, Recomendación de controles y la documentación de resultados.

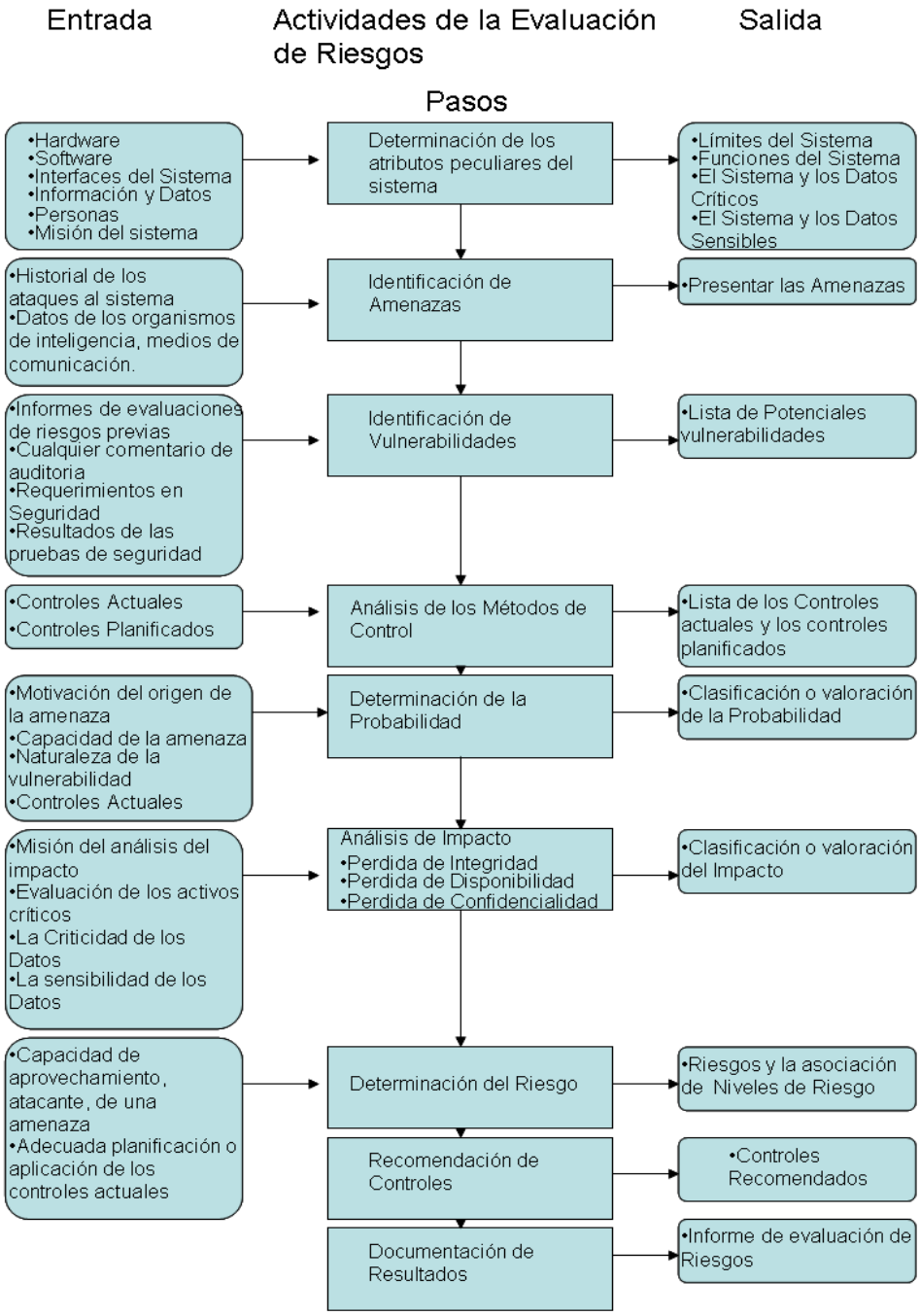

Figura 3 Esquema organizacional de la Metodología de Evaluación de Riesgos.
Cabe mencionar que los pasos de identificación de amenazas, identificación de vulnerabilidades y el Análisis de impacto pueden realizarse de forma paralela

2.3.1. Determinación de los Atributos Peculiares en un Sistema

En la evaluación de riesgos para un sistema de TI, el primer paso es definir el **alcance del esfuerzo**. En este paso las fronteras del sistema de TI son definidas junto con los recursos y la información que constituye al sistema. La determinación de los atributos peculiares en un sistema establecerán el alcance del esfuerzo en la evaluación de riesgos delimitando la autorización operacional (o acreditación) y proveyendo información (por ejemplo *hardware, software*, sistemas de conectividad, la división de responsabilidad o el personal de apoyo) fundamental para definir el riesgo. Para el caso de múltiples sistemas interrelacionados, es importante que los dominios de interés, y todas las interfaces y dependencias sean definidos antes de aplicar la metodología de Administración de Riesgos.

La identificación de riesgos para un sistema de TI requiere un entendimiento profundo del ambiente de procesamiento del sistema La persona o personas quienes conducen la evaluación de riesgos debe por lo tanto primero recolectar **información relativa al sistema** la cual es clasificada como sigue:

- ✓ *Hardware*
- ✓ *Software*
- ✓ Interfaces del sistema (ejemplo internos y conectividad externa)
- ✓ Datos e Información
- ✓ Personas quienes dan soporte y usan el sistema de TI
- ✓ Misión del sistema (ejemplo los valores del sistema o la importancia de estos para la organización).
- ✓ Datos y sistemas **Sensitivos**, el nivel de protección sensitivo se refiere al nivel que requiere una protección caracterizada por mantener el sistema y la integridad, confidencialidad, y disponibilidad de los datos.

Adicionalmente la información relacionada con el ambiente operacional de los sistemas de TI y los datos se incluye, pero no se limitan, a lo siguiente:

- ✓ Los requerimientos funcionales del sistema de TI.
- ✓ Usuarios del sistema (por ejemplo usuarios que proveen soporte técnico para los sistemas de TI, usuarios de aplicaciones quienes utilizan el sistema de TI para realizar funciones del negocio).
- ✓ Políticas de seguridad que rigen al sistema de TI (políticas organizacionales, requerimientos federales, leyes, prácticas industriales).
- ✓ Arquitectura de seguridad del sistema.

- ✓ Topología actual de la Red (ejemplo diagrama de red).
- ✓ Protección de almacenamiento de información que resguarde el sistema y la disponibilidad, confidencialidad, e integridad de los datos.
- ✓ Flujo de información referente al sistema de TI (ejemplo interfaces del sistema, esquema de organización de las entradas y las salidas del sistema).
- ✓ Controles técnicos usados por los sistemas de TI (ejemplo construcción de módulos o la agregación de productos de seguridad que permitan la identificación y autenticación, los **controles de acceso discrecional** o **obligatorio**, auditoria, protección de información residual, métodos de cifrado).
- ✓ Administración de los controles usados en los Sistemas de TI (normas de comportamiento, planificación de la seguridad).
- ✓ Controles operacionales usados por los sistemas de TI (por ejemplo personal de seguridad, respaldos, contingencia, reanudación y recuperación de operaciones, mantenimiento del sistema, almacenamiento fuera de sitio, establecimiento de cuentas de usuario y procedimiento de eliminación, controles para segregación de las funciones de los usuarios; como es el acceso a los usuarios privilegiados versus acceso de usuarios estándares).
- ✓ Seguridad Física ambiental para los sistemas de TI (por ejemplo protección de la instalación, políticas del centro de datos "*data center*")
- ✓ La seguridad del medio ambiente implementada para el ambiente de procesamiento del sistema de TI (por ejemplo controles para: humedad, agua, la energía, la contaminación, la temperatura y productos químicos).

Para un sistema que está en la fase de iniciación o desarrollo, la información del sistema puede obtenerse a partir del diseño o en el documento de requerimientos. Para un sistema de TI bajo desarrollo es necesario definir reglas claves de seguridad y planificar los atributos para el futuro del sistema de TI. Los documentos del diseño del sistema y el plan de seguridad del mismo pueden proveer de información útil sobre la seguridad de un sistema de TI que está en desarrollo.

Sobre el sistema de TI operativo, los datos recogidos sobre el sistema en su entorno de producción, incluidos los datos sobre la configuración del sistema, la conectividad, documentados y los no documentados, y los procedimientos y prácticas. Son por lo tanto la descripción del sistema, que puede ser basada en la seguridad proporcionada por la infraestructura esencial o en los futuros planes de seguridad para el sistema.

Todas o una combinación de las siguientes **técnicas,** pueden ser utilizadas para la **recopilación de información** relevante para el sistema de TI dentro de las fronteras operaciones de este:

Cuestionarios. Para recolectar información relevante, el personal de evaluación de riesgos, puede desarrollar un cuestionario con respecto a la administración y la planificación de controles o los controles ya usados por el sistema de TI. Este

cuestionario debe ser distribuido a aquellos que lo van a aplicar como el personal técnico y personal administrativo no técnico quienes están diseñando o dando soporte al sistema de TI. El cuestionario debe también ser usado durante las visitas en sitio (in situ) y en las entrevistas.

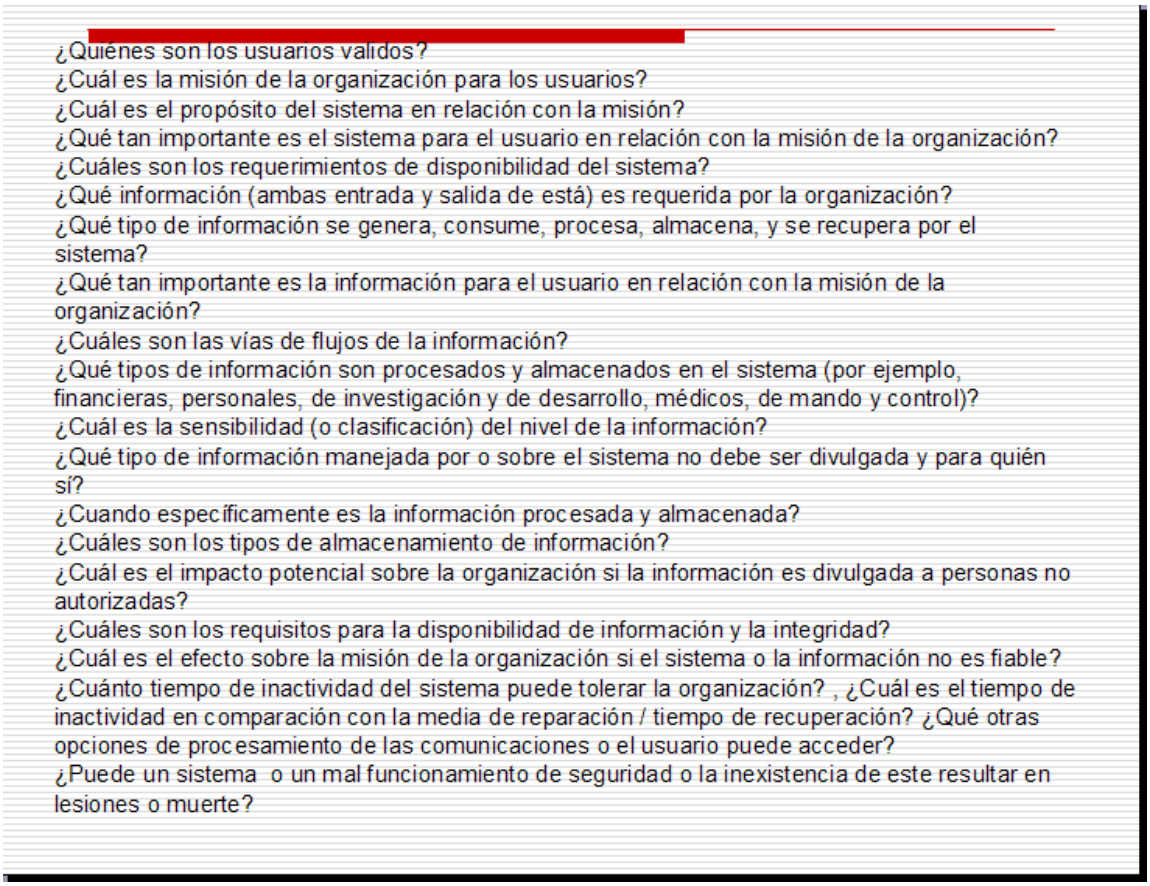

Figura 4 Ejemplo de Cuestionario

Las entrevistas en sitio (in situ). Las entrevistas con el personal de soporte y el personal administrativo del sistema de TI pueden permitir evaluar los riesgos en el personal para recolectar información útil sobre el sistema de TI (por ejemplo como es operado y manejado el sistema). Las visitas en sitio, también permitirán la evaluación de riesgos en el personal, con la finalidad de observar y recolectar información sobre los aspectos en seguridad física, ambiental y operacional del sistema de TI (Las preguntas en la entrevista deben ser adaptadas en base al SDLC del sistema de TI evaluado). Para sistemas todavía en la fase de diseño, la visita en sitio sería de manera personal mediante ejercicios de recopilación de datos que podrían proporcionar la oportunidad de evaluar el entorno físico en el cual el sistema funcionará.

Revisión de documentos. Documentos de Políticas (ejemplos documentación de legislación, directivas), documentación del sistema (ejemplo guía de usuario para el sistema, manual administrativo del sistema, diseño y requerimientos del sistema, documentos de adquisición), y documentación relativa a la seguridad (ejemplo reportes de auditoria previos, reportes de evaluación de riesgos, resultados de pruebas al sistema, **plan de seguridad del sistema**, políticas de seguridad), pueden proporcionar buena información sobre los controles de seguridad usados y previstos para el sistema de TI. El objetivo del análisis del impacto de una organización o la evaluación de sus activos críticos, proporciona información respecto al sistema y los datos críticos o sensitivos.

El plan de seguridad del sistema se realiza durante la fase inicial, una evaluación de riesgos debe ser usada para desarrollar dicho plan en forma inicial.

Uso de Herramientas de Escaneo[3] **Automatizado.** Métodos técnicos proactivos que pueden ser utilizados para recolectar eficientemente información del sistema. Por ejemplo, una herramienta de red que localice y represente gráficamente la distribución relativa de las partes de un sistema interconectado (*network mapping*) que permitirá identificar los servicios que están funcionando sobre un grupo grande de *hosts*[4] y proporcionar una manera rápida de elaborar perfiles individuales de los objetivos del sistema o sistemas de TI.

La información reunida puede ser conducida durante el proceso de evaluación de riesgos, desde la determinación de los aspectos peculiares del sistema y a través de la Documentación de Resultados.

Por lo tanto la salida del Paso 1, determinación de los aspectos peculiares del sistema, conseguirá una buena imagen del ambiente del sistema de TI y la delimitación de las fronteras de éste.

2.3.2. Identificación de Amenazas

Una amenaza es la posibilidad de que un indicio inminente[5] se ejecute con éxito sobre una determinada vulnerabilidad. Una vulnerabilidad es una debilidad que puede ser desencadenada accidentalmente o explotada intencionalmente. Un indicio inminente no presenta un riesgo cuando no existe una vulnerabilidad que pueda ser explotada.

[3] Las herramientas de escaneo tienen la finalidad de someter mediante algún mecanismo a una exploración con la finalidad de producir una representación mayormente detallada del objeto o situación en cuestión.
[4] Un host en términos generales es una computadora con una posición especifica en una red de computadoras (*network*), También puede denominarse nodo.
[5]Indicio inminente considérese como un evento próximo a suceder y que tiene la posibilidad de con llevar un riesgo (origen de una amenaza). Cualquier intento y método con un objetivo de explotación intencional de una vulnerabilidad o también como una situación o método que puede accidentalmente desencadenar una vulnerabilidad.

Para determinar la probabilidad de una amenaza se debe considerar los indicios inminentes (origen de la amenaza), las posibles vulnerabilidades y los controles existentes.

La identificación de los indicios inminentes o el origen de una amenaza tienen como objetivo recopilar en un listado el extracto de los posibles indicios inminentes que son aplicables al sistema de TI que se esta evaluando.

El **origen de una amenaza** es definida como cualquier circunstancia o evento con potencial para causar daño a un sistema de TI. Las más comunes pueden ser: naturales, humanos o ambientales.

Las amenzas de origen natural son: los terremotos, las inundaciones, los tornados, avalanchas, tormentas eléctricas, entre otros eventos. En cuanto a las amenzas de origen humano, es decir, los eventos que son activados o causados por los seres humanos incluso actos involuntarios (introducción de datos de forma inadvertida) o acciones deliberadas (Ataque basados en la red, colocar *software* malicioso, el acceso no autorizado a información confidencial). Y las amenazas de origen ambiental (a largo plazo, la falta de energía eléctrica, la contaminación los productos químicos, fugas de líquidos)

En la evaluación del origen de una amenaza es importante considerar todos los posibles indicios inminentes que puedan causar daño a un sistema de TI y a su entorno de procesamiento. Aunque para exponer una amenaza para un sistema de TI localizado en un desierto puede no incluir inundaciones naturales, debido a la baja probabilidad de que un evento de este tipo se produzca, las amenazas ambientales, como la explosión de una tubería puede inundar la habitación donde se encuentra el equipo de computo y causar daño a los activos y recursos de TI en una organización. Las amenazas de origen humano pueden ser a través de actos intencionados, como ataques deliberados por personal malicioso, o empleados disgustados, o actos no intencionales como negligencia y errores.

Un ataque deliberado puede ser cualquier intento malicioso para obtener acceso sin autorización a un sistema de TI (por ejemplo a través de adivinar las contraseñas) con el fin de comprometer el sistema y la integridad de los datos, la disponibilidad, la confidencialidad o un benigno pero no obstante, útil, intento de burlar la seguridad de un sistema. Un ejemplo de este último tipo de ataque de carácter deliberado, es el programa que contiene escrito en el código, por el que lo elaboró, un caballo de Troya, con la finalidad de saltarse los controles de seguridad del sistema con la premisa de cumplir con su supuesto trabajo, el cual por supuesto no incluye sembrar código malicioso.

La **motivación** y los recursos para llevar a cabo un ataque donde el origen de la amenaza es humana y potencialmente peligrosa. A continuación se presentan una visión general de las amenazas humanas comunes, sus posibles motivaciones, así como los métodos o **acciones amenazantes** por los cuales se puede llevar a cabo un ataque.

Origen de la amenaza	Motivación	Acciones Amenazantes
Hacker[6], Cracker[7] [4]	Reto Ego	Hacking[8] [5] Ingeniería social[9] [6]
	Rebelión	Intrusión a sistemas, robo Acceso no autorizado al sistema.
Crimen informático[10]	Destrucción de información. Ilegal divulgación de la información. Beneficio monetario. Alteración no autorizada de datos.	Crimen informático (por ejemplo la manipulación de datos de entrada cualquier persona que tenga acceso a las funciones normales del procesamiento de los datos en la fase de adquisición de los mismos). Actos Fraudulentos (por ejemplo, la repetición, suplantación, intercepción) Vender Información Alteraciones (*spoofing*[11]) Intrusión al sistema

[6] *Hacker* es un experto en alguna o varias ramas de las Tecnologías de Información y las telecomunicaciones: programación redes de computadoras, sistemas operativos, hardware. *Hacker* de la palabra inglesa hace referencia a divertirse con el ingenio. *Hacker* es toda aquella persona con elevados conocimientos informáticos independientemente de la finalidad con que los use.

[7] Un *cracker* es alguien que viola la seguridad de un sistema informático por un beneficio particular o para hacer daño, como la modificación de código fuente de un programa (denominado *cracking*). También se les denomina hackers a los aficionados a la informática que buscan defectos, puertas traseras. *Cracker* es aquel individuo que se especializa en saltar las protecciones anti-copia de software, de ahí el nombre crack para definir los programas que eliminan las restricciones en las versiones de demostración de software comercial.

[8] En resumen, el hacking es la técnica o arte de encontrar los límites de los productos, aparatos y servicios digitales de informática o comunicaciones y compartirlo con otros y/o los fabricantes mismos de ésos productos.

[9] La ingeniería social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Un ingeniero social usará comúnmente el teléfono o Internet para engañar a la gente y llevarla a revelar información sensible, o bien a violar las políticas de seguridad típicas. Con este método, los ingenieros sociales aprovechan la tendencia natural de la gente a confiar en su palabra, antes que aprovechar agujeros de seguridad en los sistemas informáticos. Generalmente se está de acuerdo en que “los usuarios son el eslabón débil” en seguridad; éste es el principio por el que se rige la ingeniería social.

[10] Los delitos informáticos son actos cometidos mediante el uso indebido de las tecnologías de información cuando tales conductas constituyen el único medio de comisión posible -o el considerablemente más efectivo- para lograr el efecto dañoso que vulnera bienes jurídicos cuya protección es necesaria. Los delitos informáticos de resultado, se refiere a conductas que vulneran los sistemas que utilizan tecnologías de información, es decir, que lesionan el bien jurídico constituido por la información, lo que implica que legislaciones penales conciban como bien jurídico la protección de los sistemas que la contienen, procesan, resguardan y transmiten, puesto que la información no es más que el bien que subyace en ellos. Los delitos informáticos de medio, recoge las conductas que se valen del uso indebido de las tecnologías de información para atentar contra bienes jurídicos tradicionales, distintos de la información contenida y tratada en sistemas automatizados.

[11] Alteración de paquetes de internet (*internet Spoofing*) Un ataque utilizando las direcciones alteradas o simuladas de paquete de Internet fuente (IP). Esta técnica explota aplicaciones que utilizan autenticación basada en direcciones IP. Esta técnica también puede permitir a un usuario no autorizado tener acceso de raíz en el sistema en cuestión.

Origen de la amenaza	Motivación	Acciones Amenazantes
Terrorismo	Chantaje Destrucción Explotación Venganza	Bomba/Terrorismo Guerra de información[12] [7] Ataques a los sistemas (ejemplo ataque de denegación de servicios distribuido DDOS[13] [8]por sus siglas en ingles) Penetración del sistema Manipulación, falsificación, alteración del sistema
Espionaje industrial (compañías, gobiernos extranjeros u otros gobiernos interesados)	Ventajas competitivas Espionaje Económico	Explotación económica Robo de Información Ingeniería social Penetración del sistema Intrusión en la privacidad de las personas. Acceso no autorizado al sistema (por ejemplo acceso a información clasificada, privada, y/o relacionada con tecnología)
Personal con acceso a información privilegiada (probablemente entrenados, molestos, maliciosos, negligentes, deshonestos, o empleados despedidos).	Curiosidad Ego Inteligencia Beneficio Monetario Venganza Errores y omisiones (por ejemplo errores al introducir datos, un error de programación)	Asalto a un empleado Chantaje Escudriño de la información privada. Abuso de los recursos de computo Fraude y robo Publicar información Corrupción de datos, falsificar la entrada de los mismos Intercepción Código Malicioso[14] (por ejemplo virus[15] [9],

[12] La guerra de la información es el uso y la gestión de la información en la búsqueda de una ventaja competitiva sobre un rival. La guerra de la información puede incluir la recolección de información táctica, la garantía de que la propia información es válida, la difusión de la propaganda o la desinformación para desmoralizar al enemigo y a la opinión pública, lo que socava la calidad de oponerse a la fuerza de información y la denegación de la recopilación de información de oportunidades a las fuerzas de oposición.

[13] Un ataque DDOS (*Distributed Denial Of Service Attack*) o Ataque de Denegación de Servicio Distribuido es un tipo especial de DoS (*Denial of Service* es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos) consistente en la realización de un ataque conjunto y coordinado entre varios equipos (que pueden ser cientos o miles) hacia un *host* víctima. Esto es posible gracias a un cierto tipo de malware (software que tiene como objetivo infiltrarse en o dañar una computadora sin el conocimiento de su dueño y con finalidades muy diversas ya que en esta categoría encontramos desde un troyano hasta un spyware.) que permite obtener el control de esas máquinas y que un atacante ha instalado previamente en ellas, bien por intrusión directa o mediante algún gusano. Los DDoS consiguen su objetivo gracias a que agotan el ancho de banda de la víctima y sobrepasan la capacidad de procesamiento de los *routers*, consiguiendo que los servicios ofrecidos por la máquina atacada no puedan ser prestados.
A las máquinas infectadas por el *malware* mencionado anteriormente se las conoce como máquinas *zombie* (zombis, en español), y al conjunto de todas las que están a disposición de un atacante se le conoce como *botnet* (red de bots normalmente es un gusano que corre en un servidor infectado con la capacidad de infectar a otros servidores de forma automatizada).

[14] Código Malicioso es software que tiene como objetivo infiltrarse o dañar las funciones de una computadora sin consentimiento de su dueño y con finalidades muy diversas como espiar, o permitir un acceso no autorizado por ejemplo.

[15] Los virus son programas que se replican y ejecutan por sí mismos, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en una computadora, además tienen, básicamente, la función de

Origen de la amenaza	Motivación	Acciones Amenazantes
		bombas lógicas[16] [10], caballos de Troya[17]) Venta de Información del personal *(Bugs)* errores del sistema Intrusión del sistema Sabotaje del sistema Acceso no autorizado al sistema.

Tabla 2 Amenazas de origen humano: La motivación y las acciones amenazantes

Esta información sería útil para una organización que estudia las amenazas de origen humano, la adaptación de estos entornos amenazantes y la determinación de los atributos peculiares expuestas de las amenazas de origen humano. Además revisando el historial de las fallas o rupturas en el sistema; reportes de violaciones de seguridad; reportes de incidentes; y entrevistas con los administradores del sistema, personal de la mesa de servicio[18] y la comunidad de usuarios durante la recaudación de información, ayudará a identificar el origen de las amenazas que tiene la posibilidad de causar daño en un sistema de TI y sus datos y que representan preocupación donde existe una vulnerabilidad.

Una estimación de la motivación, de los recursos y capacidades necesarias para llevar a cabo un ataque con éxito, debe desarrollarse después de identificar el origen potencial de la amenaza, con el fin de determinar la probabilidad de ocurrencia de la amenaza, al explotar una vulnerabilidad en un sistema. Esto queda conformado dentro del paso de determinación de la probabilidad.

La exposición de las amenazas o el listado del origen potencial de las amenazas, deben adecuarse a la organización y a su entorno de procesamiento de manera individual (por ejemplo los hábitos de cómputo del usuario final). En general, la

---

propagarse, replicándose, pero algunos contienen también una carga dañina (payload) con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando tráfico inútil.

[16] Las bombas lógicas son en cierta forma similares a los troyanos: se trata de código insertado en programas que parecen realizar cierta acción útil. Pero mientras que un troyano se ejecuta cada vez que se ejecuta el programa que lo contiene, una bomba lógica sólo se activa bajo ciertas condiciones, como una determinada fecha, la existencia de un directorio con un nombre dado, o el alcance de cierto número de ejecuciones del programa que contiene la bomba; así, una bomba lógica puede permanecer inactiva en el sistema durante mucho tiempo y por tanto sin que nadie note un funcionamiento anómalo hasta que el daño producido por la bomba ya está hecho.

[17] Un caballo de Troya (también llamado Troyano) es una pieza de software dañino disfrazado de software legítimo. Los caballos de Troya no son capaces de replicarse por sí mismos y pueden ser adjuntados con cualquier tipo de software por un programador o puede contaminar a los equipos por medio del engaño. Su nombre es dado por su peculiar forma de actuar como los Troyanos de la historia, entrando en la computadora, ocultos en otros programas aparentemente útiles e inofensivos pero que al activarse crean problemas a la computadora al desarrollar la acción de estos archivos infecciosos.

[18] Mesa de Servicio (Service Desk) Punto único de contacto de clientes y usuarios, en el apartado de Servicios de Asistencia (Service Support) se hondará más en esta función característica de la metodología de ITSM (Administración o Gestión de servicios de TI) de donde se desprenden las buenas prácticas y procedimientos de ITIL

información sobre las amenazas de origen natural (por ejemplo inundaciones, terremotos y tormentas) debe estar disponible fácilmente.

Amenazas conocidas ya han sido identificadas por muchos gobiernos y organizaciones del sector privado. Las herramientas de detección de Intrusos, cada vez son más convenientes y frecuentes utilizarlas, y el gobierno y las organizaciones de diferentes sectores tanto público como privado, continuamente recopilan datos sobre eventos de seguridad, mejorando así la capacidad para evaluar en forma realista las amenazas. Algunos ejemplos se pueden encontrar en:

Medios masivos, particularmente recursos basados en Web como es SecurityFocus.com, SecurityWach.com, SecurityPortal.com, y SANS.org

Al finalizar este paso, de identificación de amenazas, se tendrá la exposición de las amenazas contenidas en un listado, con el origen de las amenazas y los sistemas vulnerables que podrían ser blancos.

2.3.3. Identificación de Vulnerabilidades

El análisis de amenazas para un sistema de TI debe incluir un análisis de vulnerabilidades asociadas con el ambiente del sistema. El objetivo de este paso es desarrollar una lista de las vulnerabilidades del sistema (desperfectos o vulnerabilidades) que pueden ser explotados por el origen o fuente de las amenazas potenciales.

"Una vulnerabilidad es una debilidad o desperfecto en los procedimientos de seguridad del sistema, en su diseño, en su implementación o en los controles internos que son realizados" [11] (pp. 15) (la vulnerabilidad es explotada de manera accidental o intencional) y como resultado de una brecha o una violación de las políticas de seguridad del sistema.

A continuación se presentan vulnerabilidades con su respectiva amenaza.

Vulnerabilidad	Origen de la amenaza	Acción Amenazante
Empleados despedidos con identificadores (ID) del sistema que no estén aún removidos.	Empleados despedidos	Ingresarse o marcase (*login*) dentro de la red de la empresa y tener acceso a los datos propiedad de la compañía.
Los *firewalls* de la compañía permiten vincularse a la entrada con el servicio de telnet[19] [12] y el	Usuarios sin autorización (ejemplos *hackers*, empleados despedidos, criminales	Usando un telnet hacia el servidor, denominado XYZ, escudriñando el sistema de

[19] Telnet es un protocolo de la pila de TCP/IP que emula una Terminal, la emulación se da por que el procesamiento realizado no se hace en la maquina del usuario si no que en una maquina remota también denominada Terminal tonta por este hecho, Telnet tiene la posibilidad de transferir datos en formato binario, emular terminales graficas, y transmitir información para ayudar en la administración centralizada de las Terminales. Telnet consigue una conexión virtual entre el cliente y el servidor.

Vulnerabilidad	Origen de la amenaza	Acción Amenazante
identificador (ID) para el usuario invitado (*guest*) esta habilitado en el servidor denominado XYZ.	informáticos, terroristas)	archivos[20] con el usuario invitado que tiene el identificador (ID) *guest*
El vendedor ha identificado deficiencias en el diseño de seguridad del sistema, sin embargo, los nuevos parches no han sido aplicados al sistema	Usuarios sin autorización (ejemplos *hackers*, empleados disgustados, criminales informáticos, terroristas)	Obteniendo acceso no autorizado a archivos del sistema debido a las vulnerabilidades conocidas sobre este.
El centro de Datos utiliza aspersores de agua para suprimir el fuego, las lonas para proteger el *hardware* y el equipo de daños causados por el agua no están en el lugar.	Fuego, personas negligentes	Los aspersores de agua están habilitados en el centro de datos

Tabla 3 Vulnerabilidades con su respectiva amenaza

Los métodos recomendados para identificar vulnerabilidades en los sistemas son la utilización de fuentes de las vulnerabilidades, la realización de pruebas de seguridad en el sistema y el desarrollo de una lista de control (*checklist*) con los requerimientos de seguridad.

Cabe mencionar que los tipos de vulnerabilidades que existen, y la metodología necesaria para determinar si las vulnerabilidades están presentes suelen variar dependiendo de la naturaleza del sistema de TI y la fase en que esté en el ciclo de vida de desarrollo del sistema (SDLC *System Developer Life Cycle*). Como a continuación se aborda.

Si el sistema no tiene el diseño todavía, la búsqueda de vulnerabilidades debe enfocarse en las políticas de seguridad de la organización, la planificación de procedimientos de seguridad, y la definición de requerimientos del sistema, y el análisis de los productos de seguridad de los proveedores o desarrolladores (por ejemplo los *white papers*[21] [13]).

Si el sistema de TI está siendo implementado, la identificación de vulnerabilidades debe ser ampliada para incluir información más específica, como es la planificación de las características de seguridad descritas en la documentación del diseño de seguridad y los resultados de las pruebas de certificación al sistema y la evaluación de este.

Si el sistema de TI está en operación, el proceso para identificar vulnerabilidades debe incluir, un análisis sobre las características de seguridad del sistema de TI,

[20] Sistema de Archivos o por la palabra en ingles *filesystem* se refiere al método para almacenar y organizar los archivos de una computadora y los datos que estos contienen para hacer más fácil el acceso a ellos.

[21] *White paper* es un documento de informe. Los *White papers* son utilizados para educar a los clientes, recogiendo un conjunto de indicios o señales que pueden conducir a la averiguación de algo por parte de una compañía o ayudan a las personas en la toma de decisiones, pueden ser también un informe de gobierno delineando una política.

además de los controles de seguridad, técnico y los procedimientos, utilizados para proteger al sistema.

Las vulnerabilidades técnicas y no técnicas asociadas con el ambiente de procesamiento del sistema de TI pueden ser identificadas a través de las técnicas de recopilación de información, descritas anteriormente. Una revisión de otras fuentes industriales (por ejemplo pagina Web del vendedor que identifican fallas y desperfectos en el sistema, comúnmente denominada *Knowledge Data Base*) serán utilizadas en la preparación de las entrevistas y en el desarrollo efectivo de los cuestionarios para identificar vulnerabilidades que pueden ser aplicables en sistemas de TI específicos (ejemplo: una versión especifica de un determinado sistema operativo[22] [14]). El Internet es otra fuente de información sobre vulnerabilidades conocidas en sistemas expuestas por los proveedores, junto con los parches inmediatos (*hot fixies*), *service packs*[23] [15], parches y otras medidas correctivas que pueden aplicarse para eliminar o mitigar las vulnerabilidades. Fuentes documentadas de vulnerabilidades que deben ser consideradas durante el análisis de vulnerabilidades incluyen, pero no están limitados a lo siguiente:

- ✓ Documentación previa de la evaluación de riesgos para el sistema de TI en cuestión
- ✓ Reportes de auditoria del sistema de TI, así como reportes de anomalías, informes de las revisiones de seguridad y reportes de evaluaciones y pruebas en el sistema.
- ✓ Lista de vulnerabilidades, como es la base de datos de vulnerabilidades NIST I-CAT
- ✓ Consultores de Seguridad
- ✓ Consultores de los proveedores
- ✓ Equipos de respuesta a emergencias y listas posteriores (por ejemplo SecurityFocus.com envío a foros)
- ✓ Aseguramiento de la Información, vulnerabilidad Alertas y boletines de sistemas militares
- ✓ Sistema de análisis de software de seguridad

Métodos proactivos empleando sistemas para pruebas, pueden ser utilizados para identificar vulnerabilidades en el sistema eficientemente, dependiendo de la criticidad del sistema de TI y la disponibilidad de los recursos (ejemplo: los fondos asignados, la tecnología disponible, las personas con la experiencia necesaria para realizar las pruebas). Los métodos de pruebas incluyen:

[22] Es el software que administra la compartición de los recursos en una computadora.
[23] *Service Pack* es una colección de actualizaciones, reparaciones y/o mejoras desarrolladas en la forma de un sencillo e instalable paquete.

- ✓ Herramientas de Escaneo automatizadas, para localización de las vulnerabilidades
- ✓ Pruebas y evaluaciones de seguridad (ST & E)[24] [16]
- ✓ Pruebas de penetración

El escaneo mediante herramientas automatizadas, para localización de las vulnerabilidades, se utiliza para escudriñar un grupo de *hosts* o una red para conocer los servicios vulnerables (por ejemplo sistemas que permiten anónimamente el envío y reenvío de correos electrónicos mediante el protocolo FTP[25] [17]) sin embargo, cabe señalar que algunas de las posibles vulnerabilidades identificadas por la herramienta de escaneo automático pueden no representan verdaderas vulnerabilidades en el contexto del ambiente del sistema. Por ejemplo, algunas de estas herramientas de escaneo tienen un índice de potenciales vulnerabilidades sin considerar el ambiente y los requerimientos en el sitio en cuestión. Algunas de las "vulnerabilidades" señaladas por el *software* de escaneo automatizado pueden no ser en realidad consideradas como vulnerables para una situación particular pero podría configurarse de esta forma ya que su entorno así lo requiere, por lo tanto este método de ensayo puede producir falsos positivos.

ST&E es otra técnica que puede ser utilizada en la identificación de vulnerabilidades en el sistema de TI durante el proceso de evaluación de riesgos. Esto incluye el desarrollo y ejecución de un plan de prueba (por ejemplo un escrito en que breve y ordenadamente se han apuntado algunas ideas o cosas con objeto de que sirva de guía para determinado fin, procedimientos de pruebas, y resultados esperados de las pruebas). El propósito de analizar la seguridad del sistema de TI es para probar lo efectivo de los controles de seguridad en un determinado sistema de TI y como estos controles tienen que estar aplicados en un ambiente operacional. El objetivo es asegurar que la aplicación de los controles cumplan con las especificaciones aprobadas de seguridad, para el *software* y *hardware* además de las políticas de seguridad de la organización o el cumplimento de los estándares industriales.

Las **pruebas de penetración** pueden ser usadas para complementar las revisiones de los controles de seguridad y asegurar que las diferentes facetas del sistema de TI

[24] Pruebas y evaluaciones de seguridad, también abreviado como ST&E por sus siglas en ingles *Security Test and Evaluation* es la examinación o análisis de las medidas proactivas que son interpuestas en un sistema de información una vez este plenamente integrado y funcional.
Los objetivos del ST&E son descubrir los desperfectos en las fases de diseño, implementación y operación que podrían permitir la violación de la política de seguridad; determinar los mecanismos adecuados de seguridad, las garantías y otras propiedades para hacer cumplir las políticas de seguridad; Evaluar el grado de consistencia entre la documentación del sistema y su implementación.
[25] El Protocolo de transferencia de archivos (FTP) proporciona los elementos básicos de la compartición de archivos entre máquinas. FTP utiliza TCP para crear una conexión virtual para la información de control y, a continuación, crea una conexión TCP para las transferencias de datos. La conexión utiliza el control de una imagen del protocolo Telnet para el intercambio de comandos y mensajes entre *hosts*.

sean aseguradas. Las pruebas de penetración, donde los empleados en el proceso de la evaluación de riesgos, pueden estar utilizando activos en un sistema de TI habilitados para resistir atentados intencionales con la finalidad de eludir los sistemas de seguridad. Su objetivo es poner a prueba el sistema de TI desde el punto de vista del originador de la amenaza e identificar las fallas potenciales en los esquemas de protección de los sistemas de TI.

El resultado de este tipo de pruebas de seguridad, optativas, ayudara a identificar vulnerabilidades en un sistema.

Durante el **desarrollo de una lista de control** (*checklist*), con los requerimientos de seguridad, el personal para la evaluación de riesgos determinará si los requerimientos de seguridad estipulados para el sistema de TI y la recaudación durante la determinación de los atributos peculiares de un sistema, están siendo cumplidos por los controles existentes o los controles previstos. Típicamente los requerimientos del sistema de seguridad, pueden ser presentados en forma de tabla, con a cual los requerimientos, acompañados de su descripción o explicación de cómo se diseñará, o implementará en el sistema, satisfacen o no, los requisitos de los controles de seguridad.

Los requisitos de seguridad de una lista de control contienen los criterios básicos de seguridad que pueden ser utilizados para la evaluación sistemática, e identificación de las vulnerabilidades en los activos (personal, hardware, software, información), procedimientos no automatizados, procesos, y la transferencia de información asociada con determinado sistema de TI en las siguientes áreas:

- ✓ Administrativa
- ✓ Operacional
- ✓ Técnica

A continuación se listan criterios sugeridos en seguridad para su utilización en la identificación de vulnerabilidades en un sistema de TI en cada área de seguridad.

Área de Seguridad	Criterio de seguridad
Administración o Gestión de la seguridad	Asignación de responsabilidades La continuidad del soporte Capacidad de la respuesta a incidentes Revisiones periódicas de los controles de seguridad Autorizar personal y el origen de las investigaciones. Evaluación de Riesgos Seguridad y capacitación técnica Separación de funciones Sistemas de Autorización y Restitución Sistema o aplicación del plan de seguridad

Área de Seguridad	Criterio de seguridad
Seguridad Operacional	Control de contaminantes esparcidos por aire (humo, polvo y químicos). Controles para asegurar la calidad del suministro de energía eléctrica. Medios de ingreso de datos (*Data media access*) y su eliminación (por ejemplo DVD, CD RW, *Diskettes*, Discos Ópticos, Cintas). Distribución de datos externos y etiquetado. Seguridad en las instalaciones (por ejemplo cuarto de cómputo, centro de datos, oficina). Control de humedad. Control de Temperatura. Estaciones de trabajo, portátiles (laptops) y computadoras autónomas para el personal.
Seguridad Técnica	Comunicaciones (por ejemplo sistemas de interconexión, ruteadores (*routers).* Criptografía. Control de Acceso discrecional. Identificación y autenticación. Detección de intrusos. Reutilización de objetos. Sistemas de auditoria

Tabla 4 Criterios de Seguridad

El resultado de este proceso, es la obtención de una lista de control que expone los requisitos de seguridad, el resultado que arroje esta lista de control puede ser utilizado como entrada para una evaluación del cumplimiento e incumplimiento. Este proceso identificará las debilidades que representa vulnerabilidades potenciales, en cuanto a los procedimientos y procesos referentes al sistema.

Como salida del paso de identificación de vulnerabilidades se obtendrá un listado de las vulnerabilidades del sistema que pueden ser explotados por una determinada fuente de amenaza.

2.3.4. Análisis de los Métodos de Control

El objetivo de este paso, es analizar los controles que tienen que ser implementados o son planificados para su implementación, por la organización, para maximizar o eliminar la probabilidad de la explotar una vulnerabilidad y hacer presente una amenaza en el sistema.

Para obtener un índice global de las posibilidades que indiquen la probabilidad que existe en una vulnerabilidad potencial a ser explotada, es mediante la construcción de asociaciones con las amenazas ambientales (paso de la determinación de la probabilidad), la implementación actual o prevista de los controles debe ser también considerada. Por ejemplo una vulnerabilidad (debilidades en el sistema o en los procedimientos) que no es probable sea explotada o que la probabilidad de ocurrencia sea baja, debido a que hay una bajo nivel de interés o capacidad con respecto al origen de la amenaza o si los controles de seguridad son efectivos pudiendo eliminar o reducir la magnitud del daño.

Los controles de seguridad rodean el uso de **métodos** tanto técnicos como no técnicos. Los controles técnicos son salvaguardas o garantías que son incorporadas dentro del *hardware, software y firmware* (ejemplos mecanismos de control de acceso, mecanismos de autenticación e identificación, métodos de cifrado, *software* de detección de intrusos). Los controles no técnicos son administrados o gestionados. Los controles operacionales, como son las políticas de seguridad, procedimientos operacionales. La seguridad física y ambiental del personal.

Las categorías de control para ambos métodos de control tanto técnicos como no técnicos, deben ser en adelante clasificados, como cualquiera de los dos, preventivos o de detección. Estás dos subcategorías son explicadas a continuación:

i. Los controles preventivos inhiben intentos de violaciones de políticas de seguridad e incluyen regulaciones: como la aplicación de controles de acceso, cifrado y autenticación.

ii. Los controles de detección advierten o alertan de violaciones o intentos de violaciones a las políticas de seguridad e incluyen algo semejante a un control como lo es: el seguimiento de auditorias, los métodos de detección de intrusos, y las sumas de verificación (*checksum*).

Más adelante se explicarán estos controles desde el punto de vista de la implementación. La aplicación de controles, semejante al ocurrido durante el proceso de mitigación de riesgos, es el resultado directo de la identificación de deficiencias en los controles actuales o los previstos durante el proceso de evaluación de riesgos (por ejemplo controles inexistentes o controles que no están apropiadamente implementados).

El desarrollo de una lista de control con los requerimientos de seguridad o la utilización de una lista de control disponible será una ayuda en la examinación de controles de una manera eficiente y sistemática, como se vio con anterioridad.

La lista de control de requerimientos de seguridad puede ser utilizada para validar el incumplimiento de la seguridad así como su cumplimiento. Por lo tanto es esencial para la actualización de dichas listas que refleje los cambios en los controles ambientales de la organización (por ejemplo cambios en las políticas de seguridad, métodos y requerimientos) para asegurar la validez de la lista de control (*checklist*).

La salida del paso referente a los métodos de control es una lista de los controles actuales utilizados para el sistema de TI y los previstos para mitigar la probabilidad de que una vulnerabilidad sea explotada y reducir así el impacto del evento adverso.

2.3.5. Determinación de la Probabilidad

Para obtener un índice global de las posibilidadesque indiquen, la probabilidad que existe de que una vulnerabilidad potencial sea explotada, es a través de la construcción de asociaciones con las amenazas ambientales, la regulación de los siguientes factores deben ser considerados:

- ✓ Origen de la amenaza, motivación y capacidad de la misma.
- ✓ Naturaleza de la vulnerabilidad
- ✓ Existencia y eficiencia en los controles actuales

La probabilidad que una vulnerabilidad potencial sea explotada, por un determinado origen de la amenaza puede, ser descrita como alta, media o baja. A continuación se describen estos tres niveles de la probabilidad.

Nivel de la probabilidad	Definición de la probabilidad
Alta	El origen de la amenaza es altamente motivado y con la suficiente capacidad, y los controles para prevenir la que la vulnerabilidad sea explotada son ineficientes.
Media	El origen de la amenaza es motivado y capaz, pero los controles establecidos pueden impedir el éxito de una vulnerabilidad explotada
Baja	El origen de la amenaza tiene escasa motivación o capacidad o los controles establecidos previenen, o por lo menos impiden de forma significativa, que una vulnerabilidad sea explotada.

Tabla 5 Definición de la Probabilidad

A la salida de este paso se obtendrá un índice en cuanto a la probabilidad de un evento fortuito por la explotación de una vulnerabilidad

2.3.6. Análisis del Impacto

El paso más importante en la medición del nivel de riesgo es determinar el impacto adverso resultado de una vulnerabilidad explotada exitosamente por una amenaza. Antes de comenzar el análisis del impacto es necesario obtener la siguiente información necesaria, como se vio en el apartado la determinación de los atributos peculiares del sistema más específicamente en la recaudación de Información relativa al sistema:

- ✓ Misión del sistema (ejemplo los procesos realizados por el sistema de TI)
- ✓ El sistema y los datos críticos (ejemplo el valor del sistema o importancia para la organización).
- ✓ El sistema y los datos sensitivos

Esta información puede ser obtenida de la documentación existente en la organización, como es el reporte del análisis de impacto de la misión o un reporte de activos críticos estimados. Un análisis del impacto de la misión (el conocer también, cómo es para algunas organizaciones el análisis de impacto al negocio, BIA por sus siglas en ingles *Business Impact Analysis*) priorizar los niveles de impacto asociados con el compromiso de los activos de información de la organización, basados en la estimación cualitativa o cuantitativa de los activos críticos y sensibles. Estimar un

activo critico, identificar y priorizar los activos de información critica y sensible de la organización (ejemplo *hardware, software,* sistemas, servicios y lo relativo a los activos tecnológicos) que soportan aquella de la que pende la decisión en la misión de la organización.

Si esta documentación no existe o esas estimaciones de la organización sobre sus activos de TI no se han realizado, el sistema y los datos sensibles pueden determinarse basándose en el nivel de la protección requerida para mantener el sistema y sus datos, con las propiedades de: disponibilidad, integridad y confidencialidad.

Independientemente del método utilizado para determinar como un sistema de TI y sus datos son sensibles, los propietarios del sistema y la información son los únicos responsables en determinar el nivel de impacto en su propio sistema e información.

En consecuencia, en un análisis del impacto, el enfoque apropiado en las entrevistas, es para los propietarios del sistema e información.

Por lo tanto, el impacto adverso de un evento de seguridad puede ser descrito en términos de pérdida o degradación de cualquier, o una combinación de cualquiera, de los siguientes tres objetivos de seguridad: integridad, disponibilidad y confidencialidad. La siguiente lista provee una breve descripción de cuales objetivos de seguridad y la consecuencia (o impacto) de que estos no sean cumplidos:

i. Perdida de integridad. El sistema y la integridad de los datos se refiere a la exigencia de que la información este protegida de modificaciones inadecuadas. La integridad se pierde si se efectúan cambios no autorizados a los datos o al sistema de TI por cualquier acto intencional o accidental. Si el sistema o la integridad de los datos no se subsanan, continuando la utilización del sistema, contaminado con datos corruptos, puede resultar en inexactitud, fraude, o la toma de decisiones equivocadamente.

ii. También la violación de la integridad, puede ser el primer paso para un ataque exitoso contra la disponibilidad y confidencialidad del sistema. Por todas estas razones, la perdida de la integridad reduce la fiabilidad en un sistema de TI.

iii. Perdida de disponibilidad. Si la misión critica del sistema es la disponibilidad para sus usuarios finales. La misión de la organización puede ser afectada. La perdida de la funcionalidad del sistema y su eficacia operacional, por ejemplo puede resultar en perdida de tiempo productivo, impidiendo así a los usuarios finales la realización de sus funciones en apoyo a la misión de la organización.

iv. Perdida de confidencialidad. El sistema y la confidencialidad de los datos se refieren a la protección de la información contra la divulgación no autorizada de esta. El impacto de la divulgación no autorizada de información confidencial puede ocasionar incluso el poner en peligro la seguridad nacional. La divulgación no autorizada, imprevista o la revelación no intencional, pueden ocasionar la pérdida de la confianza del público (instituciones bancarias), la vergüenza o acciones legales en contra de la organización.

Algunos de los impactos tangibles pueden ser medidos cuantitativamente, dentro de la perdida de los ingresos, el costo de reparación del sistema, o el nivel de esfuerzo requerido para corregir el problema causado por el éxito de una amenaza en acción. Otros impactos (por ejemplo perdida de la confianza pública, perdida de la credibilidad, daño hacia los intereses de la organización) pueden no ser medidos en unidades especificas, pero pueden ser calificados o descritos en términos de alto, medio o bajo impactos. Debido a la naturaleza genérica de esta discusión a continuación se designan y describen algunas categorías cualitativas. Alto, medio o bajo impacto.

Magnitud del Impacto	Definición del impacto
Alto	El explotar la vulnerabilidad (1) puede resultar muy costoso por la pérdida de importantes activos materiales u otros recursos; (2) puede violar significativamente, dañar o impedir la misión organización, la reputación, o de interés general; O (3) en humanos puede provocar la muerte o lesiones graves.
Medio	El explotar la vulnerabilidad (1) puede dar como resultado una costosa perdida de activos tangibles o recursos; (2) puede, violar, dañar o impedir la misión de la organización, la reputación o interés de esta; (3) puede resultar en lesiones humanas.
Bajo	El explotar una vulnerabilidad (1) puede resultar en perdida de algunos activos tangibles o recursos o (2) puede afectar notablemente la misión de la organización, la reputación o interés de la misma.

Tabla 6 Magnitud del impacto, definición

Al llevar a cabo el análisis del impacto, debe considerarse las ventajas y desventajas de la **estimación cualitativa versus la cuantitativa.** La principal ventaja del análisis de impacto cualitativo es: que da prioridad a los riesgos e identifica las áreas para su inmediata mejoría en el tratamiento de la vulnerabilidad. La desventaja del análisis cualitativo es: que no provee mediciones cuantificables de la magnitud del impacto, por lo tanto, el hacer un análisis de costo-beneficio para cualquier control recomendado es difícil.

La principal ventaja de un análisis de impacto cuantitativo es que proporciona una medida de la magnitud del impacto, el cual puede ser utilizado en el análisis costo-beneficio de los controles recomendados. La desventaja es que dependiendo del índice numérico utilizado para expresar la medida, el significado del impacto del análisis cuantitativo puede ser confuso, requiriendo el resultado ser interpretado de una manera cualitativa. Adicionalmente otros factores deben ser considerados para determinar la magnitud del impacto. Esto puede incluir pero no estar limitado a:

- ✓ Una estimación de la frecuencia del origen de la amenaza explotada por la vulnerabilidad sobre un periodo de tiempo especifico (por ejemplo un año).
- ✓ Un costo aproximado para cada aparición del origen de una amenaza explotada por una vulnerabilidad.
- ✓ Un factor de peso basado en un análisis subjetivo del impacto relativo para una determinada vulnerabilidad explotada.

A la salida del análisis del impacto se obtendrá la magnitud de éste (alto, medio, bajo).

2.3.7. Determinación del Riesgo

El propósito de este paso es evaluar el nivel de dicho riesgo para el sistema de TI, es decir, la determinación del riesgo para una determinada vulnerabilidad con su respectiva amenaza. Puede ser expresada como una función de:

i. La probabilidad de una fuente dada de amenaza, que intente ejercer una determinada vulnerabilidad.

ii. La magnitud del impacto debida a la fuente exitosa de una amenaza ejercida en una vulnerabilidad.

iii. La adecuación de los controles de seguridad, previstos o existentes, para reducir o eliminar el riesgo.

iv. La medida del riesgo o escala de riesgo y una matriz de nivel de riesgo, debe ser desarrollada, a continuación se presenta un modelo de matriz de nivel de riesgo, además de describirse el resultado de los niveles de riesgo.

v. La determinación final para la misión del riesgo es derivada por múltiples índices asignados al estimar la factibilidad de una amenaza (probabilidad) y el impacto de la amenaza.

A continuación se muestra como el índice de riesgo general puede determinarse basándose en las aportaciones de estimación de la amenaza y las categorías de impacto de ésta.

La matriz que figura a continuación es una **matriz** de 3 x 3 **la amenaza de riesgo** (Alto, Medio y Bajo) y la amenaza de impacto (Alto, Medio y Bajo). Dependiendo de los requisitos del sitio y la granularidad de la evaluación de riesgo deseada, algunos sitios pueden utilizar una 4 x 4, o una matriz de 5 x 5. Este último puede incluir un **muy baja / muy alta amenaza** y un **muy bajo / muy alta amenaza de impacto** para generar un impacto **muy bajo / muy alto nivel de riesgo**. A "Muy Alto" nivel de riesgo puede requerir posiblemente el cierre del sistema o interrupción de todas las tecnologías de integración del sistema y las pruebas de esfuerzo.
La matriz, en la siguiente tabla, muestra en general, los niveles de riesgo Alto, Medio y Bajo y como se derivan. La determinación de los niveles de riesgo puede ser subjetiva. La razón de esta justificación puede ser explicada en términos de probabilidad asignada para cada nivel de estimación de la amenaza y un valor asignado para cada nivel de impacto. Por ejemplo:

i. La probabilidad asignada para cada nivel estimado de amenaza es: 1.0 para Alto, 0.5 para medio, 0.1 para bajo.

ii. El valor asignado para cada nivel de impacto es: 100 para alto, 50 para medio y 10 para bajo.

Estimación de la amenaza	Impacto		
	Bajo (10)	Medio (50)	Alto (100)
Alto (1.0)	Bajo 10 x 1.0 = 10	Medio 50 x 1.0 = 50	Alto 100 x 1.0 = 100
Medio (0.5)	Bajo 10 x 0.5 = 5	Medio 50 x 0.5 = 25	Medio 100 x 0.5 = 50
Bajo (0.1)	Bajo 10 x 0.1 = 1	Bajo 50 x 0.1 = 5	Bajo 100 x 0.1 = 10

Tabla 7 Escala de Riesgo: alto (>50 y hasta 100) medio (>10 y hasta 50) bajo (>1 hasta 10)

Si el nivel indicado en relación con determinados temas es tan baja como para ser considerada como "insignificantes" o no significativos (valor <1 en la escala de riesgo de 1 a 100), uno puede tenerlo por separado, en una cuenta a parte, en vez de trasladarlo a una acción administrativa. De este modo se asegurara de que no se pasa por alto cuando se este conduciendo el siguiente periodo de evaluación de riesgos. Este riesgo puede moverse hacia un nuevo nivel de riesgo sobre una reevaluación, debido a un cambio en la estimación de la amenaza y/o el impacto de ésta y el porqué de su criticidad.

A continuación se **describen los niveles de riesgo** de la matriz anterior. Esta escala de riesgos, con este índice, alto, medio y bajo, representa el grado o nivel de riesgo para determinado sistema de TI, la facilidad o procedimiento puede ser expuesto si una determinada vulnerabilidad se ejerce. La escala de riesgo también presenta las acciones, que el representante administrativo, los propietarios de la misión, deben tomar para cada nivel de riesgo.

Nivel de Riesgo	Descripción del riesgo y acciones necesarias
Alto	Si una evaluación o la determinación de las propiedades están evaluadas como de alto riesgo, hay una fuerte necesidad de medidas correctivas. Un sistema existente puede continuar operando, pero un plan de acción correctivo debe ser puesto en marcha lo más pronto posible.
Medio	Si una observación es valorada como de riesgo medio, las acciones correctivas son necesarias y un plan debe ser desarrollado para incorporar las acciones correctivas dentro de un periodo razonable de tiempo.
Bajo	Si una observación es descrita como de riesgo bajo, el sistema de aprobación de la autoridad designada (DAA por sus siglas en ingles *Designated Approving Authority*)[26] [18] debe determinar si las medidas correctivas son necesarias o decidir aceptar el riesgo.

Tabla 8 Escala de riesgo y acciones necesarias

[26] La aprobación de la Autoridad Designada (DAA por sus siglas en ingles *Designated Approving Authority*) en el departamento de defensa de los Estados Unidos es el funcionario con autoridad para asumir oficialmente la responsabilidad del funcionamiento de un sistema a un nivel aceptable de riesgo.

A la salida del paso 7, Determinación del riesgo, se obtendrán los niveles de riesgo (Alto, medio, bajo).

2.3.8. Recomendación de Controles

Durante esta etapa del proceso, los controles que pueden mitigar o eliminar los riesgos identificados, como las operaciones apropiadas, para la organización se proporcionan. El objetivo de recomendar controles es reducir el nivel de riesgo para el sistema de TI y sus datos llevándolos a un nivel aceptable. Los siguientes factores deben ser considerados en la recomendación de controles, además de soluciones alternativas para minimizar o eliminar los riesgos identificados. Factores para la determinación de controles:

- ✓ Eficacia de las opciones recomendadas (por ejemplo la compatibilidad con sistema)
- ✓ Legislación y regulación
- ✓ Política organizacional
- ✓ Impacto operacional
- ✓ Seguridad y Fiabilidad

La recomendación de controles es resultado de un proceso de evaluación de riegos, que aporta entradas para un proceso de mitigación de riesgos durante el cual, los procedimientos recomendados y los controles técnicos de seguridad son evaluados, priorizándolos e implementándolos.

Cabe señalar que no todos los posibles controles recomendados pueden ser implementados para reducir la perdida. Para determinar cuales son requeridos y apropiados para una determinada organización, es necesario realizar una relación costo-beneficio, como se explica en la sección de los riesgos residuales, debe llevarse a cabo para proponer la recomendación de controles, para demostrar que el costo de implementación de controles puede ser justificado por la reducción en el nivel de riesgo. En adición, el impacto operacional (por ejemplo el rendimiento en el sistema) y la viabilidad (por ejemplo requerimientos técnicos, la aceptación por los usuarios) o la introducción de las opciones recomendadas debe ser evaluada cuidadosamente durante el proceso de mitigación de riesgos.

2.3.9. Documentación de Resultados

Una vez que la evaluación de riesgos se ha completado (origen de las amenazas, identificación de vulnerabilidades, evaluación de riesgos y recomendación de los controles previstos) El resultado debe ser documentado en un reporte oficial o en una sesión informativa.

Un informe de evaluación de riesgos es un informe de gestión que ayuda a los altos cargos directivos, los propietarios de la misión, a tomar decisiones sobre las políticas, procedimientos, presupuesto, y el funcionamiento del sistema y de la gestión de cambios. A diferencia de una auditoria o informe de investigación, que busca al infractor, un informe de evaluación de riesgos no debe ser presentado en una manera acusatoria, sino como un enfoque sistemático y analítico para evaluar el riesgo a fin de que la alta dirección comprenda los riesgos y se asignen recursos para reducir y corregir posibles pérdidas. Por esta razón, algunas personas prefieren hacer frente a la amenaza y a la respectiva vulnerabilidad como observación en vez de las determinaciones del informe de evaluación del riesgo.
Como salida del paso 9, documentación y resultados se obtiene el reporte de evaluación de riesgos que describe las amenazas y vulnerabilidades, medidas de riesgo, y recomendaciones proporcionadas para la implementación de controles.

2.3.9.1. Ejemplo de un Reporte de Evaluación de Riesgos

Reporte
Resumen ejecutivo **I. Introducción** ✓ Propósito. ✓ Alcance de la evaluación de riesgos. Describe los componentes del sistema, elementos, usuarios, localizaciones del sitio (si aplica) y cualquier otro detalle del sistema que esta considerado en la evaluación. **II. Propuesta de Evaluación de riesgos.** Breve descripción de la propuesta usada para conducir la evaluación de riesgos, como es: ✓ Los participantes (ejemplo miembros del equipo de evaluación de riesgos) ✓ La técnica usada para recabar información (por ejemplo el uso de alguna herramienta, cuestionarios) ✓ El desarrollo y descripción de la escala de riesgo (ejemplo matriz de nivel de riesgo de 3 x 3, 4 x 4 o 5 x 5) **III. Determinación de los atributos peculiares en un sistema** Determinación de los atributos peculiares en un sistema, incluyendo hardware (servidores, ruteadores y *switches*), *software* (por ejemplo: aplicaciones, sistemas operativos, protocolos), las interfaces del sistema (por ejemplo enlaces de comunicaciones) datos, y usuarios. Proporcionar un diagrama de conectividad o un organigrama de entradas y salidas del sistema para delimitar el alcance de este esfuerzo de evaluación de riesgos. **IV. Declaración de Amenazas**

Reporte
Recopilar y listar el origen de las amenazas potenciales y asociarlas con las acciones amenazantes aplicables para el sistema evaluado. **V. Resultados de la evaluación de Riesgos** Listado de observaciones (vulnerabilidad con su respectiva amenaza). Cada observación debe incluir. ✓ Número de observación y una breve descripción de la misma (ejemplo: Observación 1: Usuario del sistema su password puede ser adivinado o ser débil). ✓ Discusión del origen de la amenaza y su respectiva vulnerabilidad. ✓ Identificación de los controles existentes de seguridad para la mitigación. ✓ Discusión de la estimación y evaluación (ejemplo alta, media, o baja estimación) ✓ Discusión del análisis de impacto y evaluación (ejemplo alto, medio, o bajo impacto). ✓ Índice de riesgo basado en una matriz de niveles de riesgo (alto, medio, o bajo nivel de riesgo). ✓ Controles recomendados o opciones alternativas para reducir el riesgo. Nótese que el término discusión se refiere al análisis o comparación de los resultados de una investigación, a la luz de otros existentes o posibles. **VI. Resumen** El número total de observaciones. Resumir las observaciones, los niveles de riesgo asociado, las recomendaciones y cualquier comentario en formato de tabla para facilitar la implementación de los controles recomendados durante el proceso de mitigación de riesgos.

2.4. Mitigación de Riesgos

La mitigación del riesgo es el segundo proceso en la administración de riesgos, involucra la priorización, evaluación e implementación de los factores de reducción de riesgo mediante la recomendación de los controles obtenidos en el proceso de evaluación de riesgos.

Debido a que la eliminación de todos los riesgos suele ser poco práctico o casi imposible, es responsabilidad de los altos directivos y los administradores del negocio emplear el menor costo e implementar los controles más apropiados, para disminuir

la misión del riesgo a un nivel aceptable, con un mínimo de efectos adversos sobre los recursos de la organización y la misión de ésta. [19](pp. 27)

2.4.1. Opciones de Mitigación de Riesgo

La mitigación de riesgos es una metodología sistemática, usada por los altos directivos y los administradores del negocio para reducir el riesgo

La mitigación de riesgos puede ser alcanzada a través de cualquiera de las siguientes opciones de mitigación de riesgo:

i. **Hipótesis de riesgo**. Para aceptar un riesgo potencial y continuar operando el sistema de TI o para implementar controles para disminuir el riesgo a un nivel aceptable

ii. **Eludir o eximir riesgos**. Para eximir riesgos por medio de la eliminación de la causa y/o consecuencia de este (por ejemplo renunciar a ciertas funciones del sistema o cesar el sistema cuando el riesgo ha sido identificado).

iii. **Limitación del riesgo**. Para limitar el riesgo por la implementación de controles que minimicen el impacto adverso, por que una vulnerabilidad ha sido explotada (por ejemplo usando un soporte preventivo, controles de detección[27] [20]).

iv. **Planeación de riesgos**. A la administración de riesgos mediante el desarrollo de un plan de mitigación de riesgos que prioricé, implemente y mantenga los controles.

v. **Investigación o reconocimiento**. Para disminuir el riesgo o la perdida por el reconocimiento de la vulnerabilidad o flujo e investigación de controles para corregir dicha vulnerabilidad.

vi. **Transferencia de Riesgo**. Para transferir el riesgo mediante el uso de otras opciones para compensar la pérdida, como la compra de seguros.

El objetivo y misión de la organización debe considerar seleccionar cualquiera de las opciones de mitigación de riesgo. Puede no ser practico el abordar todos los riesgos conocidos por lo que debe darse prioridad a la amenazas, con su respectiva vulnerabilidad, que tienen el potencial significativo de causar daño en la misión de la organización. Así mismo en el resguardo de la misión de la organización y sus sistemas de TI, por que cada organización tiene sus propios objetivos y un ambiente único. La opción usada para mitigar el riesgo, además de los métodos para la implantación de controles puede variar. La elección del mejor de los enfoques

[27] Controles de detección son asignados para reservar o dilatar para otro tiempo los errores e irregularidades que se están llevando acabo y asegurar su pronta corrección. Estos controles representan una continuidad de gastos operativa son con frecuencia costoso, pero necesarios, Los controles de detección suministran los medios para corregir errores de datos, además de modificar los controles existentes o la recuperación de los activos perdidos.

consiste en la utilización de las tecnologías apropiadas entre los distintos proveedores de productos de seguridad, junto con la correspondiente opción de mitigación de los riesgos y las medidas administrativas consideradas no técnicas consideradas.

2.4.2. Estrategia de Mitigación de Riesgos

Como responsabilidad de los altos directivos, propietarios de la misión, y los administradores del negocio, es la de conocer los riesgos potenciales y los controles recomendados cuestionando: ¿cuándo y sobre qué circunstancias debe tomarse determinada acción?, ¿cuándo se implementaran estos controles para mitigar el riesgo y proteger su organización?

La gráfica de mitigación de riesgo, que se muestra a continuación, aborda estos cuestionamientos. Los puntos apropiados para la implementación de acciones de control son indicados por la palabra SI en la figura.

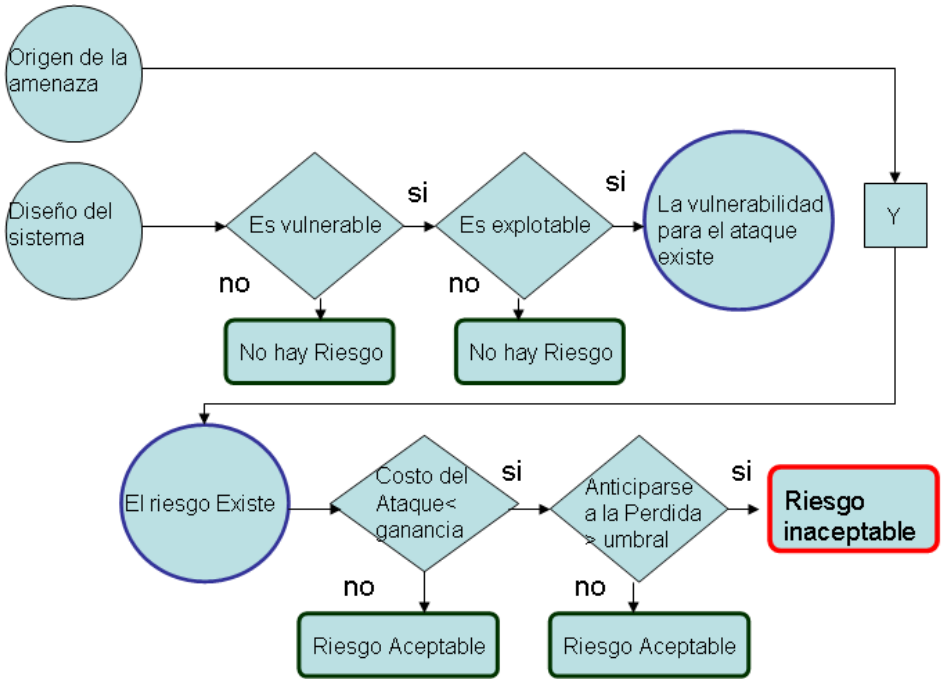

Figura 5 Puntos de acción para la mitigación de riesgos

Si el costo del ataque es mayor que la ganancia obtenida el riesgo puede considerarse aceptable, de otra forma habría que cuestionarse si la perdida anticipada es mayor que estar en el umbral (medidas emergentes por ejemplo DRP *Disaster Recovery Plan*) el riesgo es inaceptable de lo contrario, si la perdida anticipada representa un gasto menor (la criticidad del activo o los servicios prestados no son prioritarios para la misión) que estar en el umbral, el riesgo se le considera como un riesgo aceptable.

Esta estrategia es además articulada en las siguientes reglas, las cuales proveen una guía sobre las acciones para la mitigación de riesgos hacia amenazas humanas realizadas intencionalmente:

Cuando una vulnerabilidad (falla, debilidad) existe: implementación de técnicas que garanticen la reducción de la probabilidad para la vulnerabilidad siendo ésta ejercida.

Cuando una vulnerabilidad puede ser ejercida: aplicar capas protectoras, al diseño de la arquitectura, y a los controles administrativos para minimizar el riesgo o prevenir su ocurrencia.

Cuando el costo del ataque es menor que la ganancia potencial: aplicar protección para disminuir la motivación del ataque por el creciente costo de éste (por ejemplo usar los controles del sistema, como limitar los accesos de un usuario y que puedan reducir significativamente el beneficio obtenido por el atacante), es decir, los recursos para llevar a cabo el ataque son considerablemente altos en comparación al beneficio obtenido por perpetrar dicho ataque.

Cuando la pérdida es demasiado grande: aplicar principios de diseño, el diseño de la arquitectura, y protección técnica como no técnica para limitar la magnitud del ataque, reduciendo así el potencial de la perdida.

La estrategia señalada anteriormente con excepción del tercer elemento de la lista, Cuando el costo del ataque es menor que la ganancia potencial, también se aplica para la mitigación de riesgos derivados del ambiente o amenazas humanas involuntarias (por ejemplo errores en el sistema o los usuarios). Ya que no puede considerarse un atacante debido a que no hay ganancia o motivación.

2.4.3. Enfoque para la Implementación de Controles

Cuando las medidas de control deben adoptarse, aplican lo siguiente:

Dirigirse hacia los riesgos más importantes y esforzarse por mitigar lo suficiente los riesgos al menor costo posible, con un mínimo impacto en las otras capacidades de la misión.

La siguiente metodología para la mitigación de riesgos describe un enfoque para la implementación de controles.

- **Paso 1. Priorizar acciones**

  Basándose en los niveles de riesgo presentados en el reporte de evaluación de riesgos, la implementación de acciones son priorizadas. En la designación de recursos, la prioridad superior debe darse a los casos de riesgo con un inaceptable índice de riesgo alto (por ejemplo un nivel de riesgo asignado como muy alto o alto). Estas vulnerabilidades con su respectiva amenaza

requerirán acciones correctivas inmediatas para proteger los intereses y misión de la organización.

A la salida de este paso se obtendrán las categorías de las acciones desde alto hasta bajo.

- **Paso 2. Evaluar las opciones en controles recomendados.**

Los controles recomendados en el proceso de evaluación de riesgos pueden no ser los más apropiado y factible para una determinada organización y el sistema de TI. Durante este paso la factibilidad (por ejemplo compatibilidad, aceptación por parte del usuario) y la efectividad (por ejemplo de acuerdo con la protección y el nivel de mitigación de riesgo) de las opciones de controles recomendados son analizadas. El objetivo es seleccionar las opciones de controles más apropiadas para minimizar el riesgo.

La salida de este paso es un listado de los controles factibles.

- **Paso 3. Conducir el análisis consto beneficio.**

Para auxiliar en la administración en la toma de decisiones y para identificar controles en un costo efectivo, se debe conducir un análisis de costo beneficio. Dicho análisis se retomará más adelante.

Al término de este paso se obtendrá un análisis costo-beneficio describiendo los costos y los beneficios de la implementación o no implementación de los controles.

- **Paso 4. Selección de controles.**

En base a los resultados del análisis de costo-beneficio, la administración determina la forma más rentable, en cuanto a los controles se refiere, para reducir los riesgos sobre la misión de la organización. Los controles seleccionados deben combinar lo técnico, operativo y lo administrativo en los elementos de control, para garantizar la seguridad adecuada en el sistema de TI y la organización. A la salida de este paso los controles están seleccionados.

- **Paso 5. asignación de responsabilidad.**

Las personas apropiadas (personal interno o la contratación externa de personal), quienes tienen los conocimientos técnicos adecuados y el conjunto de habilidades necesarias para aplicar los controles identificados, se les asigna la responsabilidad. La salida del paso 5, es un listado de la asignación de responsabilidades al personal competente.

- **Paso 6. Elaborar un plan de implementación para protección.**

Durante este paso, un plan de implementación para protección (o plan de acción) es desarrollado.

El plan debe, como un mínimo, contener la siguiente información:

- Riesgo (vulnerabilidad con su respectiva amenaza) y su asociado nivel de riesgo (documentado en el informe de evaluación de riesgos)
- Controles recomendados (documentado en el informe de evaluación de riesgos)
- Acciones priorizadas (con la prioridad dada para las cuestiones con muy alto y alto nivel de riesgo).
- Controles previstos seleccionados (determinado sobre la base de factibilidad, eficiencia, beneficios para la organización y costos).
- Recursos requeridos para la implementación de los controles previstos seleccionados.
- Lista de los grupos de personas organizados y el personal.
- Fecha de inicio para la implementación
- Fecha prevista para la finalización de la implementación
- Requerimientos de mantenimiento

El plan implementado para protección prioriza las acciones a implementarse y los proyectos desde la fecha de inicio hasta la fecha objetivo para la finalización de la implementación. Este plan ayudara y acelerará el proceso de mitigación de riesgos. Se muestra un ejemplo en forma de tabla de un plan implementado de protección.[28]

- **Paso 7. Implementación de controles seleccionados**

Dependiendo de determinada situación la implementación de controles puede disminuir el nivel de riesgo pero no eliminar el riesgo. Esto se denomina riesgo residual y será abordado más adelante. El producto de este paso se obtendrá el riesgo residual.

[28] Véase la Tabla Plan implementado para protección en el paso 7, Implementación de controles seleccionados.

Ejemplo de Plan implementado para Protección.

(1) Riesgo (Vulnerabilidad con su respectiva amenaza)	(2) Nivel de Riesgo	(3) Controles Recomendados	(4) Prioridad de las acciones	(5) Selección de Controles Planificados	(6) Recursos requeridos	(7) Responsable equipo/personas	(8) Fecha de inicio/Fecha de Fin	(9) Requerimientos de mantenimiento / Comentarios
Usuarios no autorizados pueden hacer un telnet hacia el servidor XYZ y escudriñar entre los archivos sensibles de la compañía utilizando el identificador de invitado (guest ID)	Alto	Rechazar el inicio de comunicación mediante el protocolo telnet No permitir "al mundo" acceso a los archivos sensibles de la compañía Desactivar el usuario invitado (guest ID) o asignar un password difícil de adivinar para esta cuenta	Alto	Rechazar el inicio de una comunicación mediante el protocolo telnet No permitir "al mundo" acceso a los archivos sensibles de la compañía Desactivar el usuario invitado (guest ID)	10 horas para reconfigurar y probar el sistema	Pablo García, administrador del servidor del sistema XYZ, Fernando López, administrador del *Firewall* del la compañía	1-9-2007 al 2-9-2007	Realizar una evaluación periódica de los sistemas de seguridad y probar, para garantizar la adecuada seguridad proporcionada para el servidor XYZ
: :								

Tabla 9 Plan implementado para protección

(1) El riesgo (vulnerabilidad con su respectiva amenaza) son producto del proceso de evaluación de riesgos.
(2) El nivel de riesgo asociado para cada riesgo identificado (vulnerabilidad con su respectiva amenaza) es la salida del proceso de evaluación de riesgos.
(3) Los controles recomendados son producto del proceso de evaluación de riesgos.
(4) La prioridad de las acciones es determinada en base a los niveles de riesgo y los recursos disponibles (por ejemplo fondos, personas, tecnología).
(5) Planificación de los controles seleccionados de la implementación de dichos controles
(6) Recursos requeridos para la implementación de controles seleccionados previstos
(7) Lista de el grupo (grupos) y las personas que serán responsables de la implementación de los nuevos controles o el crecimiento de estos.
(8) Fecha de inicio y la fecha proyectada para finalización de la implementación de los nuevos controles o el crecimiento de estos.
(9) Requerimientos de mantenimiento para los nuevos controles o el crecimiento de estos después de la implementación.

La siguiente figura representa la metodología recomendada para la mitigación de riesgos.

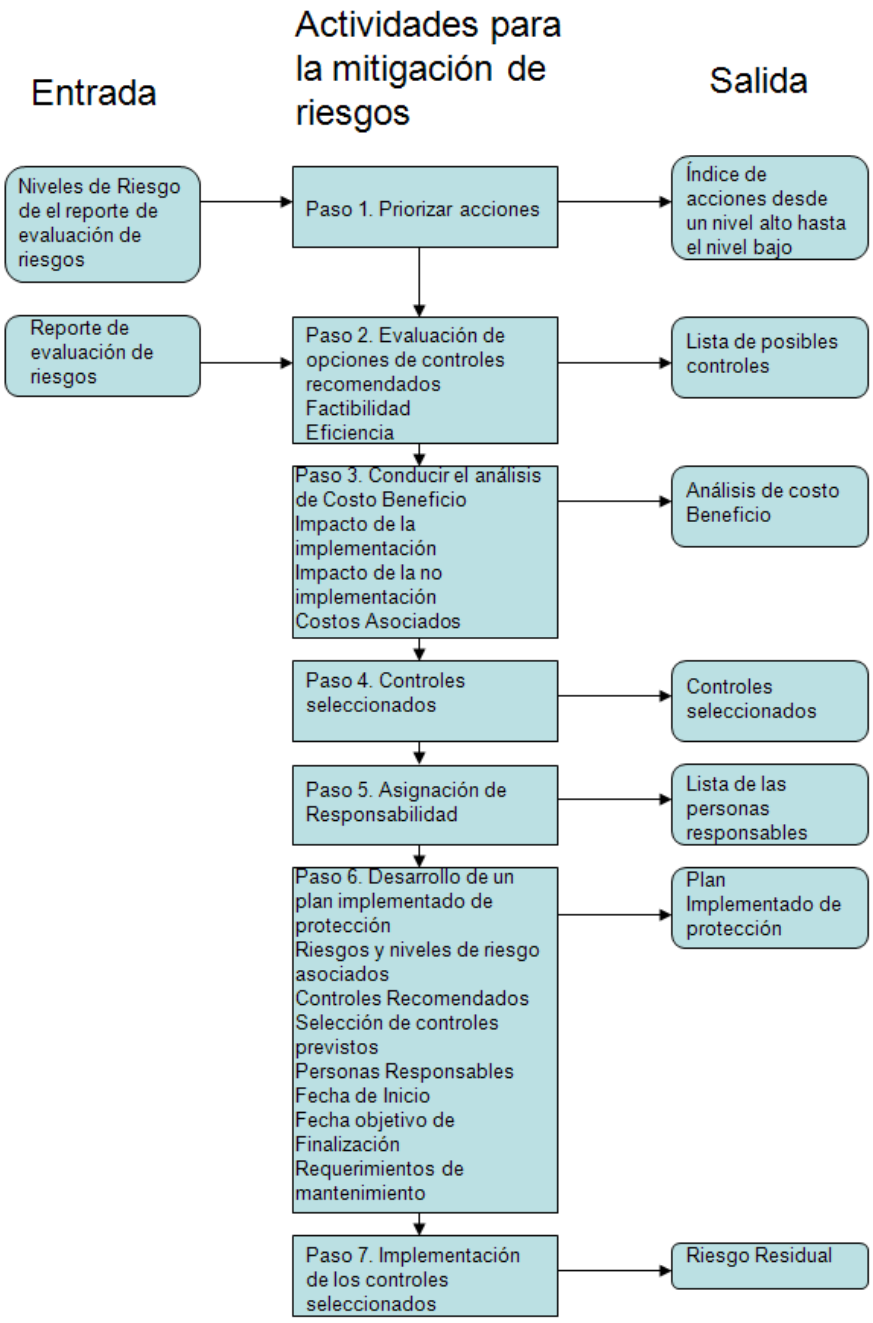

Figura 6 Diagrama de la metodología de mitigación de riesgos

2.4.4. Categorías de Control

En la implementación los controles recomendados para mitigar el riesgo, en una organización deben considerar la parte técnica, administrativa y operacional en los controles de seguridad o una combinación de tales controles, para maximizar la efectividad de los controles para sus sistemas de TI y la organización. Los controles

de seguridad cuando son utilizados apropiadamente, pueden prevenir, limitar o impedir el daño de la fuente de una amenaza en la misión de la organización.

El proceso de recomendación de controles incluirá la elección entre una combinación de controles operacionales, técnicos y administrativos para mejorar la postura de seguridad de la organización. Las compensaciones que una organización tendrán, para considerar sus decisiones, vistas, de una forma ilustrada, involucrarán el imponer la utilización de contraseñas complejas para minimizar el riego de que las adivinen, las rompan o *crackeen*. En este caso los controles técnicos requeridos se adhieren en el *software* de seguridad esto puede ser más complejo y caro que un procedimiento de control, pero el control técnico puede ser más eficaz. Por otra parte, un procedimiento de control puede ser implementado de una manera simple con un memorando a todas las personas afectadas y una modificación de las directrices de seguridad de la organización, pero el garantizar que los usuarios sigan de manera consistente el memorando y las directrices será difícil y requerirá concientizarlos, en lo que a seguridad se refiere, mediante la capacitación y aceptación por parte de los usuarios.

2.4.4.1. Controles Técnicos de Seguridad

Los controles de seguridad técnicos para la mitigación de riesgos pueden ser configurados para proteger contra cualquier tipo de amenaza. Estos controles pueden tener un rango de medidas, simples a complejas y usualmente involucran arquitectura de sistemas; disciplinas de ingeniería; y paquetes de seguridad con una combinación de *hardware, software y firmware*. Todas estas medidas deben trabajar juntas, para asegurar la criticidad y seguridad de los datos, la información y las funciones de los sistemas de TI, los controles técnicos pueden ser agrupados dentro de las siguientes categorías consideradas según el propósito primario:

i. Soporte. El apoyo de los controles es genérico y debe subrayar las capacidades de seguridad. Estos controles deben ser puestos en un orden para implementar otros controles.

ii. Prevención. Los controles preventivos se enfocan en la prevención sobre las brechas de seguridad desde su ocurrencia, en primer lugar, como por ejemplo, el transigir o consentir en parte con lo que no se cree justo, razonable o verdadero, a fin de acabar con una diferencia en este caso con respecto a la privacidad.

iii. Detección y recuperación. Estos controles se enfocan en detectar y recuperarse de una brecha de seguridad.

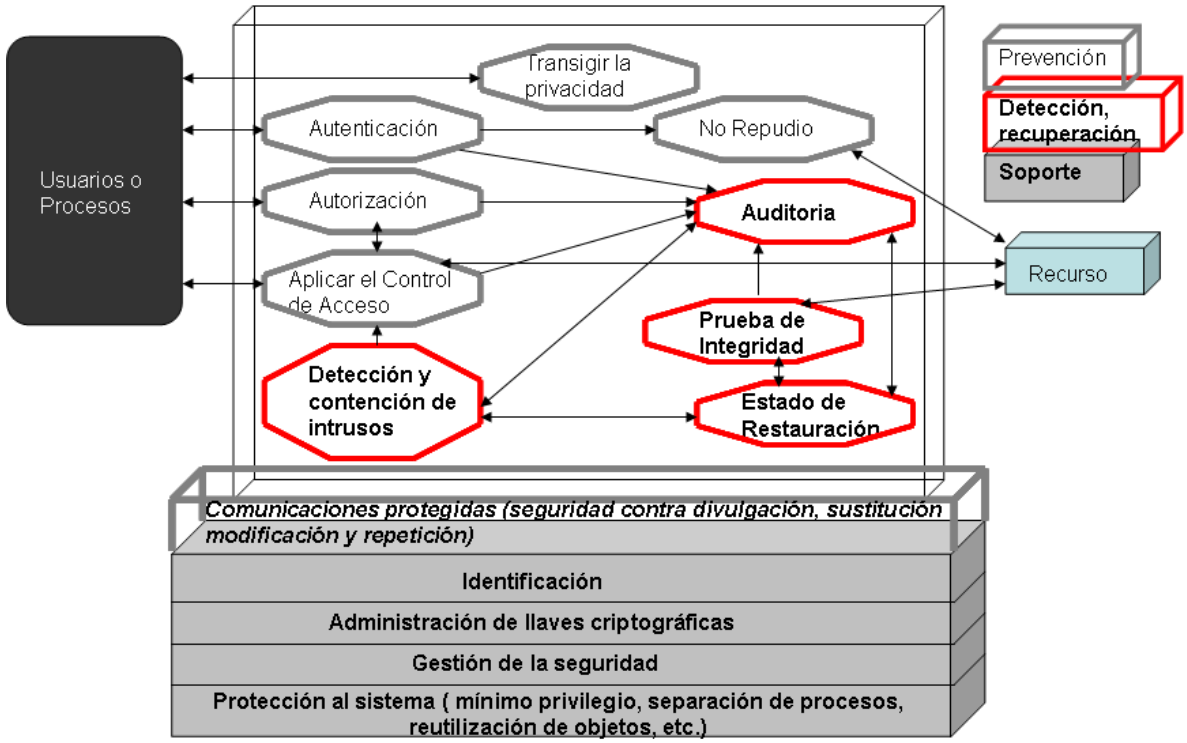

Figura 7 Controles técnicos de seguridad

2.4.4.2. Soporte a los Controles Técnicos de la Seguridad

El apoyo a los controles es, por su propia naturaleza, dominante e interrelacionado con otros controles. El soporte a los controles está como sigue:

Identificación. Estos controles proporciona la capacidad para identificar de forma única a usuarios, procesos, y recursos informáticos. Para implementar otros controles de seguridad (por ejemplo: Control de Acceso Discrecional[29] [21] (pp. 49) [DAC], control de Acceso Mandatario [30] [22] (pp. 45) [MAC], confiabilidad[31]), es esencial para ser identificados ambos, tanto objetos como sujetos.

Administración de llaves criptográficas. Las llaves criptográficas deben ser administradas con seguridad cuando las funciones criptográficas son implementadas en diversos controles. La administración de llaves criptográficas incluye la generación de llaves, distribución, almacenamiento y mantenimiento.

[29] Control de Acceso Discrecional o DAC por sus siglas en ingles, el usuario que desarrolla, adquiere u obtiene un archivo (programa, aplicación dispositivo, etc.) se considera como su dueño, y como tal es el único con la capacidad de asignar derechos sobre el archivo para otros usuarios.
[30] Control de Acceso Mandatario u Obligatorio también denominado MAC por sus siglas en ingles, los usuarios reciben un nivel de autorización de acceso y la información se clasifica según su sensibilidad. Estos dos parámetros se combinan para crear Clases de Acceso.
[31] La confiabilidad o también el seguimiento de sesión con la finalidad de responsabilizar y rendir cuenta de los recursos correctamente utilizados.

Gestión de la seguridad. Las características de seguridad para un sistema de TI deben ser configuradas (por ejemplo habilitarse o deshabilitarse características) para satisfacer las necesidades de una determinada instalación y dar cuenta de los cambios en el entorno operacional. La seguridad del sistema puede ser construida dentro del sistema operativo o la aplicación. Los productos de seguridad comerciales, desde adiciones por parte de un fabricante y de los productos de seguridad disponibles.

Sistemas de protección. El fundamento de un sistema de seguridad con diversas capacidades funcionales es la confianza, en base a la implementación técnica. Esto representa la calidad de la implementación desde la perspectiva del diseño de procesos utilizado y de la manera en la cual la implementación fue realizada. Algunos ejemplos de sistemas de protección son: la protección de información residual (también conocidos como objetos de rehúso), mínimo privilegio (o lo que necesitas saber), separación de procesos, modularidad, implementación de modelos de capas, y la minimización de los requerimientos que son de confianza.

2.4.4.3. Controles Técnicos Preventivos

Estos controles que pueden inhibir intentos de violación de políticas de seguridad incluyen lo siguiente:

Autenticación. La autenticación es un control que provee la manera de verificar la identidad de un sujeto para asegurar que la identidad declarada es valida. Los mecanismos de autenticación incluyen contraseñas (*passwords*), números de identificación personal, o PIN's, por sus siglas en ingles, y tecnología de autenticación emergente, que provee una robusta autenticación (por ejemplo *tokens*[32] [23], tarjeras inteligentes[33] [24] (*smart cards*), certificados digitales[34] [25](pp. 55), Kerberos[35] [26])

[32] Token es un unico identificador el cual es generado y enviado desde un servidor a un software cliente para identificar una interacción, también denominada sesión *token*. Los *tokens* denominados de seguridad, también conocidos como *tokens* en *hardware*, *token* para autenticación o *token* criptográfico, es un dispositivo fisico que un usuario autorizado de los servicios de computo se le da para auxiliar en el proceso de autenticación. En cuanto al *token* de acceso, se refiere a un objeto del sistema representando al sujeto a las operaciones de control de acceso.

[33] Tarjeta inteligente, tarjeta con chip o tarjeta con un circuito integrado (ICC *integrated circuit card*) es definido como una tarjeta de bolsillo con un circuito integrado incrustado el cual puede procesar información. Esto indica que puede recibir entradas que se procesa, por medio de la solicitud en la aplicación de la tarjeta con el circuito integrado (ICC), y entregado como una salida. Las tarjetas de memoria contiene únicamente memoria no volátil, la memoria que almacena los componentes, y algunos periféricos específicos para la seguridad lógica. Las tarjetas con microprocesador contienen memoria volátil y componentes de microprocesador. Las tarjetas inteligentes son normalmente hechas de plástico, PVC, la tarjeta presenta también en algunos casos un holograma que impide la falsificación.

[34] Certificado digital, en criptografía llave publica certificada, es un identificador que contiene información de su propietario, es decir, estos certificados relacionan la llave pública con algunos de sus atributos. Es avalado por una tercera entidad confiable. Su autenticidad es garantizada por el hecho que solo un organismo oficial puede expedirlo, utilizado para transacciones electrónicas.

Autorización. Los controles de autorización habilitan especificaciones y posterior administración de las acciones permitidas (por ejemplo el propietario de la información o el administrador de la base de datos que determina quien puede actualizar un archivo compartido por un grupo de usuarios en línea)

Aplicar el control de acceso. La integridad de los datos y confidencialidad son aplicados por controles de acceso. Cuando un sujeto requiere acceso tiene que estar autorizado para acceder a un proceso en particular, esto es necesario para aplicar lo definido en la política de seguridad (por ejemplo MAC o DAC). Estas políticas basadas en controles son aplicadas vía mecanismos de control de acceso distribuidos a través del sistema (por ejemplo etiquetas de sensibilidad correspondientes a un MAC; DAC para permisos de grupos de archivos, listas de control de acceso, roles RBAC[36], perfiles de usuarios)

La efectividad y fortaleza del control de acceso, depende de las correctas decisiones del control de acceso (por ejemplo como las reglas de seguridad que están configuradas) y la fortaleza de la aplicación de control de acceso (por ejemplo el diseño de *software* y *hardware* de seguridad).

No repudio. Los sistemas de seguimiento de sesión, también llamados de responsabilización sobre la utilización de los recursos del sistema, dependen de la habilidad de asegurar que los remitentes no pueden negar el envío de esta información y que los receptores no pueden negar el haberla recibido. El no repudio abarca tanto la prevención como la detección. Esta situado en la categoría de prevención (como se muestra en la figura anterior), debido a que la aplicación de mecanismos impide que se concrete una acción repudiada (por ejemplo la utilización de certificados digitales que contienen una transformación realizada con la llave privada de una autoridad certificadora y que avala al firmante, que ostenta el certificado, cuando este realiza una transformación con su respectiva llave privada que es conocida, únicamente, por el firmante). Como resultado estos controles son típicamente aplicados en el punto de transmisión y recepción.

Comunicaciones protegidas. En un sistema distribuido, la capacidad de cumplimiento de los objetivos de seguridad es altamente dependiente de una

---

[35] Kerberos es el nombre de un protocolo de autenticación en redes de computadoras, el cual permite comunicaciones individuales sobre redes no seguras, probando su identidad de manera segura. Esto es también una suite de software libre del MIT que implementa este protocolo. Este diseñado con el propósito del modelo cliente servidor y proveyendo una autenticación mutua, ambos el usuario y el servidor verifican la identidad del otro, los mensajes del protocolo Kerberos son protegidos contra los ataques de replicación e intercepción o escucha. Kerberos se basa en criptografía de llave simétrica y requiere una tercera parte confiable Extensiones de Kerberos puede prever el uso de la criptografía de clave pública durante ciertas fases de la autenticación.

[36] RBAC por sus siglas en ingles *Role Based Access Control*, control de acceso basado en roles, se basa en tres aspectos. Grupos y usuarios, roles donde los usuarios y grupos son asignados y privilegios, los atributos de cada rol o capacidades de acceso la granularidad de este control de acceso permite asignar un grupo de privilegios característicos de un rol y otros mas específicos con el objetivo del menor privilegio.

comunicación fidedigna. Los controles de comunicaciones protegidas garantizan la integridad, disponibilidad y confidencialidad de información sensible y critica mientras esta en transición. La protección de comunicaciones utiliza métodos de cifrado de datos (ejemplo VPN, Redes Privadas Virtuales, por sus siglas en ingles *Virtual Private Network*, IPSEC, protocolos de ip seguros); y desarrollo de tecnologías criptográficas (por ejemplo AES, 3DES, SHA-1), para minimizar las amenazas en redes como son repetición, intercepción, husmeo de paquetes, el monitoreo de conversaciones en la red por una tercera parte no deseada.

Transigir la privacidad.

Tanto el gobierno como el sector privado están requiriendo cada vez más el mantener la privacidad. Los controles para transigir la privacía, es decir, la protección durante la transacción (por ejemplo SSL *Secure Socket Layer*[37], SSH, *Secure Shell*[38]), protegen en contra de la perdida de la privacidad, con respecto a las transacciones realizadas por un particular.

2.4.4.4. Controles Técnicos de Detección y Recuperación

Los controles de detección advierten de violaciones o intentos de violación de las políticas de seguridad, incluye tales controles como el seguimiento con fines de auditoria, métodos de detección de intrusos, entre otros. Los controles de recuperación pueden ser usados para restaurar recursos de cómputo perdidos. Estos son necesarios como un complemento para soporte y prevención de medidas técnicas, ya que ninguna de las medidas en estas otras áreas es perfecta. Los controles de detección y recuperación incluyen:

Auditoria. La auditoria de eventos relevantes de seguridad y el monitoreo y seguimiento de anormalidades en el sistema son elementos claves en la detección de un hecho posterior y la recuperación de brechas de seguridad.

Detección y contención de intrusos. Es esencial para detectar brechas de seguridad (por ejemplo actividades sospechosas) de modo que puede producirse una respuesta a tiempo. También para detectar brechas de seguridad, pero si no hay una repuesta efectiva es de poca utilidad. Los controles de detección y contención de intrusos proveen estas dos capacidades.

Prueba de Integridad. Los controles que prueban la integridad (por ejemplo herramientas de integridad del sistema) analizan la integridad del sistema y las irregularidades, además de identificar las exposiciones y las amenazas potenciales. Estos controles no previenen violaciones en las políticas de seguridad pero las detectan y auxilian a determinar el tipo acciones correctivas necesarias.

---

[37] Secure Socket Layer es un protocolo criptográfico que provee comunicaciones seguras en una red, como Internet, para aspectos como la navegación Web, el correo electrónico, mensajes instantáneos (*messenger*) y otros datos transferidos.

[38] SSH es un protocolo de red que permite el intercambio de datos entre dos computadores sobre un canal seguro. SSH utiliza criptografía de llave pública para autenticarse con la computadora remota y permitir a la computadora remota autenticar a l usuario si es necesario.

Estado de restauración a un estado seguro. Este servicio habilita a un sistema para regresar a un estado conocido como seguro, después de que una brecha de seguridad ocurre.

Detección y erradicación de virus. El software de detección y erradicación de virus que son instalados en un servidor y el usuario de la estación de trabajo que detecta, identifican y remueve para asegurar la integridad de los datos del sistema.

2.4.4.5. Gestíón de Controles de Seguridad

La gestión de controles de seguridad, en conjunto con los controles técnicos y operacionales, es implementada para administrar y reducir el riesgo de pérdida y proteger la misión de la organización. La gestión de controles se enfoca en lo estipulado en la política de protección de la información, además de sus directrices y normas, que se llevan acabo a través de procedimientos operacionales, para cumplir los objetivos y misión de la organización.

2.4.4.6. Gestión de Controles de Seguridad Preventivos

Estos controles incluyen lo siguiente:

- Asignar a los responsables de la seguridad para garantizar que se proporciona la seguridad adecuada para la misión critica de los sistemas de TI.
- Desarrollar y mantener el plan de sistema de seguridad para documentar los controles actuales y dirigir los controles previstos en los sistemas de TI, apoyando la misión de la organización.
- Implementar controles de seguridad de personal, incluyendo la separación de funciones, el mínimo privilegio, y los usuarios del equipo de cómputo, mediante el registro de acceso y terminación.
- Conducta de concientización sobre la seguridad y la capacitación técnica, para garantizar que el usuario final y los usuarios del sistema estén concientes de las reglas de comportamiento y su responsabilidad en la protección de la misión de la organización.

2.4.4.7. Gestión de Controles de Seguridad de Detección

La gestión de controles de detección es como sigue:

- Implementación de controles de seguridad personal, incluyendo personal de limpieza, investigación de antecedentes, rotación de funciones
- Realizar revisiones periódicas de los controles de seguridad para garantizar que los controles son efectivos
- Llevar a cabo auditorias periódicas al sistema

- Realizar la administración de riesgos en curso de la evaluación y mitigación de los riesgos
- Autorizar a los sistemas de TI para dirigir y aceptar el riesgo residual

2.4.4.8. Gestión de Controles de Seguridad de Recuperación

Estos controles incluyen lo siguiente:

- Proveer continuidad de soporte y desarrollo, evaluación y mantenimiento del plan de continuidad de las operaciones para la reanudación del negocio y asegurar la continuidad de operaciones durante emergencias o desastres.
- Establecer una capacidad de respuesta a incidentes, para preparar, reconocer, reportar y responder al incidente con la finalidad de devolver al sistema a un estado operacional.

2.4.4.9. Controles de Seguridad Operacional

Las normas de seguridad de una organización deben establecer un conjunto de controles y directrices para asegurar que los procedimientos de seguridad que rigen el uso de los activos y recursos de TI de la organización se llevan a cabo correctamente, de acuerdo con la misión y objetivos de la organización. La administración desempeña un papel fundamental en la implementación supervisada de la política, asegurando así, el establecimiento de controles apropiados.

Los controles operacionales, implementados de acuerdo a una base conjunta de requerimientos (por ejemplo controles técnicos) y las buenas prácticas de la industria, son utilizados para corregir deficiencias operacionales que pueden llevar al origen de una amenaza potencial, esto ,para asegurar la consistencia y uniformidad en la seguridad de las operaciones. Los procedimientos y métodos para la aplicación de controles operacionales deben de estar claramente definidos, documentados paso a paso y además de mantenerse.

Los controles de seguridad operacional incluyen; los presentados a continuación en los apartados de: Controles operacionales de prevención y controles operacionales de detección.

2.4.4.10. Controles Operacionales de Prevención

Los controles operacionales de prevención son:

- Control de acceso a medios de datos (CD-ROM, cintas, discos duros, entre otros) y su eliminación (por ejemplo control de acceso físico, métodos de *degaussing*[39] [27])
- Límite de distribución de datos externos (por ejemplo el uso de etiquetado)
- Software de control de virus
- Garantizar protección al equipo de computo (por ejemplo guardias de seguridad, procedimiento para los visitantes en sitio, sistema de identificación electrónico, control de acceso biométrico, administración y control de cerraduras y llaves, barreras y vayas)
- Asegurar los armarios donde se encuentra la instalación eléctrica, los equipos de interconexión (*swithches, routers*, entre otros) y el cableado.
- Proporcionar capacidad de respaldo (por ejemplo procedimientos para un respaldo regular de datos y del sistema) archivo de los registros (*logs*) de la base de datos que guardará todos los cambios utilizados en varios escenarios de recuperación).
- Establecer el almacenamiento fuera de sitio y la seguridad
- Protección de portátiles (laptops), computadoras personales (PC), estaciones de trabajo.
- Protección a los activos de TI de daños por incendio (por ejemplo, los requisitos y procedimientos para la utilización de extintores de incendios, lonas, sistemas de rociadores en seco).
- Proporcionar fuentes de energía eléctrica de emergencia (por ejemplo, las necesidades de suministros de energía ininterrumpibles, generadores de potencia en sitio).
- Control de humedad y temperatura de la instalación del equipo de cómputo (por ejemplo el funcionamiento de aire acondicionado, disipadores de calor).

2.4.4.11. Controles Operacionales de Detección

Los controles operacionales de control incluyen lo siguiente:

- Proporcionar seguridad física (por ejemplo el uso de detectores de movimiento, cámaras de vigilancia o circuito cerrado de vigilancia, sensores y alarmas)

[39] Degaussing (borrado seguro) es el proceso de disminuir o eliminar un comportamiento no deseado en un campo magnético. Lleva el nombre de Carl Friedrich Gauss, uno de los primeros investigadores en el campo del magnetismo. Debido a la histéresis magnética, generalmente no es posible reducir un campo magnético completamente a cero, de modo degaussing normalmente inducido por un muy pequeño, pero conocido, campo magnético.

- Asegurar la seguridad ambiental (por ejemplo el uso de detectores de humo y detectores de incendio, sensores y alarmas).

2.4.4.12. Análisis Costo- Beneficio

Para asignar los recursos en función de los costos y aplicar medidas eficaces de control, las organizaciones, después de la identificación de todos los controles posibles y la evaluación de su viabilidad y eficacia, debería realizar un análisis de costo-beneficio para cada propuesta de control para determinar qué controles son necesarios y apropiados para sus circunstancias.

El análisis de costos y beneficios puede ser cualitativo o cuantitativo. Su objetivo es demostrar que los costos de la aplicación de los controles pueden ser justificados por la reducción del nivel de riesgo. Por ejemplo la organización puede no querer gastar $1, 000,000 en un control para reducir un riego que costaría $20,000.

Un análisis costo- beneficio, para proponer nuevos controles o el crecimiento de los actuales, se compone de lo siguiente:

- Determinar el impacto de la implementación de nuevos controles o el incremento de estos.
- Determinar el impacto de la no aplicación de los nuevos controles o del crecimiento de los actuales
- Estimar el costo de la implementación esto puede incluir, pero no limitar a lo siguiente:
  - ✓ Comprar hardware y software
  - ✓ Reducir la efectividad operacional, si el rendimiento del sistema o su funcionalidad es reducida para aumentar la seguridad.
  - ✓ Costo de la aplicación de nuevas políticas y procedimientos
  - ✓ Costo de la contratación de personal adicional para aplicar las políticas, los procedimientos, o los servicios.
  - ✓ Gatos de capacitación
  - ✓ Costo del mantenimiento
- Evaluando los costos de implementación en contra de la criticidad del sistema y los datos para determinar la importancia para la organización la implementación de nuevos controles en vista de sus costos y del impacto relacionado.

La organización tendrá que evaluar los beneficios de los controles en términos de mantener una postura aceptable de la misión de la organización; del mismo modo evaluar el costo de implementación de los controles necesarios. Lo relativo al costo

de la no implementación de los controles para la misión, determinarán en si es factible renunciar a su aplicación.

Ejemplo de un Análisis Costo-Beneficio (se explica a continuacióny se trata de un caso ficticio): El sistema X almacena y procesa información crítica para la misión, además de información de carácter privada, sensible, relacionada con los empleados; sin embargo, la auditoria del sistema no se ha habilitado (*logs*, bitácoras). Un análisis de costos se realiza para determinar si la función de auditoria debe estar habilitada para el sistema X.

Los puntos siguientes (1), (2) abordan el impacto intangible (por ejemplo factores de disuasión) para la aplicación o la no aplicación de los nuevos controles. El punto (3) es una lista de los activos tangibles (por ejemplo el costo actual)

(1) El impacto de habilitar la característica de auditoria del sistema: La característica de auditoria del sistema permite al administrador de seguridad del sistema monitorear las actividades de los usuarios, pero alentará al sistema y su rendimiento, por lo tanto afectará la productividad de los usuarios. También la implementación, de la auditoría en el sistema, requerirá recursos adicionales como los descritos en el punto (3).

(2) El impacto de no habilitar la característica de auditoria del sistema: Las actividades de los usuarios de sistema y las violaciones pueden no ser monitoreadas o rastreadas, si la función de auditoria del sistema está deshabilitada y la seguridad no puede ser maximizada para proteger los datos confidenciales de la organización y la misión.

(3) El costo estimado por habilitar la característica de auditoria del sistema:

Costo por habilitar la característica de auditoria del sistema- No tiene costo la característica esta incorporada
$0
Personal adicional para realizar la revisión de auditoria y el archivo, por año
$xx, xxx
Capacitación (por ejemplo capacitación del sistema de auditoria, generación de reportes)
$x, xxx
Auditoria del mantenimiento de datos (por ejemplo almacenarlos y archivarlos), por año
$x, xxx
Añadir software que presente reportes de auditoria.
$x, xxx
El costo total estimado
$xx, xxx

Tabla 10 Costos auditoria del sistema

Los administradores de la organización deben determinar que constituye un nivel

aceptable de riesgo con respecto a la misión. El impacto de un control puede ser evaluado, y el control, ya sea incluido o excluido, será determinado por la organización posteriormente, mediante un rango de los niveles de riesgo posible. Este rango puede variar entre las organizaciones; sin embargo las siguientes reglas se aplican para determinar el uso de nuevos controles:

- Si el control, reducirá el riesgo más de lo necesario, entonces encontrar si existe una alternativa menos cara.
- Si el control costaría más que la reducción de los riesgos previstos, entonces encontrar algo más.
- Si el control no reduce suficientemente los riesgos, entonces busque más controles o controles diferentes.
- Si el control proporciona la reducción del riesgo de manera suficiente y es eficaz en función del costo, entonces hay que utilizarlo.

Frecuentemente el costo de implementación de un control es más tangible que el costo de no aplicarlo. Como resultado de ello, el administrador representa un papel fundamental en las decisiones relativas a la implementación de medidas de control para proteger la misión de la organización.

2.4.4.13. Riesgo Residual

Las organizaciones pueden analizar la extensión de la reducción de riesgos generada por los nuevos controles o el incremento de estos, en términos de reducir la probabilidad de **amenaza** o el **impacto**, ambos parámetros definen el nivel de riesgo mitigado sobre la misión de la organización.

La implementación de nuevos controles o el incremento de estos puede mitigar el riesgo por:

- ✓ La eliminación de algunas de las vulnerabilidades del sistema (fallas y debilidades), lo que redujo el número de posibles vulnerabilidades con su respectivo origen de amenaza.
- ✓ Agregar un control dirigido a reducir la capacidad y la motivación del origen de una amenaza. Por ejemplo, un departamento determina que el costo por instalación y mantenimiento de aditamentos de software de seguridad para PC *Stand-alone* que almacenan archivos sensitivos no es justificado, pero que los controles administrativos y físicos deben aplicarse, para que el control de acceso físico a la PC sea mas difícil (por ejemplo almacenar las computadoras personales, PCs, en una habitación bajo llave en custodia del administrador).
- ✓ Reducir la magnitud de los efectos adversos (por ejemplo limitar el alcance de una vulnerabilidad o modificar la naturaleza de la relación entre el sistema de TI y la misión de la organización).

La relación entre la implementación de controles y el riesgo residual se representa gráficamente a continuación.

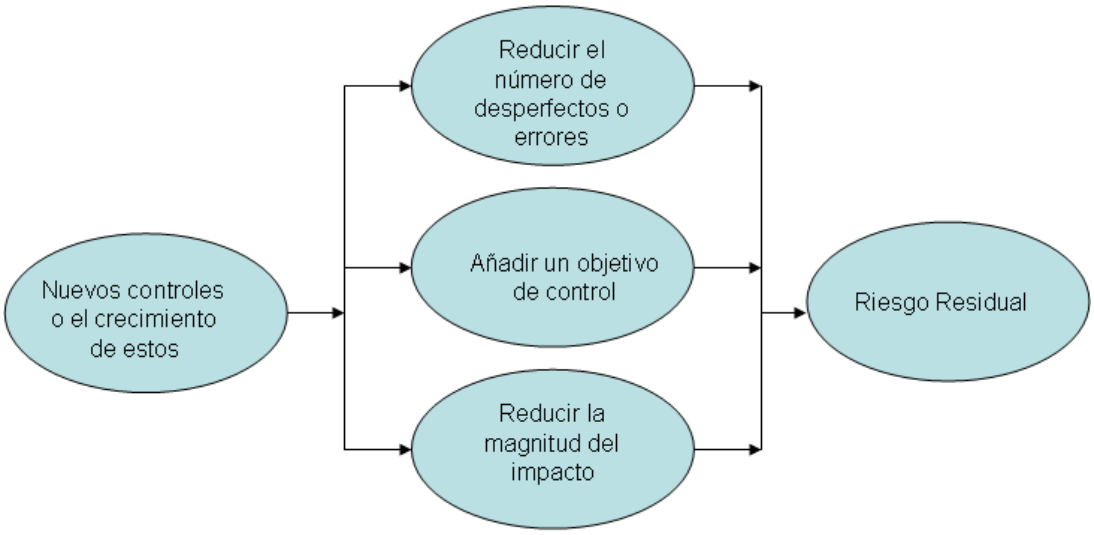

Figura 8 Controles implementados y el riesgo residual

El riesgo que quede después de la implementación de nuevos controles o el crecimiento de estos es el riego residual.

Prácticamente un sistema de TI no está libre de riesgos y no todos los controles implementados pueden eliminar el riesgo que estos pretenden resolver o reducirlo a cero.

Una organización desde la alta dirección, es decir, mediante la autorización de una autoridad Designada (DAA[40]), que es responsable de la protección de la organización y la misión de activos de TI, debe permitir (o acreditar) al sistema informático iniciar o continuar funcionando. Esta autorización o acreditación se deberá realizar por lo menos cada 3 años o cuando se realizan cambios importantes al sistema de TI. La intención de este proceso es identificar los riesgos que no están totalmente dirigidos y determinar si se necesitan controles adicionales para mitigar los riesgos identificados en el sistema de TI. Para las agencias federales, después de los controles se han puesto en marcha para los riesgos identificados, la DAA firmará una declaración para aceptar cualquier riesgo residual y autorizar el funcionamiento del nuevo sistema informático o de la continuación de la tramitación del actual sistema de TI. Si el riesgo residual no se ha reducido a un nivel aceptable, el ciclo de administración del riesgo debe repetirse para identificar una manera de reducir el riesgo residual a un nivel aceptable. [28](pp. 40)

[40] *The Designated Approving Authority*, DAA por sus silgas en ingles, en el Departamento de Defensa de los estados unidos, es el funcionario con autoridad para asumir oficialmente la responsabilidad de la explotación de un sistema a un nivel aceptable de riesgo.

2.5. Evaluación y Estimación

En la mayoría de las organizaciones, la red propia, continuamente es ampliada y actualizada, sus componentes han cambiado, sus aplicaciones de software se han remplazado o actualizado con nuevas versiones. Además, se producirán cambios en el personal y las políticas de seguridad con el tiempo.

Estos cambios significan que nuevos riesgos aparecerán y los riesgos previamente mitigados pueden convertirse en una preocupación. Por lo tanto, el proceso de administración de riesgos está en curso y evolucionando.

En esta sección se hace hincapié en las buenas prácticas y la necesidad de un curso de evaluación de los riesgos además de la estimación y los factores que conducen al éxito del programa de administración de riesgos.

2.5.1. Buenas Prácticas de Seguridad

El proceso de evaluación de riesgos es repetido, usualmente, por lo menos cada tres años para los organismos federales[41]. Sin embargo la administración de riesgos debe ser dirigida e integrada en el SDLC (*System Developer Life Cycle*) para los sistemas de TI, no porque esto sea requerido por las leyes o las regulaciones, si no es considerado una buena práctica y soporte para los beneficios de negocio o misión de la organización.

Debería establecerse un calendario para la evaluación y mitigación de riesgos de la misión, pero mediante procesos periódicamente efectuados, deben ser también flexibles para permitir cambios cuando estos sean justificados tales como cambios importantes y cambios en el procesamiento ambiental del sistema de TI ambos resultando en modificación de las políticas y nuevas tecnologías.

En este capítulo se explicó una metodología de análisis y administración de riesgos, en el capítulo siguiente se integran varios de los conceptos explicados, en está capítulo, con un enfoque relacionado a la organización en base a su misión y objetivos y la infraestructura que soportan a éstos, utilizando ITIL, buenas prácticas, y la Administración de Servicios enfocados al Negocio.

[41] Como está dispuesto por la circular de la OMB A- 130 para mayor información con respecto a este organismo de los Estados Unidos de América y más precisamente esta circular revisar el link: http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html

Referencias Capítulo 2

[1]*Robert Richardson* **CSI Survey 2007 The 12th Annual Computer Crime and Security survey** P.13 Computer Security Institute 2007.

[2]*Robert Richardson* **CSI Survey 2007 The 12th Annual Computer Crime and Security survey** P.15 Computer Security Institute 2007.

[3]*Gary Stoneburner, Alice Goguen, and Alexis Feringa* "**Risk Management Guide for Information Technology systems Recommendations for the National Institute of Standars and Technology NIST SP 800-30"** p. 8 July 2002. Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930

[4] *Romero E. Alfonso Et al.* "**Cracker"**. Wikipedia la enciclopedia ibre. Disponible en: http://es.wikipedia.org/wiki/Cracker Leído el 16 Octubre 2007.

[5]*Sánchez Alejandro Et a*l. **"Hacker. Hacker vs Cracker".** Wikipedia la enciclopedía Libre Disponible en: http://es.wikipedia.org/wiki/Hacker Leído el 16 Octubre 2007.

[6] *Nonualco Pedro Et al*. "**Ingeniería Social"** Wikipedia la enciclopedia Libre. Disponible en: http://es.wikipedia.org/wiki/Ingenier%C3%ADa_social_(seguridad_inform%C3%A1tica) Leído el 16 Octubre 2007.

[7]*Farmbrough Rich Et al*. **"Information warfare"** from Wikipedia, the free encyclopedia Disponible en: http://en.wikipedia.org/wiki/Information_warfare Leído el 16 Octubre 2007.

[8]*Goldberg Ivan* **"K.GLOSSARY OF INFORMATION WARFARE TERMS"**
Disponible en: http://www.psycom.net/iwar.2.html Leído el 16 Octubre 2007.
Damiman Ached Et al. **"Botnet"**. Disponible en: http://es.wikipedia.org/wiki/Botnet Leído el 16 Octubre 2007.
Park Chong-Dae Et al. **"Denial-of Service-Attack"** form Wikipedia, the free encyplopedia Disponible en: http://en.wikipedia.org/wiki/DDOS Leído el 16 Octubre 2007.
Damiman Ached Et al. **"Malware"** Wikipedia la Enciclopedia Libre Disponible en: http://es.wikipedia.org/wiki/Malware Leído el 16 Octubre 2007.

[9] *Wikipedia la Enciclopedia Libre.* **"Virus informático"**. Disponible en: http://es.wikipedia.org/wiki/Virus_informatico Leído el 16 Octubre 2007.

[10] *Villalón Antonio.* **"Bombas lógicas"**. Disponible en: http://es.tldp.org/Manuales-LuCAS/SEGUNIX/unixsec-2.1-html/node77.html Leído el 16 Octubre 2007.

[11] *Gary Stoneburner, Alice Goguen, and Alexis Feringa*. **"Risk Management Guide for Information Technology systems Recommendations for the National Institute of Standars and Technology NIST SP 800-30"** p. 15 July 2002. Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930

[12] *RAD COM Academy* **"TELNET"** Disponible en: http://www.protocols.com/pbook/tcpip9.htm#TELNET Leído el 17 Octubre 2007.

[13]*Quiggin Jonh Et al.* **"White paper"** from Wikipedia, the free encyclopedia. Disponible en: http://en.wikipedia.org/wiki/White_paper Leído el 17 Octubre 2007.

[14] Wikipedia, the free enciclopedia. **"Operating system"** Disponible en: http://en.wikipedia.org/wiki/Operating_system Leído el 18 Octubre 2007.

[15] *Adams Michael Et al.* **"Service pack".** Wikipedia, the free encyclopedia Disponible en: http://en.wikipedia.org/wiki/Service_pack Leído el 18 Octubre 2007.

[16] *Wack John, Miles Tracy, Murugiah Souppaya* **"Guideline on Network Security Testing Recommendations of the National Institute of Standards and Technology Section 2-2 NIST Special Publication 800-42".** Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930 October 2003.

[17] *RAD COM Academy.* **"FTP"** Disponible en: http://www.protocols.com/pbook/tcpip7.htm Leído el 18 Octubre 2007.

[18] *Derksen Bryan Et al.* **"Designated Approving Authority"**. From Wikipedia, the free encyclopedia Disponible en: http://en.wikipedia.org/wiki/Designated_Approving_Authority Leído el 23 Octubre 2007.

[19] *Gary Stoneburner, Alice Goguen, and Alexis Feringa*. **"Risk Management Guide for Information Technology systems Recommendations for the National Institute of Standars and Technology NIST SP 800-30"** p. 27 July 2002. Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930

[20] *State University of New York Institute of Technology.* **"Preventive and detective controls"** Disponible en: http://www.sunyit.edu/internal_control/preventative_control.inc Leído el 24 Octubre 2007.

[21] *Daltabuit Enrique* 2004. **"Control de Acceso"**, p.49. En el módulo 5: Control de Acceso, del Diplomado de Seguridad Informática, Centro Educativo Multidisciplinario Polanco, México, D.F. 6 Diciembre 2004- 6 de Enero 2005. Centro Educativo Multidisciplinario Polanco, México, D.F.

[22] *Daltabuit Enrique* 2004. **"Control de Acceso"**, p.45. En el módulo 5: Control de Acceso, del Diplomado de Seguridad Informática, Centro Educativo Multidisciplinario Polanco, México, D.F. 6 Diciembre 2004- 6 de Enero 2005. Centro Educativo Multidisciplinario Polanco, México, D.F.

[23] *Macrakis Stavros, Et al*. **"Token Computing"** from Wikipedia the free encyclopedia Disponible en: http://en.wikipedia.org/wiki/Token Leído el 31 de Octubre 2007.

[24] *Li Andrew, et al.* **"Smart Card"** from wikipedia the free encyclopedia Disponible en: http://en.wikipedia.org/wiki/Smart_cards Leído el 31 octubre 2007.

[25] *Hernandez Leobardo, M Martinez.* 2004. "**Aplicaciones Criptográficas**", p.55. En el módulo 3: Aplicaciones Criptográficas, del Diplomado de Seguridad Informática, Centro Educativo Multidisciplinario Polanco, México, D.F. 3- 17 noviembre 2004. Centro Educativo Multidisciplinario Polanco, México, D.F.

[26] *Hartman Sam, et al*. "**Kerberos (protocol)"** from Wikipedia the free encyclopedia Disponible en: http://en.wikipedia.org/wiki/Kerberos_%28protocol%29 Leído el 30 octubre 2007.

[27] *Carré Lee, et al,* **"Degaussing"** from Wikipedia the free encyclopedia Disponible en: http://techfinder.businessweek.com/businessweek/search/browse/55083/55083.jsp Leído el 1 noviembre 2007. Peripheral Manufacturing. Inc. Computer/Hard Drive and Tape Degaussers &

Degaussing (Erasing) Service Disponible en: http://en.wikipedia.org/wiki/Degaussing Leido el 1 noviembre 2007.

[28] *Gary Stoneburner, Alice Goguen, and Alexis Feringa* **"Risk Management Guide for Information Technology systems Recommendations for the National Institute of Standars and Technology NIST SP 800-30"** p. 40 July 2002. Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930

Capítulo
3
Metodología ITIL/BSM

Resumen

ITIL® se fundamenta en un conjunto de buenas prácticas para la gestión de servicios y cómo éstos tiene relevancia para una organización, es decir cómo es que la interacción entre los procesos, las personas y los productos, refiriéndose a este último como las herramientas y la tecnología, se unen para afrontar los retos de una organización. Este marco de buenas prácticas pretende facilitar la entrega de servicios de TI, de alta calidad, mediante un conjunto de procedimientos de administración ideados con la finalidad de ayudar a las organizaciones a lograr calidad y eficiencia de las operaciones con tecnología de Información.
ITIL® es un conjunto de libros donde se encuentran documentados los procesos referentes a la provisión de servicios de Tecnología de Información hacia la organización. Estos procesos cubren una o más tareas relacionadas con el desarrollo del servicio, administración de infraestructura y soporte de servicios de TI entre otros.

ITIL® toma un proceso basado en el acercamiento para administrar y proveer servicios de TI; las actividades de las Tecnologías de la Información son divididas dentro de procesos, cada uno de los cuales tiene tres niveles:

- Estratégico: Los objetivos de una organización se determinan, junto con un esbozo o perfil de métodos para alcanzar los objetivos.
- Táctico: la estrategia se traduce a una estructura de organización apropiada y a los planes específicos que describan qué procesos tienen que ser ejecutados, qué activos tienen que ser desplegados, y cuáles son los resultados que los procesos deben dar.
- Operacional: Con esta perspectiva operacional se dice que:

  Se ejecutan los planes tácticos, además de que los objetivos estratégicos se alcanzan dentro del tiempo especificado.Estas mejores prácticas de Administración de servicios de TI (*IT Service Management-ITSM*[1]) pueden servir de guía para la mejora continua de las Tecnologías de Información independientemente de la estructura actual o nivel de madurez de la organización.

BSM[2] (*Business Service Management*) es un objetivo de los negocios, y una promesa del potencial de los proveedores. Un buen plan de Administración de Servicios del

[1] ITSM es una disciplina basada en procesos, enfocada en alinear los servicios de Tecnologías de Información proporcionados con las necesidades de las empresas, poniendo énfasis en los beneficios que puede percibir el cliente final, además propone cambiar el paradigma de gestión de TI, por una colección de componentes enfocados en servicios "end-to-end" usando distintos marcos de trabajo con las "mejores prácticas", como por ejemplo la Information Technology Infrastructure Library (ITIL) o el eSCM (*enabled Service Capability Model*).
[2] Forrester Research, Inc. define BSM como: Administración de Servicios de Negocio a los enlaces dinámicos de negocio enfocados en los servicios de TI sostenidos por la infraestructura Tecnológica. El enfoque de los negocios en los servicios de TI puede ser un servicio específico de estas

Negocio va más allá de los típicos estándares de Administración de las TI y el negocio; este:
"*fusiona los objetivos de las TI y el negocio. Una Plataforma de Administración de Servicios, en ingles Bussines Service Plataform (BSP), es el fundamento de una solución efectiva de BSM. Por emplear una solución de BSP, el negocio entero utiliza las herramientas que supervisan, divulgan, y manejan servicios de negocio. En adición la estrategia global incluye una poderosa relación mapeando el repositorio de datos como base a través de un plataforma robusta y versátil; Base de datos de Administración de la configuración, en inglés Configuration Management Data Base (CMDB). Últimamente, una BSP puede proporcionar la supervisión en tiempo real de la salud y del estado de los servicios del negocio.*"[1]

Las TI son un conjunto de herramientas diseñadas para ayudar a reunir a las organizaciones, sus objetivos corporativos y los objetivos del negocio. Sin importar la tecnología existente o las aplicaciones, es oportuno que los servicios provean la información necesaria inmediatamente. Las TI algunas veces ofrecen soluciones racionalizadas para cuestiones de administración complejas por la adquisición del poder de la tecnología para grandes cantidades de procesamiento de datos, y la transformación de esos datos en información significativa. Las TI plantean nuevos desafíos para los negocios. Incluso pueden retardar el tiempo de reacción de un negocio substancialmente, especialmente en los ambientes que combinan sistemas múltiples y dispares bajo una actividad económica importante.

A finales de 1980 y principios de 1990, BSM fue introducido como una estrategia para alinear las TI y los objetivos del negocio de una vez por todas ayudando a la administración a saber como el desempeño y disponibilidad de los recursos de TI afectan los mecanismos que fortalecen el negocio.

BSM se basa en este conjunto de buenas prácticas teniendo en cuenta que las empresas dependen cada vez más de su infraestructura informática en sus operaciones y que esta infraestructura debe estar alineada con las prioridades empresariales, sin embargo, la administración del entorno tecnológico se vuelve complejo por su constante cambio. Este cambio debido en gran medida al clima competitivo de las organizaciones.

La organización debe ser capaz de priorizar sus operaciones informáticas en función de los objetivos del negocio, comprender el impacto que los cambios tecnológicos ejercen y como estos cambios afectan la infraestructura informática.

BSM Permite entonces:

- Planificar las relaciones entre los elementos informáticos y lo servicios de negocio.
- Gestionar el impacto que la tecnología de la información ejerce sobre el negocio

---

Tecnologías o parte de un proceso de negocio, pero es un soporte más significativo y visible a la métrica del negocio por el propietario del mismo.

- Establecer prioridades en las incidencias con el fin de asegurar la realización y disponibilidad de los servicios más críticos.
- Gestionar peticiones de servicio y cambios informáticos de acuerdo con su relevancia e impacto en el negocio
- Analizar y optimizar la eficacia de los servicios informáticos en función de los compromisos de nivel de servicios de negocio.

En base a lo explicado con anterioridad se ahondará más en las temáticas de ITIL como una metodología que expone buenas prácticas en la administración de Servicios, mientras que BSM, con un enfoque más puntual, en la utilización de herramientas que supervisan, divulgan y manejan servicios de negocio.

---

3 Metodología ITIL/BSM

3. Metodología ITIL

Aparentemente se tienen segmentos del negocio aislados, aunque en realidad todos están asociados para el cumplimiento de la misión de la organización. Por ejemplo la prestación de servicios muchas veces no seria posible sin la gestión de infraestructura, de la misma manera las perspectivas del negocio no se darían sin la prestación de servicio y los servicios no serian posibles sin un soporte a estos.

El punto de interacción que se da entre estos segmentos del negocio es la búsqueda del cumplimiento de la misión de la organización, basada claramente en las perspectivas del negocio y la prestación de servicios.

La prestación de servicios requiere que se le de soporte al servicio para que éste siempre disponible, la disponibilidad la podemos lograr mediante la gestión o administración de la infraestructura. Aunque, como se ha mencionado con anterioridad, es uno de los servicios de seguridad que no se puede garantizar, he aquí que muchas organizaciones invierten considerablemente, para evitar estar indisponibles el menor tiempo posible.

ITIL propone el establecimiento de estándares para auxiliar en el control[3], operación y administración de los recursos. El planteamiento es mediante la revisión y la reestructuración de procesos, tanto los ya establecidos como los futuros tomando en cuenta el nivel de eficiencia para obtener una mejora continua.

[3] El proceso para determinar lo que se está llevando a cabo, valorización y, si es necesario, aplicando medidas correctivas, de manera que la ejecución se desarrolle de acuerdo con lo planeado, Además de regular las actividades, de conformidad con un plan creado para alcanzar los objetivos de la empresa.

Las actividades comprendidas, en cada caso, relacionadas con los procesos de negocio deben de documentarse para la utilización de otros miembros afines o de la misma área, al igual que los cambios con la finalidad de focalizar la posible falla, dictaminar los activos que se ven involucrados e informar anticipadamente para la toma de medidas afines al cambio, además de que quedan asentados todos los movimientos realizados.

La documentación de los cambios realizados persigue el objetivo de implantar un método con el cual identificar cual es la naturaleza del cambio, mediante la descripción breve del mismo, y establecer quien es el responsable, tanto la persona que autorizó el cambio como el que lo llevó acabo.

El marco de referencia ITIL se conforma de: [2]

- Administración de servicios (*Management services*)
- Planificación para la aplicación de la Administración de los servicios (*Planning to Implement Service Management*)
- Administración de las Aplicaciones (*Application Management*)
- Gestión de la seguridad (*Security Management*)
- Gestión de la Infraestructura- Tecnología de la información y las comunicaciones (*ICT Infraestructure Management*)
- La perspectiva del Negocio (*The Business Perspectiva*)

A continuación se describen cada uno de los anteriores.

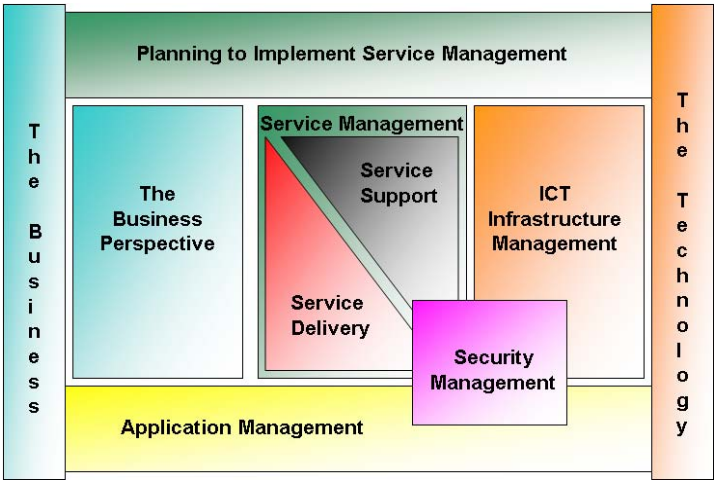

Figura 1 Marco de Referencia ITIL

3.1 Administración de Servicios (Services Management)

ITIL postula que el servicio de soporte, la administración y la operación se realiza a través de 10 procesos y una funcion contenidos en lo que se denomina, Servicio de Asistencia (*Service Support*), que se dividen en:

1. Manejo de Incidentes
2. Manejo de problemas
3. Manejo de configuraciones
4. Manejo de cambios y
5. Manejo de software

Y la Entrega de Servicios (*Service Delivery*), con las funciones:

6. Gestión de niveles de servicio (*Service Level Management*)
7. Gestión de la Capacidad (*Capacity Management*)
8. Gestión de la Continuidad del Servicio de TI (*IT Service Continuity Management*)
9. Gestión de la Disponibilidad (*Availability Management*)
10. Gestión de las Finanzas (*Financial Management*)

En cuanto a la función, es denominada Centro de Servicio a Clientes (*Service Desk*), que es el punto único de contacto entre los usuarios y la disciplina basada en procesos y está enfocada en alinear los servicios de Tecnologías de Información proporcionados con las necesidades de las empresa, es decir, entre los usuarios y la Administración de servicios de TI (ITSM).

En la siguiente figura se muestran los procesos y la función contenidos en la Administración de Servicios y se explica cada uno de estos procesos.

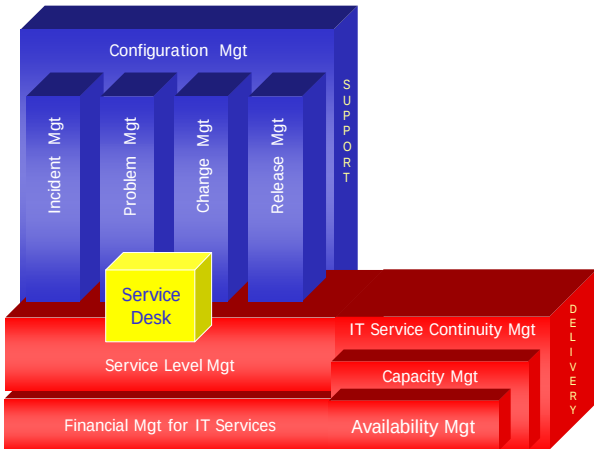

Figura 2. 10 procesos y 1 función que están contenidos en la entrega de servicios y el servicio de asistencia de ITIL

3.1.1 Servicio de Asistencia (Service Support)

La disciplina de Servicio de Asistencia (*Service Support*) para ITIL se centra en el usuario de los servicios de ICT[4] y se refiere sobre todo al asegurarse de que puede tener acceso a los servicios apropiados para apoyar las funciones del negocio. Relacionado con el control de acceso, la identificación y la premisa de otorgar el mínimo privilegio para desarrollar eficientemente sus funciones en la organización. En un negocio, los clientes y los usuarios son el punto de entrada al modelo de proceso. Cliente[5] y usuarios[6] están implicados en el servicio de asistencia cuando:

- Solicitan cambios.
- Necesitan la comunicación, actualizaciones.
- Tienen dificultades, preguntas.

El Centro de Servicio a Clientes (*Service Desk*) tiene como objetivo proporcionar un sólo punto de contacto para clientes y usuarios, además de facilitar la restauración de la operación normal del servicio, dentro de los niveles y prioridades establecidas, minimizando el impacto en el negocio, es decir, intentará resolverlo, si hay una solución directa o crea un incidente[7]. Los incidentes inician una cadena de procesos: manejo de incidentes, manejo de problemas, control de cambios del cambio, manejo de software y manejo de las configuraciones. Esta cadena de procesos utiliza la Base de Datos de Gestión de la Configuración (*Configuration Manager Data Base*, CMDB), que registra cada proceso, y crea los documentos de la salida para el seguimiento, por lo tanto las actividades del Centro de Atención a clientes son:

- ✓ Ser el punto único de contacto de TI hacia los clientes y usuarios, en inglés *Single Point of Contact* SPOC
- ✓ Registrar y dar seguimiento a incidentes, requerimientos y cambios estándares (manejar el ciclo de vida del incidente)
- ✓ Evaluación inicial de requerimientos e incidentes
- ✓ Enlace con proveedores
- ✓ Administrar expectativas definidas en los Acuerdos de Nivel de Servicio, SLAs
- ✓ Promover los servicios

---

[4] ICT (*information and communications technology*) ICT incluye tecnologías como computadoras de escritorio y portátiles, *software*, periféricos y conexiones hacia Internet que son previstos para satisfacer procesamiento de información y funciones de las comunicaciones.

[5] Cliente es quien en general recibe el servicio; usualmente el administrador responsable por el costo / pago del mismo, ya sea a través de un cargo directo o de manera indirecta en términos de necesidades. (Ejemplo: el Departamento de Ventas).

[6] Usuario es la persona que recibe los servicios día con día (Ejemplo: el vendedor del departamento de ventas)

[7] Incidente es cualquier desviación de la operación estándar, que causa o puede causar una interrupción o reducción de la calidad del servicio de TI.

Dentro de el Servicio de Asistencia se describen otros procesos que a continuación se explican.

3.1.1.1 Manejo de Incidentes

El objetivo del manejo de incidentes o también denominado como la **Gestión de incidentes**, en inglés *Incident Management*, es restaurar la operación normal del servicio tan rápido como sea posible, minimizando el impacto adverso en la operación del negocio y del usuario, asegurándose de mantener los mejores niveles de calidad y **disponibilidad del servicio**.

Para este proceso se tiene un diagrama que en cada una de sus fases maneja cuatro pasos básicos que son: propiedad, monitoreo, manejo de **secuencias**[8] y comunicación.

En el proceso de manejo de **incidentes** vemos que se da como primera etapa la detección del incidente (es cuando el sistema presenta alguna anomalía o falla, y que esto se puede traducir en un error en el sistema o que el usuario no puede hacer algo y recurre a pedir ayuda), cuando el **usuario** pide **ayuda** se dirige al Centro de Servicios al cliente (***Service Desk***); ya que lo tenemos identificado se hace una **clasificación** del incidente (vemos si el error que se presenta es conocido o si nunca se ha presentado) y de la mano va el soporte inicial (es el punto en el que el cliente llega a la **mesa de servicio** a solicitar ayuda, porque no sabe o no puede hacer algo).

La **prioridad** en la resolución de un incidente o problema se parámetriza de acuerdo a su **impacto** y **urgencia**, es decir, el retraso en tiempo aceptable para el usuario y para el negocio. Es el grado percibido de preocupación por el incidente basado en otros criterios (sensibles al tiempo).

Por definición el Centro de Servicios a clientes (*Service Desk*) o también denominada **mesa de servicio** es el *front line* o primer nivel de soporte. La **escalación** se presenta cuando un incidente no puede ser solucionado, dentro del tiempo acordado, entonces alguien con más autoridad y experiencia será involucrado. Otros miembros del **equipo de soporte** con más habilidades y experiencia son del 2do o 3er nivel y se involucran en pocos incidentes pero con alto grado de complejidad, teniendo así varios niveles de soporte, en caso de que el incidente sea conocido se hace el **procedimiento** de solicitud de servicio (se ejecutan los pasos a seguir según el manual de procedimientos para poder llegar a la solución de una forma viable y eficiente). Algunos de estos incidentes conocidos, han sido producto del análisis de riesgos realizado previamente y la instauración de dicho procedimiento permite contener el incidente y darle solución.

El transferir un incidente del 1er. nivel a 2do.nivel involucra más especialistas o acceso a privilegios para solucionar un incidente y consiste en el proceso de transferir

[8] La prioridad es la secuencia en la cual un incidente o problema requiere ser resuelto, se acuerdo a su impacto y urgencia.

un incidente de un individuo o equipo a otro. Este tipo de escalación se produce, generalmente, por falta de conocimiento o experiencia. Se puede producir cuando los periodos de tiempo se agotan, y se le conoce como escalación **Funcional-horizontal** (*Funtional-escalation*). También la escalación **jerárquica-vertical** (*herarchical-scalation*) que puede realizarse en cualquier momento del proceso de solución, es hacia una persona de mayor rango, cuando determine que el incidente no se va a resolver en el tiempo definido, esto debe ocurrir antes de que se termine el tiempo definido en los **Acuerdos de Nivel de Servicio**[9]**.** En estos casos aparece la figura de DAA, el cual, como se mencionó anteriormente, se encargará de la toma de decisiones siempre en pro de minimizar el impacto a las operaciones, Niveles de servicio y operacionales, con respecto a la misión y objetivos de la organización.

Se utiliza el método para atacar un incidente o problema[10], sea por una solución temporal o a través de una técnica, ya que desde el punto de vista del cliente, no se puede confiar en un aspecto particular de un servicio que se sabe tiene problemas. Parte de la Gestión de Incidentes y la Gestión de Problemas (Un nuevo problema debe ser creado para cada incidente cuando no existe una solución rutinaria o relación con algún problema o **error conocido**), es el presentar y elaborar los detalles para **soluciones temporales** ; una vez que ya que se la dio una solución al incidente por medio del manual de procedimientos se recurre a la **documentación** y **contabilización** del incidente, para ver que tanta incidencia tiene este caso; finalmente se hace una evaluación para ver si efectivamente se resolvió el incidente de forma satisfactoria y en supuesto de ser afirmativa se cierra el incidente y el otro supuesto seria que de la solución que se planteo no es lo suficientemente eficiente o acertada para que resuelva el problema y se recurre a hacer una **investigación** y un **diagnostico** de la situación para ver como es que se puede atacar el problema de frente y resolverlo; una vez que se tiene todo un contexto analizado se recurre a la ejecución de la propuesta de solución del incidente y se hace un estudio para ver si el incidente es recuperable o si es caso perdido (la mayoría de los casos son recuperables, pero cuando el nivel de daño es muy fuerte, se da el caso de que se de por perdido); y finamente se **cierra** el incidente y esta solución se documenta en una base de datos a la que se le llama **base del conocimiento** o "*Knowledge Data Base*" (aquí vienen documentadas todas las soluciones, y se establecen los pasos a seguir para que se hagan de forma eficiente) para que al momento de volverse a presentar el incidente ya va a estar documentado y esto hace que sea más fácil, rápida y eficiente su resolución. Esto mejora enormemente a la toma de decisiones.

---

[9] Acuerdos de Nivel de Servicio en inglés Services Level Agrameent (SLA´s). Son Contratos escritos entre un proveedor de servicio y su(s) cliente(s) en el que se documenta el nivel acordado para la calidad del servicio.

[10]Problema es una condición identificada en múltiples incidentes que exhiben síntomas comunes y de la cual no se conoce la causa (y se confirma que un Item de Configuración (CI) falla). Algunos de los problemas relacionados con aspectos de seguridad, al igual que su origen o fuente se mencionaron en el capítulo anterior

En resumen las **actividades** relacionadas con el manejo de incidentes son las siguientes:

Detección y registro

- ✓ Registro de detalles básicos del incidente
- ✓ Alertar a especialistas de grupos de soporte cuando sea necesario
- ✓ Comenzar los procesos de manejo de solicitudes de servicio

Clasificar y otorgar soporte inicial

- ✓ Clasificar incidentes
- ✓ Asignar el impacto y la urgencia con la finalidad de definir la prioridad
- ✓ Relacionar con la CMDB[11]
- ✓ Proporcionar soporte inicial, encontrando una solución rápida
- ✓ El cierre de incidentes o la asignación a los especialistas además de informar a los usuarios

Investigación y diagnóstico

- ✓ Evaluación del incidente
- ✓ Colectar y analizar toda la información relacionada para la solucionar el incidente
- ✓ Solución y recuperación
- ✓ Solucionar el incidente, usando la solución/temporal (*workaround*) o alternativas, generar Solicitud de cambio (RFC)[12]
- ✓ Tomar acciones de recuperación

Cierre

- ✓ Confirmar la solución con el cliente o quien la haya registrado
- ✓ Propiedad, monitoreo, seguimiento y comunicación
- ✓ Monitorear, escalar incidentes
- ✓ Informar al usuario

3.1.1.2 Manejo de Problemas

El **objetivo** de este proceso es **prevenir y reducir** al máximo los **incidentes**, y esto trae consigo una reducción en el nivel de incidencia, es decir, "*encontrar la causa raíz de los problemas actuales y potenciales, para minimizar el impacto adverso en el negocio causado por incidentes y problemas relacionados con errores dentro de la infraestructura de TI* "[3].Una vez encontrada la causa, se busca disminuir la recurrencia de incidentes y problemas, iniciando acciones de mejora. Es tanto reactivo como proactivo.

[11] Base de Datos de Gestión de la Configuración (*Configuration Manager Data Base*)
[12] Petición/solicitud/pedido de Cambio, en inglés *Request for Change* RFC

Por otro lado nos ayuda a proporcionar soluciones rápidas y efectivas para asegurar el uso estructurado de recursos.

En este proceso lo que se busca es que se pueda tener pleno control del **problema**[13], esto se logra dándole un **seguimiento y un monitoreo al problema**.

El diagrama de este proceso es muy particular, ya que se maneja en dos fases: la primera esta relacionada con lo que es el **control del problema** y la segunda es con el **control del error**.

En lo que respecta a la fase de **control del problema**: primero se tiene que **identificar** el problema en base a alguna sintomatología; ya que tenemos este antecedente, pasamos a la **clasificación** de los problemas (en este proceso al igual que en el proceso de manejo de incidentes tenemos que ver si es un **problema conocido** o **error conocido**[14]. Un error conocido cuenta con una **solución temporal**[15] o una **alternativa permanente**), en caso de ser conocido, se recurre al **procedimiento** de solicitud de servicio, donde se van a aplicar las soluciones de acuerdo a como están en el manual de procedimientos; y en caso de no ser conocido se tendría que hacer una fase de **investigación** para ver que es lo que genera el problema y más tarde hacer un **diagnostico**; ya que tenemos un diagnóstico tenemos que hacer un RFC (*Request For Change* o **Solicitud de Cambio**). Esta solicitud de cambio implica que se va a tener que **implementar** la solución y finalmente se va a hacer una **evaluación** para ver si se resolvió el problema de raíz. En caso de que sí funcione esta solución se pasa a la **documentación**.

Con lo que respecta a la segunda fase del modelo, el **control del error** se hace por medio de una **identificación** del error en general, posteriormente se hace una especie de **registro**, y este va a servir para **clasificar** el error; ya que se tiene una clasificación y se recurre a una **evaluación** de que tanto **daño** generó o puede llegar a generar el error, esto con la finalidad de **cuantificar** los desperfectos que podría llegar a causar en caso de que el error prevalezca y no se solucione; posteriormente se hace la resolución o corrección del error (este puede deberse a varios aspectos: configuraciones, falta de seguridad, inconsistencia de datos, etc.); y este modelo tiene una fase muy difícil, que es determinar que problemas están asociados o cómo es que al momento de cambiar algo en el sistema, se va a cambiar de forma uniforme

[13] Una condición identificada en múltiples incidentes que exhiben síntomas comunes y de la cual no se conoce la causa (y se confirma que Elemento de configuración falla en inglés *Item of Configuration* -CI falla)

[14] Error conocido es un problema del que se conoce la causa raíz y se tiene identificada la falla en el Elemento de Configuración (CI). Un error conocido cuenta con una solución temporal o una alternativa permanente. A partir de un error conocido puede generarse un Requerimiento para cambio *Request For Change [RFC]*. Sin embargo, la situación permanecerá como error conocido hasta que el cambio se haya implantado y sea definitivo.

[15]Solución Temporal en inglés *Workaround* es un método para “atacar” un incidente o problema, sea por una solución temporal o a través de una técnica, Se deben presentar y elaborar los detalles para soluciones temporales.

y no se va a alterar, y que presente inconsistencias. Por ejemplo que es lo que pasaría si cambio algunos de los datos en la configuración del sistema, se tendría que afectar el sistema de manera uniforme para que siga en equilibrio y no este cambiado en algunas partes y en otras que se quede como estaba antes.

Las actividades relacionadas con el proceso de manejo de problemas incluyen:

Control de problemas

- ✓ Identificación y registro
- ✓ Clasificación y asignación
- ✓ Investigación y diagnóstico
- ✓ Solución y cierre

Control de errores conocidos

- ✓ Identificación y registro
- ✓ Investigación de la solución
- ✓ Definición de la solución
- ✓ Evaluación del problema/revisión
- ✓ Cierre

3.1.1.3 Manejo de Configuraciones

También se le conoce como Gestión de la configuración en inglés *Configuration Management* su **objetivo** es proveer con **información real** y **actualizada** de lo que se tiene **configurado** e **instalado** en cada sistema del cliente, es decir, "*identificar, controlar, mantener y verificar las versiones de los elementos de configuración a fin de formar el modelo lógico de la infraestructura de TI*". [4]
A través de:

- ✓ Controlar todos los activos y configuraciones de la organización y servicios de TI.
- ✓ Proporcionar información exacta de la configuración y su documentación para apoyar al resto de los procesos de Service Management.
- ✓ Proporcionar una base sólida para la administración de incidentes, problemas, cambios y versiones.
- ✓ Verificar los registros de configuración contra la infraestructura y corregir las desviaciones.

Este proceso es de los más complejos, ya que se mueve bajo cuatro vértices que son: **administración de cambios, administración de liberaciones, administración de configuraciones y la administración de procesos diversos.**

La administración de la configuración incluye a la infraestructura[16] de TI, la Base de Datos de Gestión de la Información (CMDB)[17] y la información contenida en la CMDB como los CI *Configurtation Item* o Elemento de Configuración que es un componente de la infraestructura que está o estará bajo el control de la Administración de configuraciones *(Configuration Management*). Pueden variar en complejidad, tamaño y tipo –desde un sistema entero hasta un módulo o un componente menor de *hardware*, además del **alcance**[18], **relación**[19] y **atributos**[20] de cada CI, donde debe indicarse el **nivel** de cada uno considerado como: el grado de **detalle** seleccionado para describir los **Elementos de Configuración**. Debe guardarse un balance entre el nivel del CI y el esfuerzo para mantenerlo.

De la CMDB debe obtenerse un estado de muestra (*snapshot*) de una parte (o del total) de los **elementos de la CMDB** registrados en un **momento histórico** determinado, el cual captura tanto la estructura como los detalles. Aún y cuando se actualizan las posiciones después de tomada la muestra (*snapshot*), los **registros** que forman parte del *baseline* se mantienen sin cambio (congelados) tanto como referencia del estado original de la CMDB y para compararse contra el estatus actual. Esto permite reconstruir cualquier CI en caso de ser necesario, a este estado se le conoce como **línea de referencia** (*baseline*)

El nivel de complejidad de este modelo es alto, ya que influyen muchas variables y muchas de ellas son dinámicas, entonces al cambiar una o varias de ellas se afecta el sistema en general, lo que hace que sea muy difícil de manipular. Aunque es lo más parecido a la realidad, porque nuestro entorno es dinámico y las decisiones de unos afectan a otros.

Por ejemplo en lo que respecta a la administración de cambios vemos que se relaciona directamente con la **administración de incidentes y de problemas**, lo que conlleva una planeación, identificación, control, seguimiento del status, verificación y auditoria de configuraciones, lo que hace que haya muchas variables.

---

[16] La infraestructura de TI es el conjunto de hardware, software y documentación asociada, que se utiliza como soporte a las metas del negocio.

[17] La CMDB es una base de datos que contiene detalles relevantes de cada *Configuration Item CI* y de la relación entre ellos, incluyendo equipo físico, software y relación entre incidentes, problemas, cambios y otros datos del servicio de TI. La CMDB no es una base de datos para los programas de administración ni es una herramienta de auditoria que proporciona información limitada acerca del software y hardware.

[18] El alcance es la gama de responsabilidades de los CIs en la que se apoya *Configuration Management* para dar seguimiento (es decir, incluye telefonía, software únicos, etc)

[19] La relación es una descripción de la interfaz o liga que existe entre CIs. Padre-hijo o conectividad directa *upstream/downstream*.

[20] Los atributos son la información que define a cada CI como único, es decir su localización, estatus, edad, número de serie, etc. Estos pueden diferir basados en el tipo de CI.

En otro ejemplo la implementación de cambios implica que se tiene que hacer la liberación y distribución de nuevas versiones, esto de da por una fase de planeación, identificación, control, revisión del status, verificación y auditoria, y puede depender de la administración de las capacidades, ya que si no se cuenta con el software o con el hardware esta fase no se podría llevar a cabo; y así se haría con todos los niveles hasta llegar al cierre del control de cambios.

Las actividades relacionadas con la gestión de la configuración son:

- ✓ Planeación (estrategia, políticas, objetivos)
- ✓ Identificación (información CIs, proceso para mantener actualizado)
- ✓ Control (Proceso para admisión, registro, monitoreo e identificación de los CIs autorizados)
- ✓ Monitoreo del estatus
- ✓ Verificación (auditorias)
- ✓ Reportes

3.1.1.4 Control de Cambios

El objetivo de este proceso, también denominado **Gestión de Cambios** *(Change Management*), es **reducir los riesgos** tanto técnicos, económicos y de tiempo al momento de la realización de los **cambios,** es decir**,** garantizar el uso de métodos y procedimientos estándares para manejar eficaz y rápidamente los **cambios**[21] en TI, de manera tal que se minimice el impacto en la calidad del servicio y que puedan tener repercusiones en la misión y objetivos de la organización, por incidentes relacionados al cambio, mejorando así la operación diaria.

Los cambios se realizan previa solicitud usado para registrar los detalles de una solicitud o petición de un cambio a cualquier *Configuration Item* CI dentro de una infraestructura o a los procedimientos y a los artículos asociados a la infraestructura, denominada RFC *Request for Change*.

Entre etapa y etapa se da una fase de monitoreo para ver que no se han sufrido desviaciones de los objetivos.

Primero tenemos un **registro** y **clasificación** del **cambio,** como por ejemplo una actualización de una PC o agregar un nuevo empleado a los usuarios (controles de acceso). IMAC- Instalar, Mover, Agregar Cambios. Pueden ser considerados como un **Cambio estándar** el cual se refiere al cambio que ha sido pre-aprobado además sigue un proceso o método establecido. Es relativamente común y con solución

[21]El cambio es una adición, modificación o retiro de CIs aprobados, soportados o en baseline, tales como *hardware*, *software*, redes, aplicaciones, ambiente, sistemas construidos y su documentación asociada que se encuentran bajo control de *Configuration Management*. Un cambio siempre puede resultar en un nuevo estatus para uno o más de los elementos de configuración.

aceptada a un requerimiento específico y se consideran la base para crear machotes (*templates*) de cambios. También encontramos los **cambios urgentes** que son cambios requeridos para resolver un incidente o problema crítico para la **continuidad de la empresa** donde la **solución temporal** puede no ser suficiente. Requieren ser revisados, aprobados y probados de manera acelerada, además de asegurar la actualización de la CMDB al terminar, tan rápido como sea posible.

Los cambios se someten a escrutinio del **Consejo Asesor de cambios** en ingles *Change Advisory Board* CAB, donde un grupo de personas dan un consejo experto sobre los **riesgos, costos y valor de los cambios**.[22] Este consejo está integrado por **representantes de TI y usuarios** / clientes de las unidades de negocio. En cuanto a los cambios urgentes existe **Comité de Emergencia del Consejo Asesor de Cambios** en ingles *Change Advisory Board Emergency Committe* (CAB/EC) que puede considerarse como la versión "*fast track*" del CAB que se convocan por la emergencia y se toman decisiones sobre los cambios urgentes.

Los cambios importantes o grandes se dirigen a la alta Administración de la compañía para su aprobación, programación e implementación por el CAB, se le denomina entonces **Consejo de la Administración** (*Management Borrad*).
Al saber que cambio se tiene hacer, se pasa a la fase de **monitoreo y planeación**, si el rendimiento es satisfactorio se da la **aprobación** del cambio, y en caso de que el rendimiento sea malo se pasa a la fase de **reingeniería** hasta que el proceso funcione adecuadamente.

Ya que se aprueban los cambio, se construyen **prototipos** o **modelos** en los que se van a hacer las pruebas, se hacen las pruebas pertinentes para ver las **capacidades** del sistema, ya que el proceso esta probado se da la **autorización** e **implementación.** Debe de existir un **Calendario de cambios o Programa de Cambios Futuros** en ingles *Forward Scheduler for Change* FSC, que contiene los **detalles** de todos los **cambios aprobados** y fechas en que van a ser implementados, los cuales deben ser **acordados** por los clientes y la empresa (*Service Level, Service Desk & Availability Management*). El *Service Desk* debe comunicar a la comunidad de usuarios sobre cualquier inconveniente (**tiempos fuera de servicio**) al implementar los cambios. Además debe existir un programa de periodos de tiempo en los que las liberaciones de cambios impactan al menor número posible de usuarios (ventana de mantenimiento) que es la **Disponiblidad de servicio proyectada**.

Al ser implementado se ve que no se hayan tenido desviaciones y se ajusta a las **necesidades** actuales que también se le considera como **revisión** post-implementación. Las actividades que caracterizan el proceso de control de cambios son:

- ✓ Registro de RFCs
- ✓ Aceptación, RFCs filtradas

[22] Véase apartado respectivo en el capítulo anterior.

- ✓ Clasificación, categoría y prioridad
- ✓ Planeación impacto y recursos
- ✓ Coordinación
    - o Construcción
    - o Prueba
    - o Implementación
    - o Revisión
- ✓ Evaluación y cierre

3.1.1.5 Manejo de Software

Su objetivo es proporcionar un punto de vista holístico de un cambio en un servicio de TI y garantizar que se consideran en conjunto todos los aspectos, tanto técnicos como no técnicos, de una versión

- ✓ Planear y coordinar el desenvolvimiento *(roll out)* exitoso del software y hardware relacionado

- ✓ Diseñar e implementar procedimientos eficientes para la distribución e instalación de Cambios en los sistemas

- ✓ Comunicar y administrar las expectativas del cliente durante la planeación y desenvolvimiento (*roll out*) de nuevas versiones

- ✓ Asegurar que las copias originales del Software están seguras en la **Biblioteca de software Definitivo**[23], *Definitive SoftwareLibrary*, DSL por sus siglas en ingles; y se actualice la CMDB

Es decir, planear y controlar exitosamente la instalación de Software y Hardware bajo tres ambientes: ambiente de desarrollo, ambiente de pruebas controladas y ambiente real.

Este proceso tiene un diagrama que marca la transición que se da de acuerdo a los ambientes por los que se va dando la evolución del proyecto, es decir, Se le conoce también como **Gestión del software** (*Release Management*).

[23]Biblioteca de software definitivo es la Biblioteca lógica (repositorio) en la cual se tiene las versiones autorizadas de todo el software que está almacenado y protegido, es una/varias bibliotecas físicas donde se tienen las copias maestras de las versiones de software, debe estar separada de la biblioteca de pruebas e incluir software autorizado y aceptado bajo un control estricto de *Change & Release Management*. Puede incluir un lugar físico en donde se almacenan las copias físicas de las copias maestras de manera protegida (Ejemplo acondicionada a prueba de incendios).

En lo que respecta al ambiente de desarrollo se observa, que se tiene que hacer la **liberación de las políticas**[24], la liberación de la planeación, el diseño lógico de la infraestructura que se va a implementar y la adquisición de software y hardware están entre los ambientes de desarrollo y de pruebas controladas. En el caso del Hardware también debe de existir un **almacén de *Hardware* definitivo**, *Definitive Hardware Store* DHS, que contiene el inventario de hardware. El hardware en DHS es utilizado para reemplazar o reparar configuraciones similares en la infraestructura, detalles de esta composición o configuraciones deben estar incluidos en la CMDB. Tanto la DSL como el DHS, se engloban en **unidades de versión** que es el Nivel al que los CIs se empaquetan en una versión para su liberación. En el caso del hardware considera si se va a cambiar toda la PC, la tarjeta o los discos duros (o incluso la RAM o el procesador) se van a cambiar de manera separada. Para el software los cambios pueden realizarse a toda la suite del sistema o bien a nivel de módulo y/o programa. Una nueva versión de un DLL, requiere la prueba de todos los paquetes que lo utilizan o inclusive la reinstalación de los mismos.

Se requiere que ambos hagan pruebas sobre el hardware y software; en el ambiente de pruebas controladas se observa que se hace la construcción y liberación de las configuraciones (nivel lógico), se hacen las pruebas para establecer los **acuerdos de aceptación**; entonces, se da la aceptación total de versiones y de modelos, se arranca la planeación y finalmente las pruebas y comunicaciones; y en lo que es el ambiente real se observa que se da la distribución e instalación.

En la etapa del ambiente real es la que se ve de forma más concreta, ya que muchas veces no se tiene idea de todo lo que pasa hasta antes de la instalación.
Se consideran las **versiones**[25] siguientes:

Versión Delta

Una versión delta o parcial es aquella que incluye sólo los CI que son nuevos o cambiaron a partir de la versión anterior. Por ejemplo, si la versión es un programa, la versión delta contiene sólo aquellos módulos que se modificaron o agregaron desde la última versión de todo el programa.

Versión Completa

Todos los componentes de unidad de versión son construidos, probados, distribuidos e implementados.

Versión de emergencia

Correcciones a un pequeño número de problemas conocidos y urgentes.

[24]La política de liberación define los roles y responsabilidades, las guías y detalles para cada sistema o servicio; incluyendo su nombramiento, numeración, criterios para determinar el impacto, estatus de emergencia, ventanas de mantenimiento y activación de su plan de reversa (back out).

[25] La versión (*release*) es una colección de nuevos y/o cambios de *Configuration Items* CIs de una unidad de versión, los cuales fueron probados e introducidos en el ambiente de producción.

En el proceso de entrega del servicio es el punto en el que el usuario se hace uno con el servicio y no sabe que hay detrás del servicio que esta recibiendo, un sin fin de actividades y de decisiones que se tuvieron que tomar para que llegar a ese punto.
Este proceso es en el que más cuidado se debe de poner, ya que en caso de haber fallas, el primero en detectarlas o en percibirlas es el usuario, y esto genera que el cliente esté insatisfecho o molesto. Repercusión en los Niveles de Servicio, pago de indemnizaciones acordadas.

Por lo general los usuarios no saben que para que puedan hacer uso de los servicios, se paso por una fase de planeación, monitoreo, análisis y por un sin fin de pruebas, con la intención de que en caso de que algo no funcione, se de en la fase de pruebas controladas y no en la fase de pruebas en ambiente real, donde el mayor afectado es el cliente.

Las **actividades** que caracterizan a la gestión del software son:

- ✓ Definición de política y planeación
- ✓ Diseño y desarrollo o compra
- ✓ Construcción/Configuración
- ✓ Prueba y aceptación
- ✓ Planeación roll out
- ✓ Comunicación, preparación y capacitación
- ✓ Distribución e instalación

3.1.2 Entrega de Servicios (Service Delivery)

La disciplina de la **Entrega de Servicios** (*Service Delivery),* se refiere sobretodo a los servicios proactivos previstos que el negocio requiere de los proveedores de ***ICT***[26] en orden de otorgar un **soporte** adecuado hacia los usuarios del negocio. Esto está enfocado en el negocio como el cliente de los servicios de Tecnologías de Información y Telecomunicaciones, es decir como aquel que **recibe servicios**, tal es el caso de transferencias electrónicas en línea, a partir de una *ICT*. La Disciplina de Entrega de Servicios consiste de los siguientes procesos.

[26] ICT (*information and communications technology*) Tecnologías de la información y las comunicaciones. ICT incluye tecnologías como computadoras de escritorio y portátiles, software, periféricos y conexiones hacia Internet que son previstos para satisfacer procesamiento de información y funciones de las comunicaciones.

Proceso	Breve Descripción del Proceso
Gestión del Nivel de Servicio (*Service Level Management*)	La Gestión de Nivel de Servicio provee un mecanismo para alinear los servicios de TI con los requerimientos del negocio, La gestión de niveles de servicio provee una manera estructurada para clientes y proveedores de servicios de TI, para que de un modo significativo tratar y evaluar que tan bien un servicio es entregado. El objetivo primario de la gestión de niveles de servicio es proporcionar un mecanismo para establecer expectativas claras con respecto a los servicios que están siendo entregados. Las actividades se incluyen dentro del proceso de creación de un catálogo de servicios, identificando requerimientos, la negociación de los Acuerdos de Nivel de Servicio (SLAs) y el manejo de la continuidad del servicio, disponibilidad, capacidad y la fuerza de trabajo.
Gestión de la Capacidad (*Capacity Management*)	Las actividades de la Gestión de la capacidad incluyen planeación, estimación de la capacidad necesaria, y controlar la capacidad de solución del servicio para satisfacer las exigencias de los usuarios dentro de los niveles de desempeño establecidos en el SLA. Esto requiere la recopilación de información sobre el uso de los escenarios, los patrones, y la carga máxima característica de la solución de servicio, así como el estado de los requerimientos realizados. Estas actividades de recopilación de datos se incluyen en el proceso de Gestión de Capacidad
Gestión de la continuidad del Servicio (*IT Service Continuity Management*)	La Gestión de la Continuidad del Servicio, también incluye la gestión de contingencias, enfocada en minimizar las interrupciones al negocio causadas por fallas en los sistemas de misión critica. Este proceso se ocupa de la planificación para hacer frente y recuperarse de desastres en TI. También proporciona orientación en el resguardo de los sistemas existentes para el desarrollo e introducción de contramedidas proactivas y reactivas. La Administración de la continuidad del negocio también considera que actividades se necesitan estar llevándose a cabo en el evento de interrupción imprevista de los servicios no atribuido a un completo impacto desastroso.
Gestión de la Disponibilidad (*Availability Management*)	El objetivo de la gestión de la disponibilidad es asegurar que los servicios de TI estén disponibles cuando sean requeridos. La disponibilidad es calculada y reportada como el porcentaje de las horas acordadas de servicio por las cuales el servicio es disponible.
Gestión de las Finanzas(*Financial Management*)	La Gestión de las Finanzas es un proceso que introduce el concepto de presupuesto, cuenta y tarifa de los servicios de la entrega de servicios de TI a los clientes. La presupuestación y cuenta involucra el entendimiento de los costos de proveer varios servicios. La gestión de las finanzas asegura que cualquiera de los servicios de TI propuesto es justificado desde el punto de vista de costos y presupuesto. Esto es muchas veces referido a un análisis de costo beneficio. Las actividades relacionadas incluyen practicas contables estandarizadas como la presupuestación, las asignaciones de gastos y otros. El concepto de reembolso permite a los departamentos internos de TI funcionar como una unidad de negocio, los controles no esencialmente exigen de los clientes, si no que permite a estos demandar el valor de su dinero.

Tabla 1 Procesos y Descripción de la Entrega de Servicios

3.1.2.1 Gestión de Nivel de Servicios (Service Level Management)

La **Gestión de Nivel de Servicios** prevé la identificación continua, monitoreo y revisión de los niveles de servicios en las TI especificados en los **Acuerdos de Nivel de Servicio**, SLA por sus siglas en inglés *Service Level Agreement*[27].

Los SLA tienen el objetivo de asegurar que se ofrece y mejora la calidad de los servicios de TI, a través de un ciclo constante de acordar, supervisar y obtener reportes, para lograr su alineación con las necesidades del negocio y una mejor relación con los clientes. Además, lleva acabo acciones que buscan erradicar el mal servicio a un costo adecuado. La **Seguridad** en las TI es una parte integral de la **Entrega de Servicios**, y como la Gestión de Niveles de Servicio es la disciplina clave para proveer la Entrega de servicios, es también últimamente responsable de asegurar que los servicios de TI son otorgados de una manera segura, y la disponibilidad de estos es maximizada dentro de los regímenes del costo y la eficiencia. Los **Planes de Contingencia** también forman parte de la entrega de Servicios para asegurarse de que los servicios se pueden recuperar y mantener en caso de un incidente serio.

Hay un número de procesos del negocio que forman parte de la Gestión de Niveles de Servicio. Estos son:

- ✓ Revisión de los servicios existentes, esto se realiza mediante la creación de un **catálogo de servicios**[28]
- ✓ Negociación con los clientes
- ✓ Revisión de los contratos de soporte de una tercera parte, los proveedores de servicio, en este caso entran los **contratos externos**, *underppining contracts* (UC´s).[29]
- ✓ Produciendo y Monitoreando los Niveles de Acuerdo de Servicio (SLA), estos SLA se basan en los **Requerimientos de nivel de servicio,** *Service Level Requirement* (SLR)[30]
- ✓ Puesta en práctica de las políticas y de los procesos de la mejora del servicio
- ✓ Establecer prioridades
- ✓ El planear el desarrollo del servicio
- ✓ Participación en el proceso de consideración de los costos de los servicios y la recuperación de estos costos (*Return of Investment*) ROI.

[27] Contratos escritos entre un proveedor de servicio y su(s) cliente(s) en el que se documenta el nivel acordado para la calidad del servicio.
[28] Catálogo de Servicio es un listado completo de todos los servicios disponibles para los clientes y usuarios.
[29] Contratos externos o contratos de servicios acordados, donde un proveedor externo mediante un contrato, cubre la entrega de los servicios hacia TI.
[30] Requerimientos de Nivel de Servicio *Server Level Requirement* SLR, son una lista de los servicios solicitados por los clientes, son una parte integral del criterio de diseño de los servicios, donde la especificación funcional es parte de estos requisitos, cubre las definiciones detalladas de las necesidades del cliente y son usados para desarrollar, modificar e iniciar servicios. Puede servir como una base para diseñar un servicio y su *Server Level Agreement* SLA.

La Gestión de Niveles de Servicio asegura que los acuerdos son en un lugar con proveedores de soporte interno de TI y proveedores externos, mediante los **Acuerdos de Nivel Operacional**, *Operation Level Agreement* OLA[31], y los Contratos Externos (UC). El proceso involucra la evaluación del impacto del cambio sobre los la calidad del servicio y los Acuerdos de Nivel de Servicio (SLA's). La Gestión de Niveles de Servicio tiene un estrecha relación con los procesos operacionales al controlar sus actividades, el papel principal de la Gestión de Niveles de Servicio es marcar las métricas establecidas y supervisadas contra un punto de referencia. Es la interfaz primaria con el cliente.

Las actividades relacionadas con la Gestión de Niveles de Servicio son:

Identificar necesidades

- **Definir servicios**, Requerimientos de Nivel de Servicio (SLR)
- **Contrato** (Acuerdo de Nivel de Servicio-SLA, Acuerdos de Nivel Operacional-OLA, Contratos Externos- UC) y que se subdividen en:
  - ✓ Negociar
  - ✓ Borrador
  - ✓ Ajustar
  - ✓ Concluir
- **Monitoreo** (Acuerdos de Nivel de Servicio-SLA) sobre los SLA para obtener lo siguiente:
- **Reporte** (*Service Level Agreement Management*-SLAM y *Red Ambar Green-RAGs*) Por ejemplo, podemos fijar el ámbar para ocuparnos de una poca desviación de SLA (calidad de 73%). Cuando golpeamos el ámbar, los clientes exigen generalmente un plan detallado del estudio y de acción alrededor de la falta en SLA. Sin embargo si es rojo entonces se considera como alejado considerablemente del SLA. Después de obtener el reporte, viene entonces:
- **Revisión** (*Service Improvent Program*-SIP y mantenimiento de Acuerdos de Nivel de Servicio-SLA, Acuerdos de Nivel Operacional-OLA, Contratos Externos-UC)

La disponibilidad para ejecutar un **Programa de Mejora al Servicio**, *Service Imporvement Program* por sus siglas en ingles SIP, "depende de varios procesos de Administración de Servicios de TI (ITSM[32]) existentes en un lugar y un nivel de capacidad suficiente para mantener el esfuerzo" [5].

[31] Acuerdo de Nivel Operacional *Opertional Level Agreement* OLA, es un acuerdo interno que cubre la entrega de servicios, realizado entre un departamento de TI y la Gestión de Niveles de Servicio.
[32] ITSM es una disciplina basada en procesos, enfocada en alinear los servicios de Tecnologías de Información proporcionados con las necesidades de las empresas, poniendo énfasis en los beneficios que puede percibir el cliente final, además propone cambiar el paradigma de gestión de TI, por una

Análogamente, un **Programa de Mejora Continua al Servicio**, en ingles *Continuous Service Improvement Program* (CSIP), requiere que los procesos de manejo de incidentes, problemas y la gestión de la Disponibilidad y Niveles de Servicio estén en periódica revisión conforme a la realización de los niveles de servicio como parte de una cotidiana revisión de actividades para la cual los Acuerdos de Nivel de Servicio (SLA) se efectuaron.

Las TI pueden promover un **Programa de Mejora al Servicio** SIP para mejorar el servicio resolviendo requisitos actuales o cambios en el negocio y/o requerimiento de capacidad de las TI, o hacia la correcta alteración crónica de los objetivos de los **Acuerdos de Nivel de Servicio** (SLA). Lo anterior es normalmente acordado en vías de las actividades de **Gestión de la Disponibilidad, y el proceso de manejo de problemas.** En ambos casos, la integración de, ambos, Gestión de la Disponibilidad y Proceso de manejo de Problemas resultará en una rápida resolución de errores sistemáticos en la infraestructura que causan el déficit en el servicio.

Algunas recomendaciones con respecto al Programa de Mejora al Servicio (SIP) son:

1. Expedir una política clara que indique el intento, la administración del soporte y una guía total para un Programa de Mejora al Servicio (SIP), especificado en el Acuerdo de Nivel de Servicio (SLA).
2. Identificar claramente los puntos que integran los procesos, y los documentos entradas y salidas requeridas para el soporte en un Programa de Mejora de Servicio (SIP) que se listan a continuación:

   - ✓ Gestión de Niveles de Servicio (SLM)
   - ✓ Proceso de Manejo de Problemas (*Problem*)
   - ✓ Gestión de Disponibilidad (*Availability*)

3. Establecer Acuerdos de Nivel Operacional (OLAs) entre los dueños de los procesos respectivos y los grupos técnicos funcionales para asegurar consistencia en la disposición y priorización de las iniciativas del Programa de Mejora al Servicio (SIP).
4. Revisión de los Factores Críticos de Éxito, CSF por sus siglas en inglés *Critical Success Factors*, y los Indicadores Claves de Funcionamiento, KPI por sus siglas en inglés *Key Performance Indicators*, (CSF/KPI's) para los procesos respectivos involucrados, estos para asegurar la identificación y captación de una métrica adecuada, revisando y reportando los datos apropiados.

---

colección de componentes enfocados en servicios "end-to-end" usando distintos marcos de trabajo con las "mejores prácticas", como por ejemplo la *Information Technology Infrastructure Library* (ITIL) o el eSCM (enabled *Service Capability Model*). Entre los que se destacan para ITIL Entrega de Servicios (*Service Delivery*) y Servico de asistencia (*Service Support*).

Identificar actividades especificas relacionadas con el Programa de Mejora al Servicio (SIP) en los roles relevantes de los respectivos miembros que participan en el proceso.

A continuación se puede observar los aspectos relacionados con el Programa Continuo de Mejora al Servicio

3.1.2.1.1 Programa Continuo de Mejora del Servicio (Continuos Service Improvement Program CSIP)

Una estrategia de un programa de mejora continua es el camino en el cual la calidad de atención y la calidad de vida de los temas (a mejorar) están en las direcciones de:

- ✓ Fijar prioridades y objetivos claros para áreas que necesitan ser monitoreadas y mejoradas- áreas de importancia para los residentes, cuidadores y empleados a través de dominios de calidad.
- ✓ Planeando e implementando, sistemáticamente Cómo monitoreando y a través del perfeccionamiento sucederán mejoras relevantes y eficientes en las actividades.
- ✓ Midiendo el progreso hacia el perfeccionamiento de los objetivos, y demostrar exactamente que nivel de atención se está proporcionando.

En resumen la **Gestión de Niveles de servicio** provee un mecanismo de alineación de los servicios de TI con los requerimientos del negocio, proporciona una manera estructurada para los clientes y los proveedores de TI de forma significativa, para discutir y determinar que tan bien se está entregando un servicio El objetivo principal de la Gestión de Niveles de Servicio es proveer un **mecanismo** para fijar expectativas claras con los grupos de clientes y usuarios con respecto al **servicio que es entregado**. Las actividades incluidas en el proceso es la creación de un catálogo de servicios, identificando requisitos, negociando Acuerdos de Niveles de Servicio (SLAs), y manejar la continuidad del servicio, la disponibilidad, la capacidad, y la mano de obra.

3.1.2.2 Gestión de la Capacidad (Capacity Management)

La Gestión de la capacidad es un proceso utilizado para administrar las tecnologías de Información (TI). El objetivo fundamental es el asegurar que las TI cumplen con las necesidades actuales y futuras de la organización de una forma rentable. Como el uso de Servicios de TI y la funcionalidad como parte del cambio evolutivo, tal es el caso de, la cantidad de potencia de procesamiento, la memoria, etc., que también cambia.

Si es posible entender lo que se exige actualmente la organización, y cómo los requerimientos cambiarán con el tiempo, este enfoque propone que la planeación del crecimiento de los servicios de TI con una transición fácil y de una manera estable o menos reactiva. Si hay picos por ejemplo, en procesamiento en un particular

momento del día, este proceso analizará que es lo que está pasando en ese momento y propondrá hacer cambios para maximizar el desempeño de la infraestructura existente, por ejemplo, afinar una aplicación, o pasar a un procesamiento cíclico por lotes en ese momento particular de transición.

Estas actividades están destinadas a optimizar el rendimiento y la eficiencia e ir hacia un plan justificado de inversión financiera. La Gestión de la capacidad se refiere a monitorear el rendimiento y la tasa de transferencia en un servidor, granja de servidores o propiamente un **análisis del rendimiento**[33] [6] para la medición de datos, incluyendo un análisis del impacto de la capacidad de las nuevas versiones (*releases*).

Ajuste en el rendimiento[34] [7]de las actividades para asegurar el más eficiente uso de la infraestructura existente.

La comprensión de la demanda de los servicios y los planes de futuro para el crecimiento del volumen de trabajo (o contracción).[35]

Influencia en la demanda de recursos[36] de cómputo.

La capacidad de planificación[8] es el proceso de determinación de la capacidad de producción que necesita una organización a la evolución de la demanda de sus productos. En el contexto de la planificación de la capacidad, la "capacidad" es la máxima cantidad de trabajo que una organización puede terminar en un Período de tiempo determinado. Desarrollando un plan para el servicio.

Una discrepancia entre la capacidad de una organización y las demandas de sus clientes resulta en una ineficiencia, ya sea en recursos subutilizados o incumplimiento

---

[33] El análisis de rendimiento (*performance analysis*), comúnmente denominado perfil, es la investigación del comportamiento de un programa usando información recogida por éste, cuando se ejecuta (es decir, es una forma de análisis dinámica del programa, en contraposición de un análisis de código estático).El objetivo habitual de el análisis de rendimiento es determinar cuales partes de un programa optimizan la velocidad o el uso de memoria.

[34] Ajuste en el rendimiento (*performance tuning*). Consiste en la mejora del rendimiento del sistema, el motivo de esta actividad es por un problema en el rendimiento, que puede ser real o previsto. Muchos sistemas responderán, para incrementar la carga, con algún acuerdo de disminución en el rendimiento. La capacidad de un sistema para aceptar una carga mayor es llamado escalabilidad y la modificación de un sistema para manejar una carga mayor es sinónimo de ese ajuste en el rendimiento. Un ajuste sistemático sigue los siguientes pasos: 1) Evaluar el problema y establecer los valores numéricos que clasifican una conducta de aceptable. 2) Medir el rendimiento del sistema antes de la modificación. 3) Identifique la parte del sistema que es fundamental para mejorar el rendimiento. Esto se llama el cuello de botella.4) Modificar esa parte del sistema para eliminar el cuello de botella. 5) Medir el rendimiento del sistema después de la modificación.

[35] La administración de la demanda Trabaja junto con el cliente para balancear cargas de trabajo y demanda. Ejemplo ejecutando ciertas tareas en horas “libres” (compilar, correr procesos en *batch* de trabajos de impresión largos); busca influenciar la demanda de capacidad, por lo general se realiza a corto plazo porque no hay capacidad suficiente, pero se puede utilizar en el largo plazo cuando es difícil justificar una actualización (*upgrade*).

[36] Identificar y evaluar tecnologías que proporcionen economía de escala (procesamiento paralelo, arreglos de almacenamiento).Monitorear e informar las tendencias de uso de recurso y desempeño a corto, mediano y largo plazo, es parte de la administración de los recursos.

a los clientes. El objetivo de la capacidad de planificación es minimizar esta discrepancia. La demanda de la capacidad de una organización varía en función de los cambios en la producción, como el aumento o la disminución de la cantidad de producción de un producto existente, o la producción de nuevos productos. Capacidad puede aumentarse a través de la introducción de nuevas técnicas, equipos y materiales, aumentar el número de trabajadores o de las máquinas, aumentando el número de turnos, o la adquisición de nuevas instalaciones de producción.

El Objetivo de la **Gestión de la Capacidad** es entender los requerimientos del negocio (**nivel esperado**), la operación de la organización (**nivel actual de entrega del servicio**) y la infraestructura de TI, a fin de asegurarse que exista la capacidad necesaria para satisfacer a **costo-efectivo**, las necesidades presentes y futuras del negocio. En otras palabras: capacidad adecuada, en el momento adecuado, al costo adecuado y alineada al negocio.
La Gestíon de la Capacidad es un proceso usado para manejar la tecnología de la Información (TI). Su meta fundamental es asegurarse que la capacidad de las TI resuelva los requisitos actuales y futuros del negocio de una manera rentable y ésta se subdivide como sigue.

3.1.2.2.1 Subprocesos en la Gestión de la Capacidad

Las actividades relacionadas con la Gestión de la capacidad se dividen en:

- **Business Capacity Management (BCM)**
  - ✓ Desarrollar el plan de capacidad [periódica]
  - ✓ Modelación[37] [ad hoc-cuando se necesite]
  - ✓ Dimensionamiento de aplicaciones[38] [ad hoc-cuando se necesite]
- **Service Capacity Management (SCM)**
  - ✓ Monitoreo de los componentes de la infraestructura [on going]
  - ✓ Análisis de tendencias [on going]
  - ✓ Ajustes (tuning) [on going]
  - ✓ Implementación [on going]
  - ✓ Administración de la demanda [on going]

[37] La Modelación mediante Técnicas y/o herramientas para predecir y optimizar los recursos, a partir de predecir el comportamiento de los servicios de TI, bajo cierto volumen y variedad de trabajo (desde estimar hasta hacer prototipos de prueba).
[38] El dimensionamiento de aplicaciones es la evaluación de los requisitos de capacidad (almacenaje, ancho de banda, soporte) necesario para las nuevas aplicaciones o los cambios en estas referentes a software.

- ✓ Llenado de la base de datos de Capacidad (CDB) [on going]

- **Gestión de la capacidad de los recursos (Resource Capacity Management-RCM**)

La Gestión de la capacidad de los recursos (RCM), es parte de la Gestión de la capacidad, la cual muestra la necesaria exigencia de servicios, en base de las demandas del negocio y deduce la capacidad de los recursos, basado en esta demanda.

Tomando la totalidad de los resultados de las pruebas de carga (Gestión del rendimiento, *performance management*[39]) [9] (pp. 15), en cuenta, la optima distribución de la carga para el sistema existente es elaborado y garantizado con la ayuda de la afinación o ajustes y el equilibrio de la carga de trabajo.

Un objetivo importante de la gestión de la capacidad de los recursos es garantizar la demanda de servicios relacionados con el rendimiento con un costo mínimo. Esto asegura que los recursos existentes sean usados de manera optima y que los ajustes necesarios se han previstos, realizándolos en el momento oportuno y en la fecha acordada. [10]

La Gestión de la capacidad apoya la óptima y rentable prestación de servicios de TI para auxiliar a la organización a igualar la infraestructura de TI con las demandas del negocio.

3.1.2.3 Gestión de la Continuidad del Servicio (IT Service Continuity Management)

El objetivo es apoyar al proceso de Administración de la Continuidad del Negocio al asegurar que la **infraestructura y servicios de TI** (incluyendo sistemas, redes, aplicaciones, soporte técnico y el Centro de servicio a clientes) puedan ser **reestablecidos** en los tiempos requeridos y acordados con la organización, es decir, la continuidad del servicio (*IT Service Continuity Management*) ayuda a garantizar la disponibilidad y la rápida restauración de los servicios informáticos en caso de desastre. El alto nivel de actividades son Análisis de riesgos, la Administración del Plan de Contingencia, Pruebas sobre el Plan de Contingencia, y la Administración de riesgos. Gran parte de estos temas se desarrollaron ampliamente en el capítulo anterior.

La gestión de la continuidad del negocio (*Business Continuity Management*-BCM), se encarga del análisis y administración de riesgos para garantizar que una organización pueda continuar operando a un nivel mínimo predeterminado. La gestión de la continuidad del negocio (BCM) reduce riesgos y desarrolla planes para restaurar las actividades del negocio si estas son interrumpidas por un desastre. Deben

[39] La medición del rendimiento es el proceso de evaluar el progreso hacia el logro de objetivos predeterminados. La gestión del rendimiento se basa en este proceso, añadiendo la comunicación pertinente y la adopción de medidas sobre los progresos realizados contra los objetivos predeterminados

considerarse todos los aspectos incluyendo la seguridad del empleado y el impacto emocional de la familia. El riesgo por su parte, como se vio con anterioridad, es una medida de exposición a la cuál una organización se encuentra sujeta. El análisis de los riesgos provee de información referente a las amenazas y vulnerabilidades de los activos y los CIs (*Configuration Item*)[40], además de sus medidas preventivas. Ésta es una combinación de la probabilidad de que ocurra una interrupción y de la pérdida posible que puede resultar de tal interrupción para el negocio.

La vulnerabilidad por su parte es una debilidad en los sistemas o activos que puede ser aprovechada por las amenazas y estas se consideran como aquellas entidades, fuerzas o circunstancias, no directamente controladas por la organización, que pueden impactar la provisión de servicio (ejemplos, fenómenos de la naturaleza, huelgas, etc.), esto puede llevar a una situación no planeada en la que se espera que uno o más de los servicios de TI no estén disponibles por un tiempo significativo, excediendo los niveles de servicio comprometidos con los clientes, es decir, un estado de crisis.

Las actividades relacionadas son:

- Iniciación
- Requerimientos y estrategia a seguir
- Implementación de la Administración de la continuidad del servicio de TI (*IT Service Continuity Management* ITSCM)
- Administración de la operación

3.1.2.4 Gestión de la Disponibilidad (Availability Management)

La Gestión de la disponibilidad permite a las organizaciones sustentar la disponibilidad de los servicios de TI con la finalidad de apoyar al negocio a un costo justificado. Las actividades de alto nivel son realizar los requerimientos de disponibilidad, compilar planes de Disponibilidad, Monitorear la Disponibilidad, además del monitoreo de las obligaciones que con lleva el mantenimiento.

La gestión de la Disponibilidad es la habilidad de un componente de TI para realizar lo convenido en el acuerdo de nivel en un periodo de tiempo.

- La Confiabilidad: responde al cuestionamiento ¿Cómo es confiable un servicio?, la Confiabilidad de un componente de TI para realizar lo convenido en el acuerdo de nivel en las condiciones descritas.
- Mantenimiento: La capacidad de un componente de TI para conservar o restablecer a un estado operacional.

[40] Elemento de Configuración (*Configuration Item*) es un componente de la infraestructura que está o estará bajo el control de la Gestión de la Configuración (*Configuration Management*). Pueden variar en complejidad, tamaño y tipo –desde un sistema entero hasta un módulo o un componente menor de hardware.

- Servicio: La capacidad de un proveedor externo para mantener la disponibilidad de componentes o su función en virtud de un contrato de terceros.
- Elasticidad: Una medida de libertad por una falla operacional y un método que mantenga la confiabilidad de los servicios. Un método popular de elasticidad es la redundancia.
- La Seguridad: Un servicio puede tener datos asociados. La Seguridad se refiere a la confidencialidad, integridad y disponibilidad de los datos, además del no repudio, la autenticación y el control de acceso,; servicios de seguridad descritos en el capítulo 1.
- La gestión de la Disponibilidad es responsable de asegurar que las aplicaciones y los sistemas estén arriba (operando) y disponibles según lo acordado en las condiciones de los Acuerdos de Nivel de Servicio (*Service Level Agreements* SLAs). El equipo encargado de la gestión de la disponibilidad revisa los requerimientos de disponibilidad de los procesos de negocio y asegura un costo efectivo en la puesta en marcha del plan de contingencia, además de probar este plan de contingencia sobre una base regular, para garantizar el conocimiento de las necesidades del negocio. Por ejemplo, las aplicaciones de Internet que soportan peticiones en línea pueden tener 30 minutos o menos para recuperar lo requerido, y que en conjunto se pueden utilizar con los componentes de infraestructura existentes proveyendo varios niveles de redundancia. Los menos críticos, etapas de aplicación no dirigidas a los clientes utilizadas por unos cuantos usuarios en pequeñas oficinas, con unos cinco días de periodo de recuperación puede preverse mediante una infraestructura no muy costosa y con capacidades limitadas de redundancia.

La gestión de la Disponibilidad es también primordial en el análisis de fallas en los componentes y su impacto (*Component Failure Impact Analysis*) sus iniciativas, determinando las causas, analizando amenazas y tomando cualquier acción apropiada para garantizar que el servicio sea disponible cumpliendo con los SLAs.

Las actividades que incluye la Gestión de la Disponibilidad son:

- Garantizar que el servicio este disponible conforme los SLAs
- Determinar la causa de fallos en la disponibilidad
- Revisar los requerimientos del negocio para la disponibilidad de los sistemas empresariales
- Catalogación de los requerimientos del negocio (misión, objetivos de la organización)
- Garantizar un apropiado plan de contingencia, puesto en marcha y probado.
- Establecimiento de alta disponibilidad, sistemas redundantes para apoyar a las aplicaciones criticas en la misión de la organización.

3.1.2.5 Gestión de las Finanzas (Financial Management)

El objetivo de la Gestión de finanzas es Proporcionar la "generación" costo-efectiva (*stewardship*) de los activos y recursos utilizados para proveer el servicio de TI

Proveer servicios a un costo razonable depende de 3 factores:

- **Calidad** – en términos operativos de capacidad, disponibilidad, desempeño, recuperación en caso de desastre y soporte
- **Costos** – en términos de gastos e inversiones
- **Requerimientos del cliente** – alineado a sus necesidades

Para que una organización externa (*Outsourcing*)[41] de TI o una organización de TI la cual es realizada como si se tratara de una entidad separada, el objetivo puede ser descrito como:

Para ser capaz de explicar plenamente el gasto en los servicios de TI y ser capaz de atribuir estos costos a la entrega de los servicios, prestados por la organización, a los clientes y asistir en la administración proveyendo los detalles y los costos de los casos de negocio[42] para proponer cambios en los servicios de TI.

A continuación se detalla cada uno de los subprocesos de la Gestión de Finanzas.

3.1.2.5.1 Subprocesos de la Gestión de Finanzas

La Gestión de las Finanzas para los servicios de TI contiene tres subprocesos:

- Presupuestar *(Budgeting)*.- predecir costos, comparación de gastos versus ingresos, reducir el riesgo de sobre-gastar, asegurar que hay suficiente para cubrir los gastos planeados)
- Seguimiento de las TI (*Accounting*) contabilizar los gastos, distribuir los costos de TI a clientes externos e internos, análisis ROI (*Return of Investment*)-caso de negocio (*business case*), identificar los costos de los cambios
- Tarifar, designación de Costos (Charging).- recuperar los costos de los servicios de TI, operar TI como unidad de negocio, influenciar el comportamiento de los clientes y usuarios

3.1.2.5.1.1 Presupuestar

El presupuestar permite que una organización tenga un plan previsto de gastos relativos a las TI, lo que reduce el riego de excederse, en cuanto a la inversión realizada, y garantizando que los ingresos están disponibles para cubrir los gastos

[41] *Outsourcing* pasó a formar parte del léxico de negocios durante la década de 1980 y se refiere a la delegación de las operaciones no esenciales de la producción interna a una entidad externa especializada en la gestión de esta operación. *Outsourcing* es la utilización de expertos de fuera de la entidad para llevar a cabo tareas específicas que la entidad una vez realizadas las tomara a su cargo.
[42] Véase Anexo C Formato de Caso de Negocio (Business Case)

previstos. Además esto permite a una organización el comparar los gastos reales con los previstos con anterioridad, con la finalidad de mejorar la confiabilidad de las predicciones al presupuestar.

3.1.2.5.1.2 Seguimiento de las TI

El seguimiento de las TI se refiere a la cantidad de dinero gastado en la prestación de Servicios de TI. Esto permite a una organización la realización de varios análisis financieros para determinar la eficiencia de la provisión de los servicios de TI y determinar las áreas donde se realizan ahorros. Esto también proveerá de transparencia financiera para auxiliar a la administración en el proceso de toma de decisiones.

Varios elementos de costos se pueden considerar para el control del seguimiento. Como se enumeran a continuación:

1) **Costos directos (*direct costs*)**

Costos relacionados de manera específica, exclusiva y completamente con un producto o servicio, donde las actividades y materiales pueden estar directa o indirectamente asociadas con el centro de costo o departamento. Ejemplo: pueden ser servidores o personal de soporte.

2) **Costos indirectos (*indirect costs*)**

Costos que no se asocian específica y únicamente a un servicio de TI y/o a un centro de costos o departamento. Ejemplo: incluyen las instalaciones, servicios de soporte, costos administrativos. Absorbidos o no absorbidos

3) **Costos fijos**

Independientemente del volumen de producción estos costos son los mismos mes a mes. Comúnmente son las inversiones en *hardware, software* y edificio, a los cuales en muchos casos se les considera su depreciación mensual, más que el precio de compra. Los costos fijos continúan aún y cuando se disminuya o se interrumpa el volumen de servicios.

4) **Costos variables**

Son los costos que cambian cuando el volumen de producción cambia. Ejemplos: personal externo, consumibles. Estos costos están ligados con los servicios proporcionados, cuando el nivel de producción incrementa los costos también lo hacen.

5) **Costos de capital**

Estos costos se aplican a los activos físicos de la organización para su uso a largo plazo. Los costos de capital son la compra o arreglo de los activos (Ejemplo: equipo de cómputo). Los costos de capital se deprecian sobre un número de años. Los costos se toman por la depreciación más que por el precio de compra.

6) Costos de operación

Costos resultados de la operación día a día de los servicios de TI. Ejemplo: costo del personal, contratos de mantenimiento de *hardware y software*, costo de licencias y los pagos repetitivos cuyos efectos puedan ser medidos en tiempos, costos, usualmente menores a 12 meses, año financiero.

3.1.2.5.1.3 Tarifar (Designación de Costos)

La designación de costos otorga la posibilidad de asignar los costos de servicios de TI de una manera proporcional y equitativa para los usuarios de estos servicios. Esto puede ser utilizado como un primer paso hacia la operación de las TI en la organización como un negocio autónomo. Esto también puede ser utilizado para alentar a los usuarios a avanzar hacia una importante dirección estratégica, por ejemplo para subsidiar nuevos sistemas e imponiendo cargos adicionales por la utilización de sistemas antiguos. La transparencia de la tarifación animará a los usuarios a evitar actividades costosas lo que incomoda ligeramente pero se llegará a alternativas disponibles más baratas. Por ejemplo un usuario puede navegar en una pantalla capturada en lugar de imprimirla.

La designación de costos, es posiblemente, el más complejo de los tres subprocesos requiriendo una gran inversión de recursos y un alto grado de atención para evitar anomalías, donde un departamento en particular puede beneficiarse de un comportamiento perjudicial para la compañía en su conjunto. La política de asignación de costos tiene que ser al mismo tiempo: sencilla, equitativa y realista. Esta asignación de costos no significa necesariamente dinero cambiando de manos. Puede tomar la forma de información, pasada a la administración sobre los costos de proveer los servicios de TI.

3.2 Planificación para la aplicación de la Administración de los servicios (Planning to Implement Service Management)

La planificación para la aplicación de la administración de los servicios es un conjunto dentro del marco de referencia ITIL que trata sobre las necesidades para la alineación del negocio y los requisitos provistos en las TI, describe como implementar o proveer la administración de los servicios de TI (*IT Service Management*)

Un enfoque para aplicar y mejorar la administración de servicio (*Service Management*) es el Programa de mejora Continua de Servicios (*Continuous Service Improvement Program*), CSIP, queda definido como un programa formal en curso dentro de una organización para identificar e introducir mejoras dentro de un área de trabajo o proceso de trabajo[11] . Este programa consiste en de los siguientes pasos en relación con una sola mejora:

a. Crear la visión

El primer paso que se ha de tener en el proceso es la creación de una declaración de visión para una CSIP. La declaración de visión describe el objetivo y el propósito de la CSIP a un alto nivel y debería adecuar las diferentes estrategias de negocio y TI. Además, la declaración sobre la visión debe estar bien comunicada las partes interesadas, para crear el compromiso y la aprobación del Programa de Mejora Continua de Servicios.

b. Analizar a la organización.

Después de haber creado una visión de las TI en la organización debe analizarse esta. Una útil técnica para determinar la posición actual de la organización es mediante un modelo de crecimiento de las TI en la organización. Este modelo determina el nivel de madurez de las TI en la organización y se basa en *Process Maturity Framework* (PMF) así como en el *Capability Maturity Model* (CMM), estos marcos de referencia quedán fuera del alacance de este trabajo por lo que solo se hace un abreve descripción a este respecto. En cuanto al PMF se integra dentro de ITIL como más adelante se observa.

La madurez de la organización se determinará en función de la visión y la estrategia, la dirección, los procesos, las personas, la tecnología y la cultura. También es necesario para entender quiénes son los interesados, porque las partes interesadas tienen un impacto en el Programa de Mejora Continua de Servicios (CSIP). Esto puede lograrse mediante la definición, la identificación y su relación con las partes interesadas. Adicionalmente, las necesidades específicas de las partes interesadas tienen que ser identificadas y esto puede dar lugar a un informe de evaluación de interesados.

El tercer paso es el análisis de la organización, consiste en evaluar el informe actual y las mediciones del sistema. Conocer la actual forma de uso y la elaboración de informes, datos y cifras da una idea de qué tan bien se ha dirigido la organización, sino que también proporcionará información acerca de la próxima actividad en los objetivos fijados.

El último paso en el análisis de la organización es la realización de los puntos de referencia. Un punto de referencia útil es una técnica de gestión para mejorar el rendimiento. En un punto de referencia diferentes partes de la organización se puede comparar, al igual que las unidades o procesos. Pero también las organizaciones como un todo pueden ser comparadas en un punto de referencia Es importante para determinar si un proceso de gestión de los servicios debería evaluarse de forma comparativa o no. El énfasis en los procesos de gestión de los servicios es esencial. Los resultados de los puntos de referencia pueden resultar en la identificación de huecos.

c. Establecimiento de metas

La siguiente actividad en el CSIP es sobre el acuerdo entre el negocio y las TI, respecto a los requerimientos y expectativas a futuro como las funciones y características de la organización, que se basan en la madurez actual de la organización. La primera medida que debe adoptarse es la creación de un modelo de

negocio, para describir el valor añadido y la justificación de la CSIP. El argumento empresarial es determinado por la madurez actual de la organización y la estrategia de la organización. Una Evaluación de los interesados, que se realizó en la actividad anterior, también puede ser una contribución para enfocar los resultados y el objetivo del programa de mejora.

Además los riesgos deben ser identificados y administrados. Un enfoque de la gestión de riesgos deben aplicarse durante el CSIP. Principalmente los riesgos relacionados con la visión empresarial, los procesos existentes y el medio ambiente de negocios y limitaciones deben ser administrados para reducir los efectos de esos riesgos.

Después de haber creado un modelo de negocio, un informe de la evaluación de las omisiones debe ser completado. Un informe de la evaluación de las omisiones o brechas es utilizado para comparar el estado actual con el estado futuro de la organización, además de los resultados de estas lagunas para superarlas, es decir, el donde se desea posicionar a la organización, donde se quiere estar. Esto proporciona información acerca de las lagunas, los riesgos y el establecimiento de prioridades sobre dónde iniciar. Una vez completado el informe de evaluación de estas omisiones, actividad necesaria para su comprensión y claridad de los problemas y los siguientes pasos que se han presentado a los principales interesados, a fin de establecer la credibilidad de la evaluación y el apoyo en relación con el cambio.

El siguiente paso es la creación de un plan de objetivos rápidos. Una rápida victoria es un éxito temprano en un programa de mejora. En el plan de metas rápidas, metas a corto plazo deben ser identificadas y alcanzadas para mantener el programa de mejora en funcionamiento, además de mantener el compromiso de alto nivel en el programa de mejora.

El último paso es la fijación de objetivos en relación con el programa de mejora en relación a la anterior definición de las necesidades de las partes interesadas. Una herramienta de gestión para el establecimiento de objetivos y la medición de los resultados para establecer un equilibrio en el cuadro de mando integral, es decir, entre los niveles jerárquicos de la empresa.

d. Llevar a la práctica la Administración de los servicios de TI

Antes de la identificación de un proceso, hay que identificar que es necesario mejorar, la primera condición que debe cumplirse es que la organización deberá documentar su estado actual y el estado deseado, que incluye un informe completo de evaluación y de las omisiones. También depende del nivel de madurez y de los objetivos estratégicos de la organización. Además de estas dependencias, es importante comprender la interrelación entre todos los procesos de Administración de los Servicios de TI (*IT Service Management processes*).

Otro aspecto que debe tenerse en cuenta durante el programa de mejora es la creación de conciencia del cambio. Esto puede hacerse mediante un plan de comunicación, que dará una explicación acerca de la política en materia de TI a las partes interesadas.

La próxima cosa a considerar es cómo los cambios van a ser alcanzados. El lograr los cambios requiere de un programa de cambio fiable.

La cultura de la organización es la cuestión principal que debe tenerse en cuenta durante el cambio de organización, debido a que los cambios en la organización podrían apoyar una aplicación determinada, que ya se utiliza y esto puede dar lugar a resistencia al cambio. Por este motivo, la cultura de la organización debe ser gestionada con el fin de evitar problemas como la resistencia al cambio.

Un factor crítico del éxito de una CSIP es la definición clara de la rendición de cuentas, las funciones y la responsabilidad en relación con los nuevos procesos y la estructura existente de la organización. Los nuevos procesos y prácticas de trabajo a menudo no se adecuan con la existente estructura organizacional, por que los procesos se entrelazan en cuanto a lo funcional se refiere. En otras palabras, los procesos pueden correr a través de toda la organización. De esta forma, los nuevos procesos y prácticas de trabajo pueden introducir nuevas funciones, que pueden superponerse a la actual estructura de la organización.

El último aspecto que debe ser tomado en cuanta con respecto a la implementación de la Administración de los Servicios de TI, es la capacitación, ésta puede contribuir a una mayor calidad en la Administración de servicios y esto encabezaría hacia una mayor productividad y asimilación de los empleados.

3.2.1 Marco de Referencia en el Proceso de Madurez (Process Maturity Framework)

Un marco de referencia de madurez proporciona el contexto para medir la madurez organizacional. El PMF[43] puede ser utilizado para medir el punto de referencia o un proceso en particular dentro de una organización, o la prestación de servicios de un tercero a la organización. El PMF es útil para el examen de la totalidad de servicios del Programa de Mejora Continua (CSIP) y aplicado a todos los procesos de ITIL, o un proceso individual.

El PMF supone que un Sistema de Gestión de Calidad (SGC)[44] es parte de la organización y hay un objetivo de mejorar uno o más aspectos de los procesos de la eficacia, la eficiencia, la economía, o la equidad.

El ITIL PMF tiene cinco niveles que se enumeran a continuación:

Nivel	PMF	Enfoque	Comentarios
1	Inicio	Technología	Tecnología de excelencia y expertos
2	Repetible	Producto / Servicio	Procesos operacionales (por ejemplo el Servicio de Asistencia [*Service Support*])

[43] PMF por sus siglas en ingles, *Process Maturity Framework,* Marco de Referencia en el Proceso de Madurez

[44] En la literatura relacionada puede referirse a las siglas QMS que significa en ingles *Quality Management System*

Nivel	PMF	Enfoque	Comentarios
3	Definir	Enfoque del Cliente	La Adecuada Gestión de nivel de servicio
4	Administrar	Enfoque del Negocio	La alineación del negocio y las TI.
5	Optimizar	Valor en la Cadena	Perfecta integración de las TI en el negocio y la creación de una estrategia.

Tabla 2 ITIL PMF

El PMF ITIL define varias dimensiones que conforman cada nivel. A determinado nivel de madurez es el resultado de los siguientes factores:

- Visión y Estrategia - "la dirección general en lo que se refiere al papel y la posición de la TI dentro de la empresa"
- Directivo - "los objetivos y metas de TI en relación con la realización de la estrategia"
- Procesos de "los procedimientos necesarios para alcanzar las metas y los objetivos"
- La gente - "los conocimientos y habilidades necesarios para llevar a cabo los procesos"
- Tecnología - "la infraestructura de apoyo para que los procesos que se lleven a cabo"
- Cultura - "el comportamiento y la actitud necesaria en relación con el papel de la TI dentro de la empresa"

Se debe tomar en cuenta que para pasar de un nivel a otro se requieren cambios sustanciales en cada una de las dimensiones.

3.3 Administración de las Aplicaciones (Application Management)

La Administración de aplicaciones es un conjunto de buenas prácticas propuestas para mejorar la calidad general de las TI, el software desarrollado y el soporte a proyectos durante todo el ciclo de desarrollo de software, con la atención particular a la reunión y definición de las necesidades que satisfacen los objetivos de negocio. El ciclo de desarrollo se ha explicado anteriormente[45].

[45] Véase apartado Ciclo de Vida del Desarrollo de un Sistema-SDLC (System Development Life Cycle) y el apartado Fases del SDLC, en el capítulo 1.

3.4 Gestión de la Seguridad (Security Management)

La Gestión de la seguridad describe la estructura apropiada de seguridad de la información en la administración de la organización.

Un concepto básico de la Gestión de seguridad es las propiedades de seguridad de la información, descritas en el capítulo 1. Aunque cabe mencionar, que es imposible garantizar la disponibilidad como servicio, por lo cual se intenta acotar el riesgo, mediante la implementación de controles y el apego a las políticas de la organización, además de las buenas prácticas. El objetivo principal de la seguridad de la información es garantizar la seguridad de la información. El asegurar la información es la protección de esta contra un riesgo determinado, como se ha mencionado en los capítulos anteriores.

- Proceso de la Gestión de la Seguridad

El Proceso de Gestión de la Seguridad consiste en las actividades que se llevan a cabo por la gestión de la seguridad de sí mismo o de las actividades que son controladas por la Gestión de la Seguridad, su objetivo es asegurar el nivel de seguridad convenido en los SLAs y en requerimientos externos definidos en contratos, leyes y políticas, además de proveer el nivel básico de seguridad independiente de externos.

Debido a las organizaciones y sus sistemas de información en constante cambio. Las actividades dentro del Proceso de Gestión de la Seguridad deben ser revisadas continuamente, con el fin de permanecer actualizados y eficaces, la Gestión de la Seguridad es un proceso continuo.

Las entradas en este proceso son los requerimientos los cuales son formulados por los clientes. Las necesidades se traducen en servicios de seguridad, la calidad de la seguridad será provista en base a estos requerimientos lo cual debe estar estipulado en la sección de acuerdos de nivel de servicio. Tanto los clientes y el plan de subprocesos tienen entradas en los acuerdos de Nivel de Servicio SLA y los niveles de servicio son una entrada para ambos los clientes y los procesos. El proveedor entonces desarrolla planes para la seguridad de la organización, en estos planes se contienen las políticas de seguridad y los Acuerdos de Nivel Operacional (OLA) Los planes de seguridad se implementan, y la aplicación se somete a evaluación. Después de la evaluación, tanto los planes y la ejecución de estos se mantienen.

Las actividades, los resultados y los productos, además del proceso son documentados. Los reportes externos se redactan y envían a los clientes Los clientes son capaces de adaptar sus necesidades sobre la base de la información recibida a través de los informes. Además, el proveedor de servicios puede ajustar su plan o de la aplicación sobre la base de sus conclusiones con el fin de satisfacer todos los requisitos establecidos en el Acuerdo de Nivel de Servicio (*Service Level Agreement SLA*), incluyendo los nuevos requerimientos.

- Control

La primera actividad en la Gestión de Seguridad es el subproceso de Control, este subproceso organiza y maneja el proceso de gestión de seguridad, la asignación de responsabilidad esta declarado en la política y en el marco administrativo.

El marco de trabajo de la gestión de la seguridad define los subprocesos para: el desarrollo de planes de seguridad, la aplicación de los planes de seguridad, la evaluación y la forma en que los resultados de las evaluaciones se traducen en planes de acción. Por otra parte, el marco de gestión define cómo deben comunicárseles a los clientes.

Las actividades que tienen lugar en el Control de Procesos se resumen en el cuadro siguiente.

Actividades	Sub-actividades	Descripción
Control[46]	Implementación de políticas	Este proceso esboza los requerimientos específicos y las reglas que tienen que ser cumplidas a fin de aplicar la gestión de la seguridad. El proceso termina con la declaración de políticas[47].
	Configuración de la seguridad de la organización	Este proceso ubica a la organización para proveer seguridad de la información. Por ejemplo en este proceso la estructura de responsabilidades es creada. Este proceso termina con un marco de trabajo en la gestión de la seguridad[48]
	Presentación de informes	Todo lo que ha sido enfocado durante todo el proceso es documentado de una forma especifica. Este proceso termina con la realización de informes.

Tabla 3 Actividades del Control de Procesos

La Implementación de políticas y la configuración de la seguridad de la organización son dos actividades que no necesariamente son secuenciales, es decir, desordenadas, después de que estas dos actividades se han llevado a cabo la actividad de presentación de informes es secuencial.

- Planear

El subproceso de planear contiene actividades que en cooperación con la Gestión de Nivel de Servicio conduce hacia la seguridad de la información en la sección de los acuerdos de nivel de servicio (*Service Level Agreements*). En este subproceso el

[46] Control es una descripción de cómo la GESTIÓN DE LA SEGURIDAD será organizada y la forma en que será administrada.
[47] Declaración de políticas son los documentos que se exponen los requisitos específicos o normas que deben cumplirse. En el ámbito de seguridad de la información, las políticas son generalmente un punto específico, que abarca un espacio único. Por ejemplo, el "Uso Aceptable" la política abarcaría las normas y reglamentos para el uso adecuado de las instalaciones de computo.
[48] Marco de trabajo en la gestión de la seguridad es el marco de referencia donde se establece la administración para iniciar y controlar la implementación de la seguridad de l a información dentro de una organización y poner en curso la disposición de la seguridad de la información.

objetivo formulado en el Acuerdo de Nivel de Servicio es especificado en la forma de Acuerdos de Nivel Operacional (*Operacional Level Agreements OLA*). Estos OLAs pueden ser definidos como planes de seguridad especificos para la organización interna de la entidad proveedor de servicio.

Además de la aportación de los Acuerdos de Nivel de Servicio (SLA), El subproceso de planear también trabaja con lo establecido en la política del proveedor de servicio en sí. Como se menciono con anterioridad la declaración de políticas es definida en los subprocesos del Control.

Los Acuerdos de Nivel de Servicio (OLA) para la seguridad de la información esta configurada y basada en los procesos de ITIL. Esto significa que son cooperativos con otros procesos de ITIL.

Por ejemplo, si la gestión de la seguridad desea cambiar la infraestructura de TI a fin de lograr la máxima seguridad, estos cambios sólo se ejecutará a través del proceso de gestión de cambios. La gestión de la seguridad deberá entregar las aportaciones (esto en forma de RFCs, Requerimiento para cambio) para este cambio. El manejo de los cambios es responsabilidad de la gestión de cambio.

A continuación se muestran las actividades de planear y sus sub-actividades con su definición.

Actividades	Sub- actividades	Descripción
Planear[49]	Crear la sección de seguridad en los acuerdos de Nivel de servicio (SLAs)[50]	Este proceso contiene las actividades que llevan a los acuerdos de seguridad en el párrafo acuerdos de nivel de servicio. Al final de este proceso la sección de seguridad en los acuerdos de nivel de servicio es creada
	Crear los contratos externos (*Underpinning Contract*)[51]	Este proceso contiene las actividades que llevan a contratos de servicio acordado (*underpinning contrats*). Estos contratos son específicos para la seguridad.
	Crear acuerdos de Nivel operacional (OLAs)[52]	Los objetivos generales formulados en el SLA se especifican en el Acuerdo de Nivel Operacional (OLA). El OLA puede verse como planes de seguridad específicos para una unidad de la organización.
	Presentación de Informes	Es creado todo el plan, el proceso es documentado de una manera específica. Este proceso termina con la generación de reportes.

Tabla 4 Sub actividades y su descripción en el subproceso de Planear

[49] Planear, esquemas formulados para los acuerdos de seguridad.
[50] Sección de seguridad de los acuerdos de Nivel de seguridad. Es el párrafo de los acuerdos de seguridad por escrito entre un proveedor de servicios y el cliente que los documenta de acuerdo con el nivel de servicio en sí
[51] Contratos de servicio acordado (*underpinning contrats*) es un contrato con un proveedor externo que cubre la entrega de Servicios que apoyan a las TI de la organización en su prestación de servicios.
[52] Acuerdo de Nivel operacional (OLA) es un acuerdo interno que abarca la entrega de servicios los cuales soporta las TI de la organización en la prestación de sus servicios

- Implementación

El subproceso de implementación se asegura de que todas las medidas, tal como se especifica en los planes, se apliquen adecuadamente. Durante este subproceso no se definen las medidas ni lo que ha cambiado. La definición o cambio de las medidas se llevará a cabo en el subproceso de planeación en cooperación con el proceso de Gestión de cambios.

Las actividades que toman lugar en el subproceso de implementación son descritas en la siguiente tabla.

Actividades	Sub-actividades	Descripción
Implementación	Clasificación y gestión de las aplicaciones de TI	Procesos de agrupación formal de los elementos de configuración (CI), por tipo por ejemplo, software, hardware, documentación, ambiente, aplicaciones. Proceso formal de identificar cambios por tipo por ejemplo de los proyectos, alcance de la solicitud de cambios, validación de la solicitud de cambio, solicitud de cambios en la infraestructura. Este proceso conduce a la evaluación clasificación y control de documentos.[53]
	Implementación de personal de seguridad	Aquí se adoptan medidas a fin de dar seguridad y confianza al personal, además de las medidas para prevenir un fraude o crimen. Este proceso termina con la seguridad del personal.
	Aplicación de una administración segura	En este proceso se especifican los requerimientos de seguridad y/o las reglas que deben cumplirse, siendo estas delimitadas y documentadas. Este proceso termina con las Políticas de seguridad.
	Implementación de controles de Acceso	En este proceso se especifican los requerimientos de seguridad en cuanto acceso y/o el acceso a las reglas que deben de ser cumplidas se delimitan y documentan. Este proceso termina con el Control de Acceso[54]
	Presentación de Informes	Toda la implementación es planeada y el proceso se documenta en una forma especifica

Tabla 5 Sub-actividades y su descripción en el subproceso de implementación

[53] Evaluación clasificación y control de documentos en un inventario exhaustivo de los bienes con la responsabilidad asignada para asegurar que protección eficiente es mantenida.

[54] Control de acceso mediante la Administración de la red para asegurar que únicamente aquellos que tiene la responsabilidad adecuada tengan acceso a los recursos e información en las redes además del apoyo en la protección infraestructura.

3.5 Gestión de la Infraestructura- Tecnología de la Información y las Comunicaciones (ICT Infrastructure Management)

La gestión de la infraestructura de tecnología de la información y las comunicaciones (ICT) son procesos recomendados en las mejores practicas para el análisis de requerimientos, planeación diseño, desarrollo y operaciones en curso de soporte tanto administrativos y técnicos de la infraestructura de ICT.

El proceso de gestión de la Infraestructura describe estos procesos dentro de ITIL que directamente se relaciona con el equipamiento de ICT y el software que está involucrado en la prestación de servicios hacia los clientes

A continuación se describen estos procesos recomendados en las mejores prácticas.

- **Diseño y Planeación de las ICT**

El diseño y planeación de las ICT proporciona un marco de trabajo y un enfoque para el diseño técnico y estratégico, además de la planeación de la infraestructura de ICT. Esto incluye la necesaria combinación de estrategia de negocios, con técnicas de diseño y de arquitectura. El diseño y planificación de las ICT[55] conduce ambos, la procuración de las nuevas soluciones de ICT, mediante la producción de las declaraciones de requerimientos (SOR)[56] o licitaciones u ofrecimientos (ITT)[57] y es responsable por la iniciación y administración de los programas de ICT para el cambio estratégico del negocio. Las salidas claves provenientes del Diseño y la planeación son:

- Las Estrategias en las ICT, Políticas y Planes.
- La arquitectura global de las ICT, además de la administración de la Arquitectura.
- Los casos de Negocio[58] [12], estudios de viabilidad, licitaciones y declaración de Requerimientos (SoRs).
- Desarrollo de la gestión de la ICT este último se refiere:

A proveer un marco de referencia para el éxito de la gestión del diseño, construcción, pruebas y la puesta en marcha (desplegar) de los proyectos con un programa global de las ICT. Esto incluye la administración de los proyectos.

---

[55] ICT es un acrónimo de tecnología de la información y las comunicaciones
[56] La declaración de los requisitos o SoR por sus siglas en ingles de *Statements of Requirement*
[57] ITT por las siglas en ingles Information Technology Tender, Licitaciones referentes a TI.
[58] El caso de negocio se utiliza para obtener el compromiso de la administración y la aprobación para la inversión en cambios en el negocio, a través de la justificación de la inversión, El caso de negocio propone un marco de trabajo para la planificación y administración de los cambios en el negocio. La viabilidad del proyecto en curso deberá ser monitoreado contra el caso del negocio, este debe de contener información que cubre cinco aspectos fundamentales: ajuste estratégico, las opciones de evaluación, aspectos comerciales, el que pueda conseguirse o alcanzarse y la adecuación.

- **La Gestión de Operaciones de ICT**

La Gestión de Operaciones de ICT provee la supervisión técnica en la infraestructura día a día. Puede relacionarse en cierto sentido con la Gestión de incidentes del *Service Support*, las operaciones es más bien técnico y no se refiere únicamente a los incidentes reportados por los usuarios, sino a eventos generados por registros en la infraestructura. Las operaciones de las ICT pueden, a menudo, trabajar estrechamente junto a la gestión de incidentes y *Service Desk*, que no son necesariamente técnicos, con el fin de proporcionar un "puente de Operaciones'. Las operaciones sin embargo, deben primeramente trabajar desde los procesos y procedimientos documentados y debería ocuparse de un cierto número de sub.-procesos como son: Respaldos y almacenamiento, monitoreo y administración de la red, sistemas de administración y monitoreo, Administración y monitoreo en bases de datos, Almacenamiento (administración y monitoreo), entre otras, las operaciones son responsables por:

- Una estable y **segura** infraestructura de ICT
- La actualización de la Biblioteca de documentación Operacional *(Operational Documentation Library ODL)*
- Un registro de todos los eventos operacionales
- Mantenimiento de operativos de vigilancia y gestión.
- *Scripts* de Operaciones
- Procedimientos Operacionales

- **Soporte Técnico en las ICT**

El Soporte Técnico en las ICT es especialista en la función técnica de la infraestructura dentro de las ICT. Principalmente como apoyo a otros procesos, tanto en la Gestión de Infraestructura y la Administración del servicio (*Service Managenement*), el soporte técnico provee de una serie de funciones especializadas: Investigación y Evaluación, *Market Intelligent*[59] [13] (en particular para Diseño y Planificación y Gestión de la Capacidad), Pruebas de concepto (PoC) y pilotos de ingeniería, especialistas en conocimientos técnicos (en particular relacionados a Problema de Operaciones y Gestión), la creación de la documentación (quizás por la Biblioteca de Documentación operacional o errores conocidos, que yacen en una base de datos).

[59] *Market Intelligence* (MI) – es la información relativa a los mercados de una empresa, se reúnen y analizan específicamente con el fin de precisar y confiar en la toma de decisiones en la determinación de oportunidades de mercado, en la estrategia de penetración en el mercado, en el desarrollo de los mercados y las nuevas cifras, es decir, es el proceso de adquirir y analizar la información a fin de comprender el mercado (tanto los clientes actuales y potenciales), para determinar las necesidades actuales, futuras y las preferencias, además de las actitudes y el comportamiento del mercado, y evaluar los cambios en el entorno empresarial que pueden afectar el tamaño y la naturaleza del mercado en el futuro.

3.6 La Perspectiva del Negocio (The Business Perspective)

La perspectiva del negocio es el nombre dado a la colección de mejores prácticas que son sugeridas para direccionar algunos de las cuestiones que a menudo son encontradas en el entendimiento y el perfeccionamiento de la provisión de servicios de TI, como parte de los requerimientos de todo el negocio es la exigencia de una alta calidad de la administración. Estas cuestiones son:

- **La Gestión de Continuidad del negocio** describe las responsabilidades y oportunidades disponibles para el administrador del negocio para mejorar lo que es, en la mayoría de las organizaciones uno de los servicios claves que contribuyen a la eficiencia y la eficacia de los negocios

- **Sobrevivencia al cambio**. Los cambios en la infraestructura de TI pueden impactar de una manera en la cual el negocio es conducido o en la continuidad de las operaciones. Es importante que los administradores del negocio tomen nota de estos cambios y garanticen que los pasos son tomados para salvaguardar al negocio de efectos secundarios adversos.

- **Transformación de las prácticas empresariales a través de un cambio radical** ayuda para controlar las TI e integrar estas en el negocio.

- **Las asociaciones y la contratación de externos**

3.7 BSM

La finalidad del *Business Service Management*[60] es la de unir el negocio con la infraestructura de TI para proporcionar servicios, es decir, la dependencia operacional con una visión transaccional, en un marco de trabajo organizado en varios aspectos como lo muestra la figura siguiente. Relación de la infraestructura tecnológica y el Negocio.

BSM está basado en el modelo de ITSM, que es un conjunto de disciplinas generalizadas, al igual que ITIL, con la finalidad de evitar el acaparamiento del mercado por una marca (un monopolio), es considerado una metodología y por lo tanto no está casada con un conjunto de productos.

Las empresas interesadas en aprovechar al máximo su infraestructura informática enfrentan numerosos problemas, que podemos resumir como: complejidad, visibilidad, priorización y costos.

Mientras la infraestructura crece en complejidad con la integración de múltiples servidores, aplicaciones, bases de datos y dispositivos, al departamento de

[60] Gestión de sistemas, aplicaciones y procesos productivos alineada a objetivos de negocio

informática le resulta cada vez más difícil comprender las prioridades del negocio y visualizar la forma en que un pequeño fallo en un componente tecnológico puede tener un impacto grave en un servicio de negocio completo.

Igualmente difícil resulta discernir y descartar aquellos fallos técnicos que, aún teniendo una cierta importancia a nivel técnico, en realidad no tienen ningún impacto significativo en el negocio (por ejemplo, cuando un componente particular está replicado, existe una solución alternativa o el problema se da fuera del intervalo crítico de disponibilidad).

La no **visibilidad** de los procesos de negocio y la dificultad al **clasificar y procesar** los eventos impiden la adecuada **priorización** de los problemas que afectan la infraestructura y los resultados de negocio.

Esto se debe a que las herramientas de monitorización disponibles, orientadas a la captura de eventos aislados, producen un elevado número de datos, pero poca información útil o manejable. Algunos estudios estiman que entre el 60 y el 80% del presupuesto de TI se dedica a la gestión de sistemas. Sin embargo, la mayoría de las empresas no dispone de ninguna herramienta para reflejar la relación entre sus servicios de negocio y la infraestructura tecnológica que los soporta.

Como si resolver el problema de la complejidad no fuese suficiente, al mismo tiempo las empresas deben cumplir estrictos objetivos de **nivel de servicio** y **reducir el coste total** de sus operaciones.

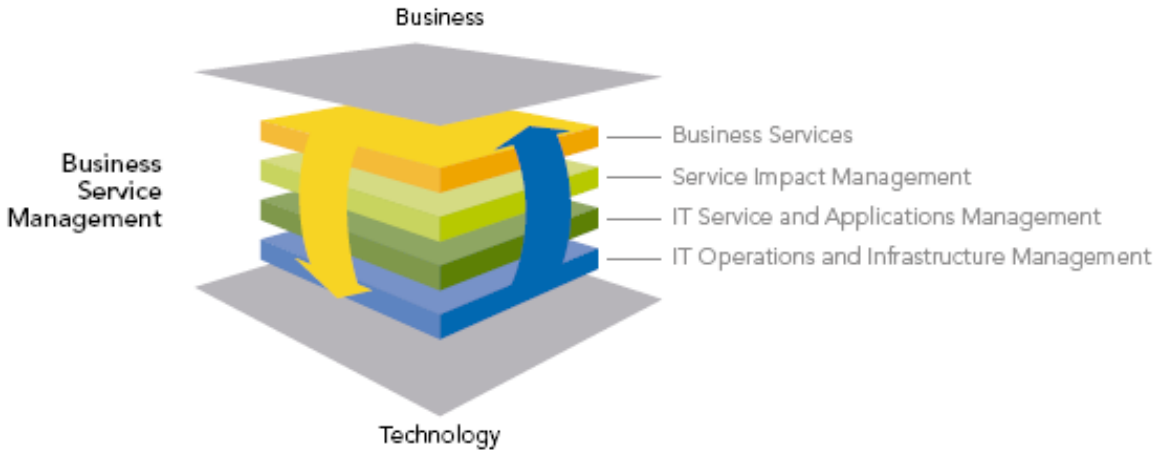

Figura 3 Relación de la Infraestructura Tecnológica y el Negocio

Business Service Management (BSM) es un proceso para la administración de los recursos de TI en aras de ofrecer el mayor valor al negocio. El objetivo del BSM es fácil de entender: Para administrar las inversiones de TI en alineación con las prioridades del negocio, con el fin de crear una ventaja competitiva. Business Service Management (BSM) es un enfoque tecnológico que se centra en un principio: dar **visibilidad a los procesos de negocio** de la empresa en lugar de en una colección

de componentes tecnológicos interrelacionados. Por ejemplo: en lugar de enfocarse en el estado de servidores, impresoras o redes, BSM proporciona una **visión integrada del estado de los procesos** de compra online, las líneas de producción, o las aplicaciones de gestión de pagos.

Operacionalmente el BSM son las mejores prácticas emergentes para la selección y utilización apropiada de los marcos de trabajo de administración en las TI, herramientas y conceptos (incluyendo software) que cubre:

Administración de Servicios de TI (*IT Service Management*) como proceso, BSM está firmemente arraigado en las mejores prácticas de *IT Service Management* como ITIL. Aunque ITIL no es la otra cara del BSM, ITIL se estableció como el precursor de las metas y objetivos de BSM con su enfoque en el valor comercial y la entrega de extremo a extremo en medición y monitoreo, por lo que ITIL es la forma más común de gestión de los servicios TI marco utilizado en BSM,

Gestión de la Calidad (*Quality Management*) BSM requiere de los elementos de un marco de calidad como Seis Sigma (*Six Sigma*) para la selección, el establecimiento de prioridades y la medición de oportunidades de mejora. Seis Sigma, Deming y Gestión Total de Calidad (*Total Quality Manegement* TQM)[61] [14] se usan comúnmente en BSM., Administración de Proyectos (*Project Management*) y Gobierno de TI *(IT Governance)*[62] [15]dispone de los límites de admisibilidad de las actividades de tecnologías de la información, teniendo en cuenta las necesidades comerciales incluidos los reglamentos, la legislación y el mercado.

BSM requiere monitorear múltiples sistemas de extremo a extremo, la manera en que se entrega el servicio versus la manera en que se aplica la TI, correlacionando el rendimiento de las operaciones de TI con el impacto en el negocio, es el distintivo de un efectivo BSM. Esto por la relación de la inversión y de la operación para los procesos de negocio, y produciendo métricas para cuantificar el impacto de los sistemas de TI sobre los procesos de negocio, BSM permite a los directivos de empresas tomar decisiones de inversión de TI basada en el valor y el riesgo, en lugar de simplemente tomar en cuenta los costos.

[61] Gestión Total de Calidad TQM por sus siglas en ingles *Total Quality Manegement* es una estrategia de gestion encaminada a la sensibilización de la introducción de la calidad en todos los procesos organizacionales. La Calidad Total proporciona un paraguas bajo el cual todos los miembros de la organización puede procurar la satisfacción de los clientes y crear continuamente inferior a los costos reales.

[62] *Information Technology Governance, IT Governance o ICT Governance*, en ingles, Gobernanza de Tecnología de la Información, Gobierno de TI o Gobierno de las TIC (Tecnologías de Información y Comunicaciones), en español, la disciplina es un subconjunto de Gobierno Corporativo que se centró en la tecnología de la información (TI), y en su rendimiento y Administración de riesgos. Se define como "*Especificación de los derechos y la decisión marco de rendición de cuentas para fomentar un comportamiento deseable en el uso de TI*" El creciente interés del gobierno de TI se debe en parte a iniciativas de cumplimiento (por ejemplo, Sarbanes-Oxley (EE.UU.) y Basel II (Europa)), así como el reconocimiento de que los proyectos de TI pueden fácilmente salirse de control y afectan profundamente el desempeño de una organización.

El concentrarse en el impacto que una incidencia puede tener en un servicio de negocio, más que en las incidencias técnicas aisladas, el personal de informática puede ser más efectivo, los niveles de servicio mejoran, las decisiones de inversión pueden efectuarse en forma más inteligente y los costes operacionales se ven reducidos.

Una perspectiva BSM implica poder gestionar de forma centralizada la **infraestructura** TI y establecer correlaciones entre ésta y la **actividad del negocio**. Mientras que la monitorización de la infraestructura TI se enfoca en áreas tales como sistemas, aplicaciones, seguridad y rendimiento, la gestión de los procesos de negocio monitoriza datos operativos e indicadores clave (KPIs)[63]

La siguiente figura muestra como está integrado el BSM y las relaciones entre los componentes.

[63] Indicadores clave de rendimiento, del inglés *Key Performance Indicators (KPI)*, miden el nivel del desempeño de un proceso, enfocándose en el "como" e indicando que tan buenos son los procesos, de forma que se pueda alcanzar el objetivo fijado

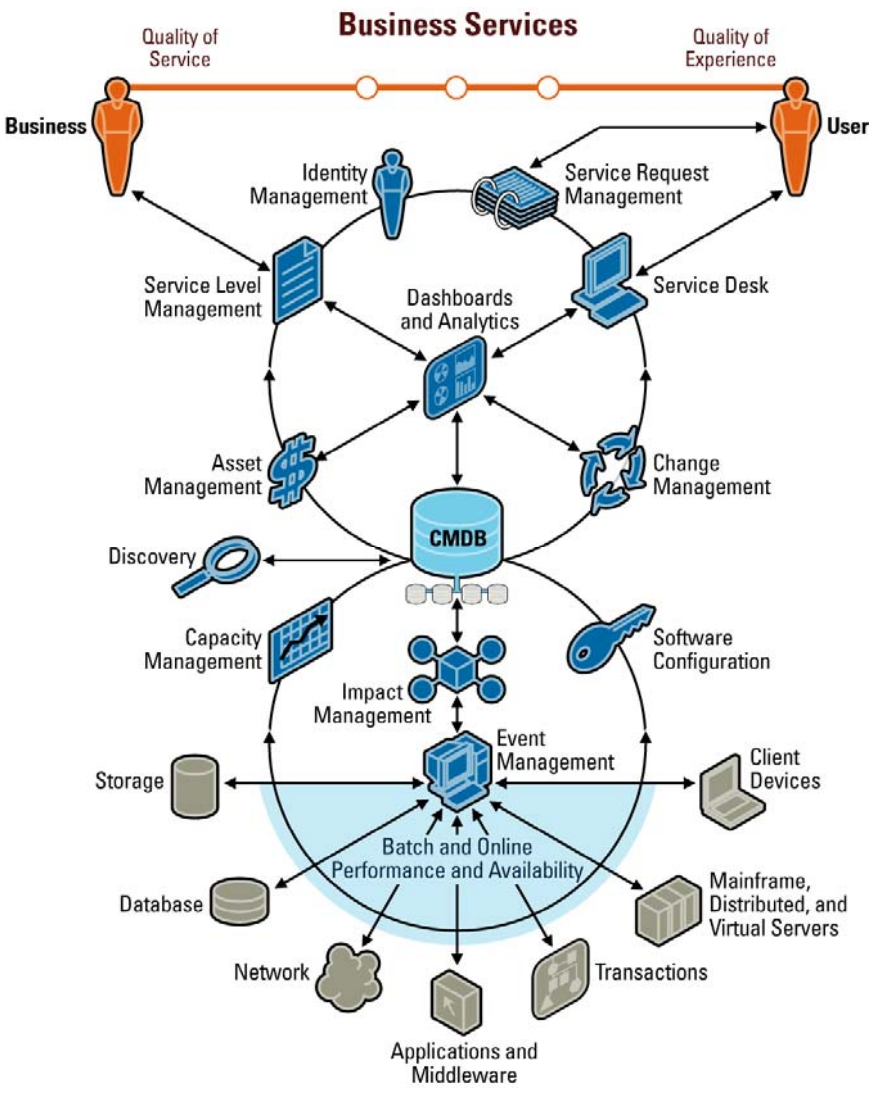

Figura 4 ***Business Service Management***

La CMDB ***Configuration Management Data Base***, es la base de datos que contiene los elementos de la infraestructura y las relaciones que cada uno de estos tiene con los demás componentes de infraestructura

El ***Discovery*** está ligado a la infraestructura y alimenta la Base de Datos de La Administración de Configuraciones CMDB (*hardware, software, topologías*), el ***Asset Management*** (Administración de Activos) permite el control de los activos mediante el seguimiento y control de los dispositivos en su ciclo de vida útil, este control de activos abarca desde los términos establecidos en los contratos de nivel de servicio y operacional, además de las características de mantenimiento.

El manejo de la configuración (*Configuration Management*) tiene una estrecha relación con el *discovery* proveyendo de información a la CMDB, a través del discovery es como se asocia con la CMDB, esto debido a que el *configuration Management* tiene como **objetivo** proveer con **información real** y **actualizada** de lo

que se tiene **configurado** e **instalado** en cada sistema del cliente, es decir, "*identificar, controlar, mantener y verificar las versiones de los elementos de configuración a fin de formar el modelo lógico de la infraestructura de TI*"[16], en cuanto al *Asset Managemet* compete solo la transición de estados y la documentación referente.

La responsabilidad de darle servicio al usuario afrontando las dudas e inquietudes de éste al igual que el de los clientes es del ***Service Desk*** es la cara del negocio aquí también se genera un modelo de control, que en conjunto con el *Configuration Management* y el ***Change Management*** dan solución a los problemas del usuario final de forma proactiva y sin necesidad de estar en sitio.

El *Change Management* dará la pauta en lo referente a fechas, previendo los problemas por falta de planeación y también se encargará de los cambios no previstos dando autorización o no a cualquier tipo de cambio mediante el control obteniendo información de la CMDB previamente poblada por el proceso de *Discovery*.

El ***Event Management*** se encarga del control de todo lo referente con la infraestructura permitiendo formar un modelo del proceso y su relación directa con el ***Impact Management*** le dará la prioridad debido a que aquí reside el modelado de los servicios (***Service Level Management***) donde se obtendrá el impacto que sufrirá el negocio por cambios y la afectación de componentes información que obtendrá directamente de la CMDB.

A continuación se explicarán el *Service Desk*, el *Asset Management* y el *Problem Management Proactive Event* y los componentes que se relacionan en un modelo focalizado excluyendo algunos componentes de la imagen previa para su mejor comprensión.

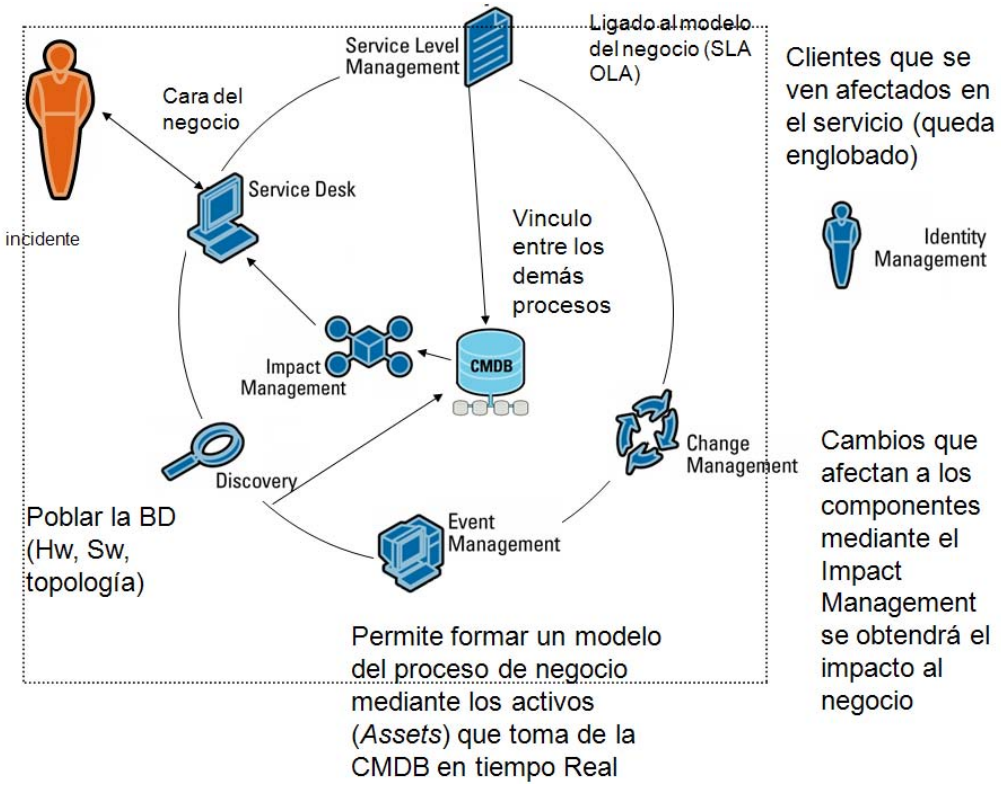

Figura 5 *Service Desk*

Si la resolución del problema no está en la CMDB el problema se escala o inclusive si este requiere para su resolución de planeación en cuanto al cambio de un componente se involucra también al *Change Management*.

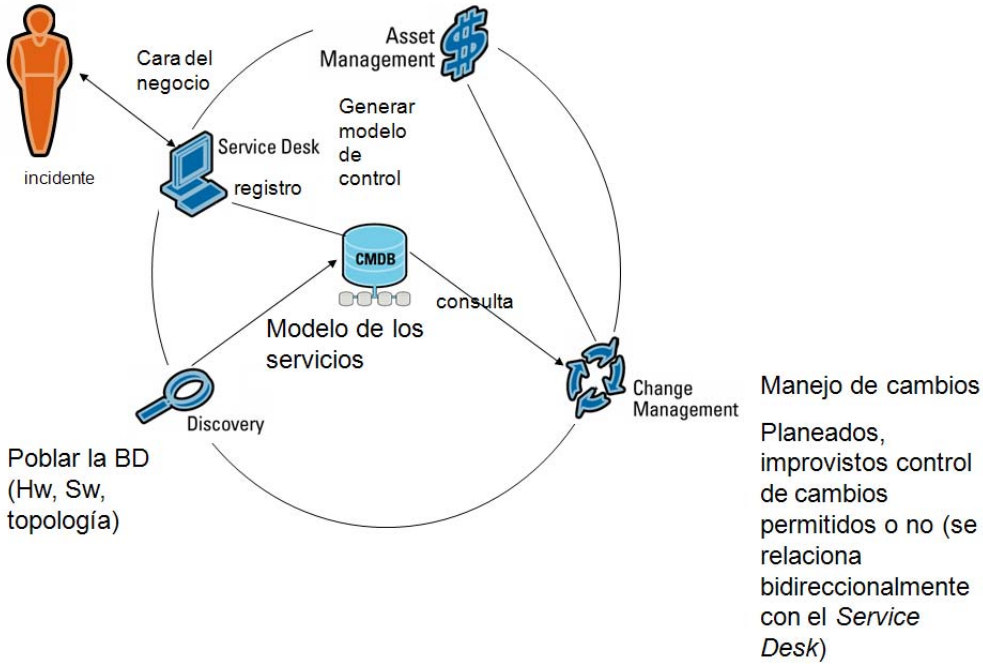

Figura 6 Interacción del Asset Management con los demás procesos

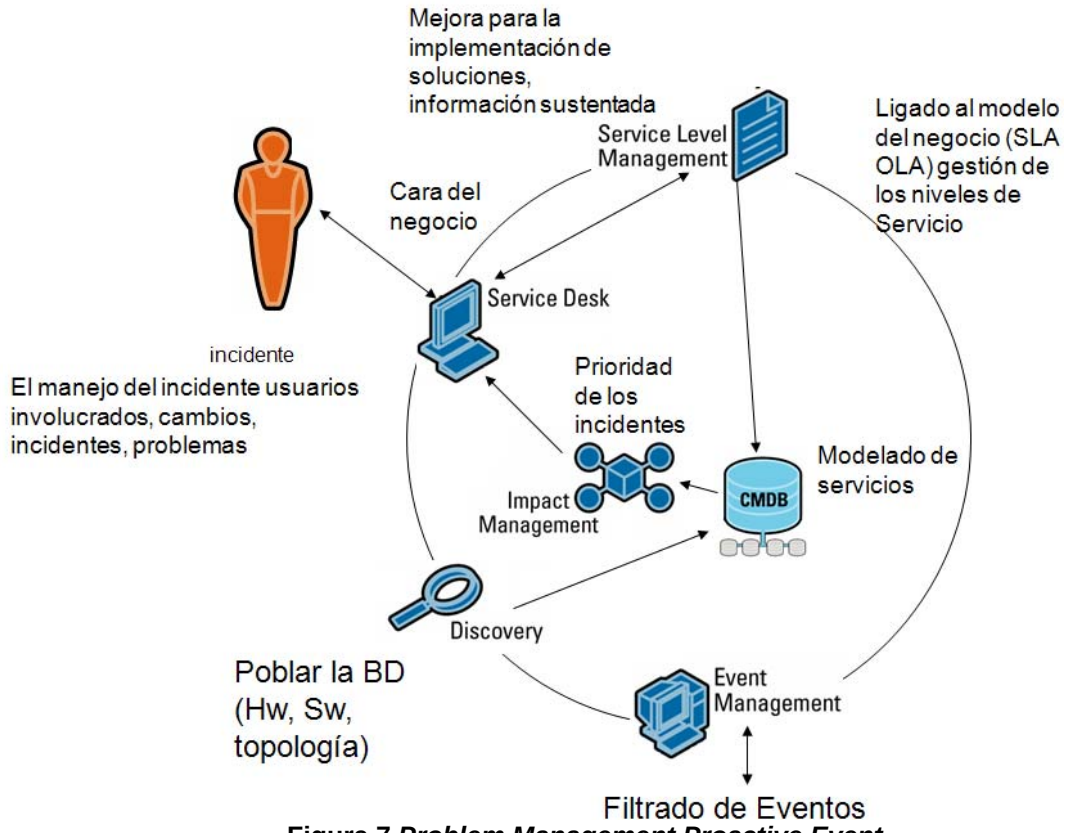

Figura 7 ***Problem Management Proactive Event***

En la tabla siguiente se explica como se relaciona la Base de Datos de Administración de Configuraciones (CMDB), con las disciplinas de la Administración de Servicios y el valor que le proporciona al negocio

Disciplinas de Administración de servicios	Valor del Negocio CMDB
Manejo de Incidentes (*Incident Management*)	Se extiende el valor del manejo de incidentes, dando acceso a la información técnica, mediante el *Service Desk*, sobre los CIs (*Configuration Items*) en relación con los registros de incidentes. Significa que el tiempo para restaurar el servicio es reducido , dando prioridad a las solicitudes entrantes, basados ya sea en el impacto al negocio o los acuerdos de nivel de servicio (SLA) y para proveer una amplia gama de información necesaria para la rápida restauración del servicio
Manejo de Problemas (*Problem Management*)	Se extiende el valor del Manejo de problemas, por la vinculación de los incidentes y problemas, y mediante el enlace de CIs en un flujo descendente y ascendente a través de estos. Significa que el tiempo de reparación es reducido mediante la optimización en el control del problema, en el control del error, en el control del error conocido, y en el análisis de la causa raíz.

Disciplinas de Administración de servicios	Valor del Negocio CMDB
Manejo de Configuraciones (*Configuration Management*)	Permite la coherencia, precisión, y el costo efectivo en la identificación, control , seguimiento del status, y verificación de todos los CIs en la CMDB
Manejo de cambios (*Change Management*)	En conjunto con el modelo de Impacto al servico (service Impact), se extiende el valor del manejo de cambios, por la relación de todos los cambios solicitados de un CI especifico afectado por estos, así como todas las demás relacionadas con los CIs. La Solicitud de Cambio puede ser categorizada por el impacto, la cual se encarga del ruteo, comunicaciones, y aprobaciones.
Manejo de Software (*Release Management*)	Permite un efectivo y automatizado manejo de software. La CMDB proporciona información precisa sobre hardware, software y configuraciones específicas que habilitan la automatización del manejo del software, así como los procedimientos, para retroceder o echar para atrás, las configuraciones en el caso de no ser estables, además de la programación del proyecto.
Centro de Servico a Clientes (Service Desk)	Se extiende el valor del Centro de servicio a Clientes por la provisión de detalles de los CI relacionados con cada servicio solicitado. Los niveles de Servicio son mejorados por la reducción de errores, disminuyendo la recolección de datos de forma manual, además de reducir el riesgo de fallo debido a cambios que impactan las funciones vitales del negocio.
Gestión de niveles de servicio (*Service Level Management*)	Permite de un extremo a otro la gestión de los niveles de servicio, que es por otro lado limitado, con una CMDB. Detallando información sobre los CIs, sus relaciones entre si, y sus relaciones vinculadas atrás con los servicios de TI, permite los acuerdos de nivel de servicio SLA (con el negocio), los acuerdos de nivel operacional OLA (con los grupos internos de TI o proveedores externos de servicios) y contratos externos [*underpinning contracts*] (con proveedores de servicio externos).
Gestión de la Capacidad (*Capacity Management*)	Permite la comprensión de la gestión de la capacidad del negocio, y la gestión de la capacidad de los recursos. Información sobre los CIs, sus relaciones entre sí, y sus relaciones para las funciones del negocio es un prerrequisito para la automatización de la gestión de la capacidad y el calculo en tiempo real de los marcos de trabajo.
Gestión de la Continuidad del Servicio de TI (*IT Service Continuity Management*)	Proporciona un repositorio central de la información que permite la gestión de la continuidad del servicio de TI. La CMDB almacena información sobre los activos de TI y las configuraciones que apoyan los procesos claves del negocio e identifica la prioridad y el nivel de acuerdo mínimo de la operación del negocio, seguida de la interrupción de un servicio importante
Gestión de la Disponibilidad (*Availability Management*)	Permite un repositorio central de información, que vincula la disponibilidad, rentabilidad y mantenimiento de los componentes de TI base. Esto entonces vincula los componentes de TI, que están atrás, de los acuerdos de nivel de servicio SLA, acuerdos de nivel operacional OLA, y los contratos externos [*underpinning contracts*]

Disciplinas de Administración de servicios	Valor del Negocio CMDB
Gestión de las Finanzas (*Financial Management*)	Proporciona información que es crítica, para una efectiva gestión de las finanzas de TI. En conjunto con la definición de los servicios en el catálogo de servicios, la información de la CMDB permite calcular los costos basados en los servicios como marcos de referencia, los cuales son componentes claves de la gestión de las finanzas, esto por su vinculación dentro de la administración de datos de los activos que mantiene la relación financiera, y dentro del sistema de planeación de los recursos de la empresa (ERP) manteniendo el registro de activo fijo.

Tabla 6 Las Disciplinas de la Administración de Servicios y su relación con la CMDB

Este capítulo desarrolló la metodología de ITIL, además de cómo se relaciona y apoya en la toma de decisiones partiendo del análisis de los riesgos identificados, con un enfoque general. El BSM, que conforma parte de las disciplinas de Administración de Servicios, es el soporte en la administración de riesgos.

El siguiente capítulo tomará lo expuesto anteriormente, en la administración de riesgos, partiendo de los aspectos a considerar en la implantación de controles, el efecto de la aplicación de estos controles a un nivel productivo, sobre todos los relativos a la seguridad de la información. Y cuáles son los factores de éxito en la puesta en marcha, debido a que la desatendida administración, por ejemplo, en el control de cambios podría representar un dolor de cabeza y reflejar una disminución en las expectativas de éxito.

Referencias Capítulo 3

[1]*Guyton Pamela.* “**Bussines Service Management. Introduction to Business Service Management == Business Service Management (BSM) is a goal for businesses, and a promise from potential providers. A good BSM”.** Wikipedia the free Encyclopedia.The 6 April 2007. Disponible en: http://en.wikipedia.org/wiki/Business_Service_Management Leído el 27 Septiembre 2007

[2]*Sogeti Belgium* **“Part 1 Capacity Management- a refresh Open Event itSMF Gelgium”** October 2007, 25th.Disponible en: www.itsmf.be/file/21/Capacity_Management/ Leído el 10 Noviembre 2007.
[3]*Konzepte y conceptos Costumer Care Associetes.”***Problem Management (EXIN: Gestión de Problemas)”** p5. Seminario Producido en México por Konzepte y Conceptos.

[4]*Konzepte y conceptos.Costumer Care Associetes* **”Problem Management (EXIN: Gestión de Problemas)”** p5. Seminario Producido en México por Konzepte y Conceptos.

[5] *Leopoldi Rick ITSM IT* **“Service Management”** Disponible en: http://www.itsm.info/ITSM.htm Leído el 5 Octubre 2007. RL Information Consulting LLC

[6] *Chunhua Liao et al.* **“Performance analysis”** From Wikipedia the free encyplopedia Disponible en: http://en.wikipedia.org/wiki/Performance_analysis Leído el 14 Noviembre 2007.

[7] *Chunhua Liao et al.* **“Performance tuning”** From Wikipedia the free encyplopedia Disponible en: http://en.wikipedia.org/wiki/Performance_tuning Leído el 14 Noviembre 2007.

[8]*Wikipedia the free encyplopedia*. **“Capacity planning”**. Disponible en: http://en.wikipedia.org/wiki/Capacity_planning Leído el 14 Noviembre 2007.

[9] *Bourne, M.,Franco, M. and Wilkes, J.* (2003). **“Corporate performance management. Measuring Business Excellence”** 2003; 7, 3; p. 15.

[10] *Genesis Comunication* 2007. **“Resourse Management”** Disponible en: http://www.genesiscom.ch/en/1/solutions/nms/Resour_1736.asp Leído el 10 noviembre 2007.

[11] *Office of Government Commerce (OGC).*2002. **“Planning to Implement Service Management. London : The Stationery Office”** .

[12]*Office of Government Commerce* **“Business Case”**. Disponible en: http://www.ogc.gov.uk/documentation_and_templates_business_case.asp Leído el 4 Diciembre 2007.
[13]*R Yoni et Al.* **“Marketing intelligence”** Disponible en: Wikipedia The Free encyclopedia http://en.wikipedia.org/wiki/Marketing_intelligence Leído el 4 Diciembre 2007.
C Rob Et Al. Market Intelligence Disponible en: Wikipedia The free Enciclopedia http://en.wikipedia.org/wiki/Market_Intelligence Leído el 4 Diciembre 2007.

[14]*Goodman David et al.* **“Total Quality Management”.** from Wikipedia the free encyclopedia Disponible en: http://en.wikipedia.org/wiki/Total_Quality_Management Leído el 12 Diciembre 2007.
[15] Weill, P. & Ross, J. W., 2004, *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*, Harvard Business School Press, Boston
[16]*Konzepte y Conceptos.* **“Costumer Care AssocietesProblem Management (EXIN: Gestión de Problemas)”** p5. Seminario Producido en México por Konzepte y Conceptos.

Capítulo
4
Administración de Riesgos de Seguridad Basados en ITIL/BSM

Resumen

El análisis de riesgos permite determinar cómo es, cuánto vale y cómo de protegidos se encuentran los activos. En coordinación con los objetivos, estrategia y políticas de la Organización, las actividades de Administración de riesgos permiten elaborar un plan de seguridad que, implantado y operado, satisfaga los objetivos propuestos con un nivel de riesgo aceptable.

La mayoría de las organizaciones han optado por SOA en los procesos de negocio, por lo que a continuación se explica en que consiste, y la relación que apoya la misión y objetivos de la organización.

---

4 Administración de Riesgos de Seguridad Basados en ITIL/BSM

4.1 Arquitectura Orientada a Servicios SOA

La arquitectura orientada a servicios, como su nombre lo dice es un estilo arquitectónico que guía todos los aspectos de creación y utilización de los procesos de negocio, empaquetados como servicios, a través de su ciclo de vida, así como la definición y aprovisionamiento de la infraestructura de TI que permite a las diferentes aplicaciones el intercambio de de datos, (como se muestra en la figura del BSM donde la infraestructura tecnológica se une a los servicios no como un lastre si no como una ventaja competitiva y con una estrategia de control optima que permite la resolución activa y proactiva en los problemas de prestación de los servicios) además de la participación de los sistemas operativos de bajo acoplamiento y los lenguajes de programación que soportan estas aplicaciones en el proceso de negocio. Estos servicios se comunican con otros pasando datos de un servicio a otro, o por la actividad coordinada entre dos o más servicios. Los conceptos de Arquitectura Orientada a Servicios permiten tener una visión del negocio completa.

Cumplir los objetivos de las organizaciones, tomando en cuenta lo estipulado en los Acuerdos de Niveles de Servicio y los Niveles Operacionales y muy en particular lo referente a la confiabilidad de la infraestructura utilizada, es la finalidad de las organizaciones.

Los afectados, que frecuentemente no son técnicos, se preguntan si estos sistemas merecen su confianza, confianza que se ve mermada por cada fallo y, sobre todo, cuando la inversión en defensa de los medios de trabajo no se traduce en la ausencia de éstos. Lo ideal es que los sistemas no fallen. Pero lo cierto que se acepta convivir con sistemas que fallan. El asunto no es tanto la ausencia de incidentes como la confianza en que están bajo control: se sabe qué puede pasar y se sabe qué hacer

cuando pasa. El temor a lo desconocido es el principal origen de la desconfianza y, en consecuencia, aquí se busca conocer para confiar: conocer los riesgos para poder afrontarlos y controlarlos. Los clientes y usuarios tiene como punto único de contacto el Centro de Servicio a Clientes (*Service Desk*) y desacredita de sobremanera el hecho de que los incidentes sean descubiertos por los clientes en primera instancia en vez de proveer de información del estado del incidente y el tiempo estimado para su resolución o el restablecimiento del servicio, el punto único de contacto es enterado de los fallos en los sistemas, traducido en la interrupción de la continuidad de un servicio, ya que éste se propago.

4.2 Concientización, Cultura en Seguridad

La idiosincrasia de la gente sometida a controles de seguridad es muy importante debido a esto su implantación se tiene que considerar como un proceso paulatino y continuo.

La implantación de los controles de seguridad requiere una organización administrada y la participación informada de todo el personal que trabaja con el sistema de información, sin una colaboración activa de las personas involucradas en el sistema de información se ve afectada la posibilidad de implementación de controles especialmente si la actitud es negativa, contraria, o se tiene la finalidad, por parte del personal o usuarios de “luchar contra las medidas de seguridad”. Es por ello que se requiere la creación de una “cultura de seguridad” que, surge de la alta dirección, permitiendo tomar conciencia a todos los involucrados de su necesidad y pertinencia.

También es necesario tomar en cuenta dos aspectos que contribuirán con la formación de esta cultura de de la seguridad.
Primeramente las políticas de seguridad corporativa las cuales deben de ser entendibles (escrita para los que no son expertos en la materia), que se difunda y que se mantenga al día y por último una **formación continua** a todos los niveles, tomando en cuenta las precauciones y reservas rutinarias, además de las actividades especializadas, según la responsabilidad adscrita a cada puesto de trabajo.
Para lograr que los controles introducidos tengan éxito en su implantación y convivan con la organización es necesario que estos controles sean en medida de lo posible poco intrusivos (algunos controles de acceso, particularmente biométricos), es decir, que no dificulte innecesariamente la actividad diaria ni ponga en peligro el alcanzar los objetivos de productividad propuestos.

Por ejemplo un dispositivo biométrico en la entrada de la organización, la cual cuenta con un gran número de empleados y a pesar de brindar un buen control de acceso las filas para poder someterse a este control pueden ser muy largas causando descontento, una solución sería el poner varios puntos donde los empleados puedan hacer la validación separando así la carga de los dispositivos biométricos en varios puntos, pero es hay que considerar si la inversión económica en esta tecnología

puede realizarse tomando en cuenta que los dispositivos biométricos pueden tener precios muy elevados.

Figura 1 Aglomeración de personas a someterse a un control de acceso[1]

Para darle solución a la implementación de un control de acceso, partiendo del ejemplo anterior, puede realizarse en los diferentes puntos de la organización que se requieran no necesariamente a la entrada si no que en lugares más pequeños, con menor afluencia de empleados, donde haya activos importantes que tiene que resguardarse, además que ameriten la inversión en su protección.

Figura 2 Biométrico empleado para el control de acceso. [2]

Las personas involucradas deben de ser concientes de su papel en la organización y con la finalidad de prevenir problemas y reaccionar cuando se produzcan, pero además de esto, una cultura documentativa de estos incidentes con el objetivo de poder prevenir incidentes y/o recuperarse más rápidamente si se presenta una

situación similar o igual. Esto tiene mayor relevancia cuando la resolución de un determinado problema necesita escalar en cuanto a la toma de decisiones, por eso es importante crear una cultura de responsabilidad, donde los potenciales problemas, detectados por los que están cercanos a los activos afectados, puedan ser canalizados hacia los puntos de decisión, además de tomar en cuenta que "*Uno de los elementos clave para una organización y también visto como herramienta competitiva es la mejora del flujo y proceso de la información y que esta información pueda ser accesible de manera rápida e interrelacionada*". [3]

La concientización es un factor fundamental en el éxito de la implantación de controles y este se enfoca, particularmente en el factor humano, personal, pero se deben considerar otros factores de riesgo como se describe a continuación.

4.3 El Manejo de configuraciones y la Administración de Servicios

El manejo de configuraciones es una parte integral de todos los procesos de la Administración de Servicios (*Service Management*). Con este manejo de configuraciones se precisa información exhaustiva sobre todos los componentes en la infraestructura y los previstos en el proceso de manejo de cambios (*Change Management*) en particular si estos cambios proveen de mayor eficacia o eficiencia en el proceso de negocio; podrían integrarse estos dos procesos, manejo de cambios (*Change Management*) y el manejo de configuraciones (*Configuration Mangement*). Como mínimo es recomendado el registro e implementación de cambios que debe estar bajo el control extenso del proceso de manejo de configuraciones (*Configuration Management*) debido a que la **evaluación del impacto** de los cambios se hace con la ayuda del proceso de manejo de configuraciones (*Configuration Management*).

Todos los cambios requeridos deben por eso estar enterados en la CMDB y la actualización de los registros como el avance de los requerimientos de cambio a través de la implementación. El manejo de configuraciones identifica las relaciones entre un elemento (CI) que ha sido cambiado y cualquier otro componente de la infraestructura, lo que permite a los propietarios de esos componentes ser involucrados en le proceso de evaluación del impacto Siempre que se haga un cambio a la infraestructura, el manejo de configuraciones asociado a los registros deben ser actualizado en la CMDB (Siempre que sea posible, esto se logra mejor mediante el uso de herramientas integradas que actualizan automáticamente los registros cuando se introducen cambios.)

La CMDB debe ponerse a disposición de todo el grupo de Servicio de Asistencia (*Service Support*) a fin de que los incidentes y problemas puedan ser resueltos más fácilmente mediante la comprensión de la posible causa del fallo en los componentes (CIs). La CMDB se utiliza también para vincular los registros de incidentes y problemas con otros registros, como el fallo de un elemento de Configuración (CI) y el usuario. El *Release Management* (manejo de entregas, manejo de software) será

difícil y propenso a errores, sin la integración del proceso de manejo de configuraciones
El proceso de Entrega de Servicios (*Service Delivery*) también se basa en los datos de la CMDB. Por ejemplo:

- Gestión de Niveles de Servicio (SLM) necesita identificar los componentes que junto con la entrega de servicios (*Service Delivery*) para que los acuerdos externos se puedan establecer.(OLA)
- La Gestión financiera necesita saber los componentes utilizados por cada unidad de negocio especialmente si la carga (económicamente) se encuentra en un solo lugar.
- Gestión de la continuidad del Servicio de TI y La gestión de la Disponibilidad para identificar los componentes para realizar el **análisis de riesgos** y los fallos en estos componentes para el **análisis de impacto**.

El manejo de configuraciones con respecto a la infraestructura[1] de seguridad. Como lo relacionado con *firewalls*, *IDS (Intrusion Detection System)* u otros dispositivos con el propósito de proveer de características de seguridad a la información que maneja el sistema durante el proceso de negocio; así como las configuraciones extras para cada situación (no es la misma configuración de un *firewall* interno [*intranet*] al que se encuentra en la DMZ) y las realizadas en otros dispositivos (Bases de Datos, S.O, entre otros; como parte del *hardening*) y el impacto de módulos extras a determinados CIs (*ad-ons* módulos específicos para robustecer la seguridad) y el impacto en la productividad como parte del funcionamiento.

[1] La Infraestructura comprende: "Capacidades básicas": la capacidad y las competencias necesarias para ejecutar un modelo de negocio de la empresa. "La red de socios": El complemento de las alianzas comerciales que otros aspectos del modelo de negocio."Valor de configuración": La razón que hace que un negocio de mutuo beneficio para las empresas y los clientes.

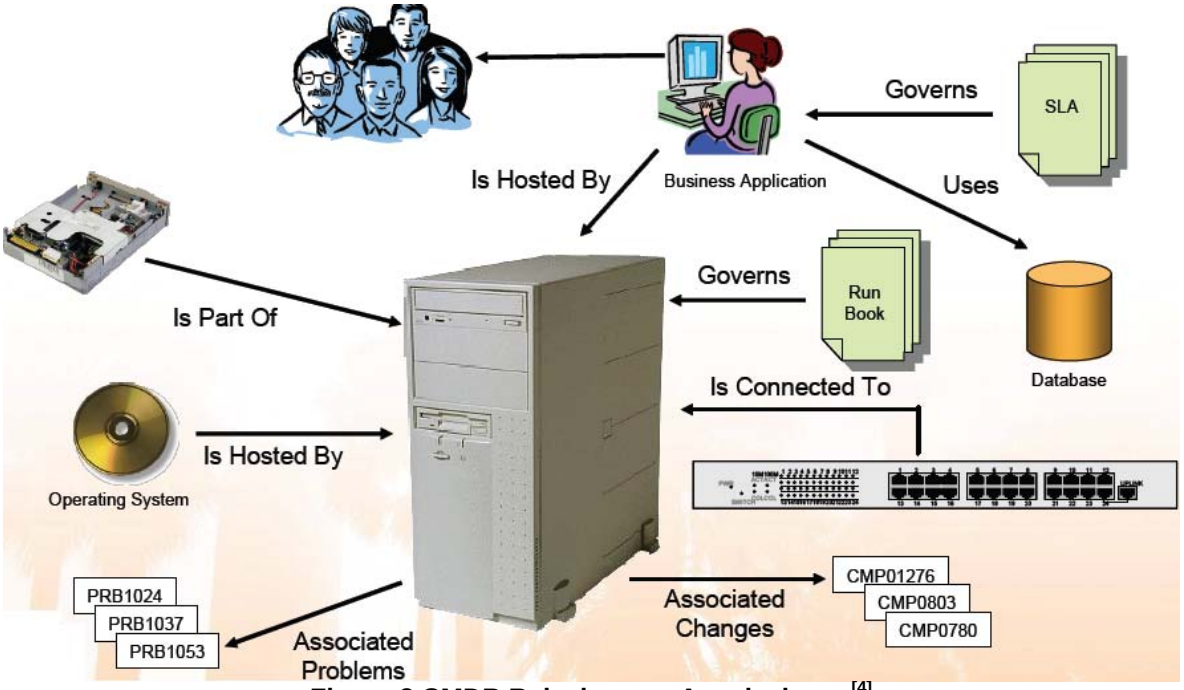

Figura 3 CMDB Relaciones y Asociaciones[4]

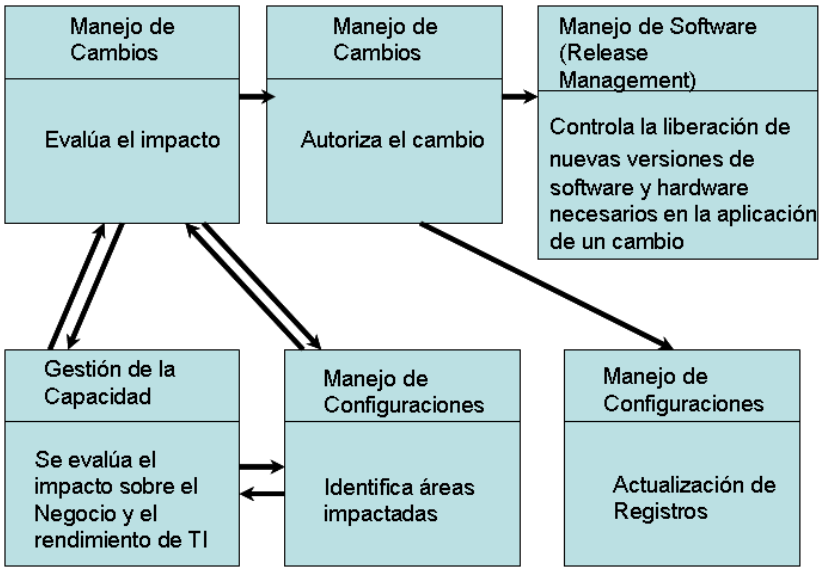

Figura 4 Relación entre el manejo de configuraciones y otros procesos de la Administración de Servicios (*Service Management*)

Cuando se produce una incidencia, el tiempo empieza a correr en contra del sistema, si; pero también en contra de los servicios que se dejan de prestar y el objetivo que ese sistema cumple para la misión de la organización. La supervivencia de una incidencia depende de la rapidez en la corrección de las actividades de reporte y

reacción. Cualquier error, imprecisión o ambigüedad en estos momentos críticos, se ve amplificado convirtiendo lo que podía ser un mero incidente en un desastre.

Las incidencias documentadas servirán para un proceso continuo de aprendizaje que se incorporarán al análisis y administración de los riesgos y es fundamental en lo sucesivo para crear un modelo que permita localizar las dependencias entre activos y el valor de cada uno de estos logrando que se refleje sobre dicho modelo la madurez de una organización, mediante el apego de dicho modelo con la realidad productiva y organizacional.

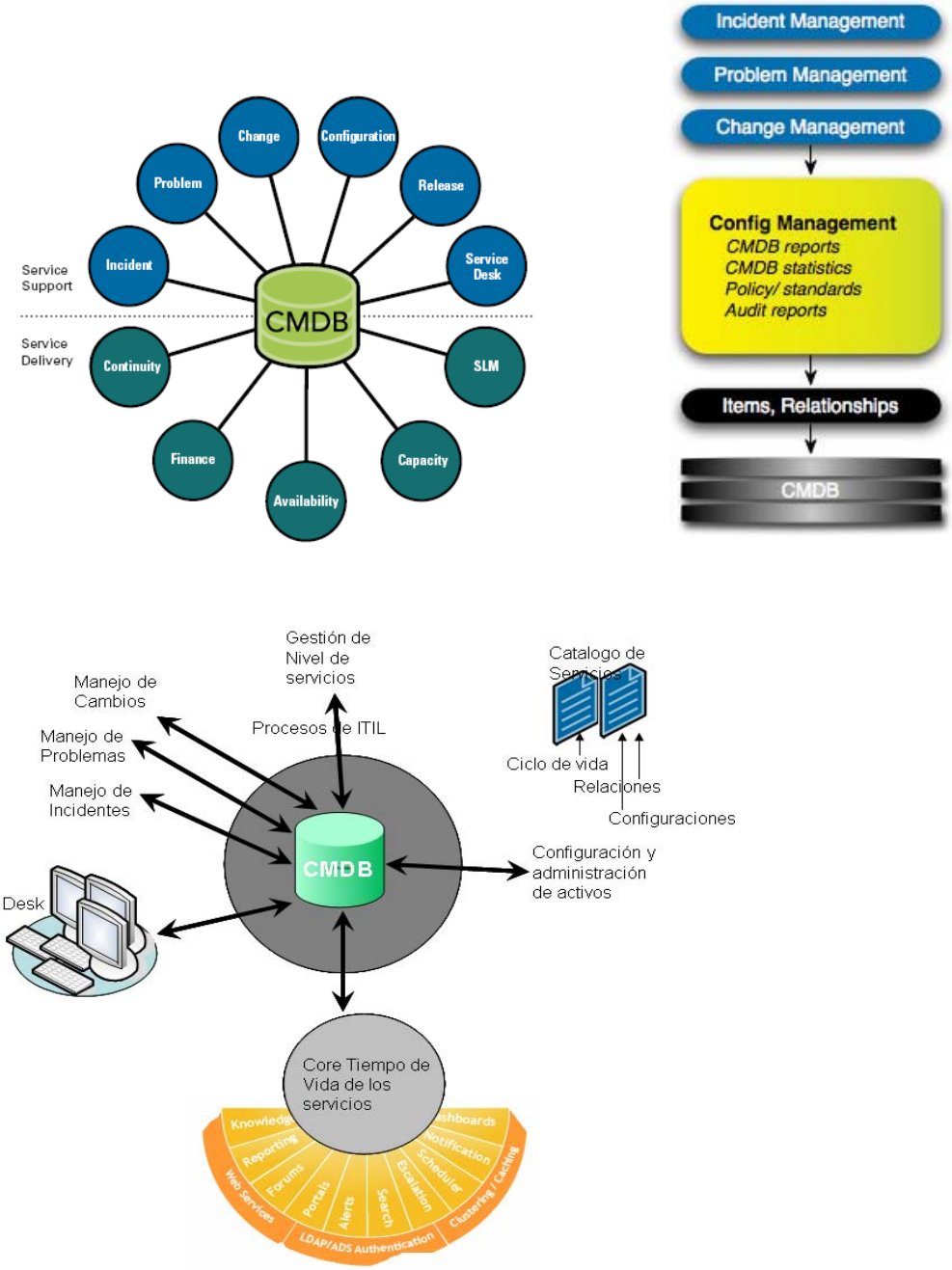

Figura 5 Relación de la Base de Datos de Manejo de Configuraciones (CMDB)

4.4 Gestión del Impacto

Las organizaciones de TI que desean lograr el pleno valor del negocio, mediante las iniciativas de la Administración de Servicios (*Service Management*), necesita tomar en cuenta la coherencia, actualización, precisión y la seguridad de la información. Por lo tanto una Base de Datos de Manejo de Configuraciones (CMDB) puede ayudar en la administración de la infraestructura más efectivamente. Una buena CMDB configurada puede ser un sencillo monitor de los elementos de configuración (CIs), su localización, su estado, y relaciones entre si; además de consolidar los datos. Esto puede proveer una fuente única de información precisa sobre los datos en el entorno de TI. Consecuentemente, los controles adecuados a implementar y/o mejorar que van desde medidas técnicas hasta una óptima organización y los respectivos acuerdos de niveles, tanto de servicios (hacia los clientes), como los operacionales (de forma interna en la organización), pueden retroalimentarse y lograr así madurez organizacional.

Las incidencias que se produzcan en el ambiente de TI (infraestructura) subyacente, debe ser captada por los controles técnicos (implica configuración de herramientas y también su relación con el manejo de configuraciones) implementados o previstos para la captación de estas incidencias, para después hacer la comparativa con el modelo de negocio. Es aquí donde se evalúa el impacto que la incidencia ejerce sobre el negocio, se identifican las causas, además de que se establecen prioridades en las que se dará respuesta en función de la relevancia para el negocio.

En conjunto, personal e infraestructura deben funcionar en base a un modelo de negocio que los vincule como a continuación se explica.

4.5 El Modelo del Negocio

Cada proceso puede desglosarse en una serie de tareas. Para cada tarea, habrá Entradas y salidas (que se muestra como objetos del mundo real [RWO] en el diagrama). RWO si estos tienen una forma física, por ejemplo, Como un pedazo de papel, o simplemente como la información electrónica, es irrelevante. Cada tarea será ejecutada en un rol. Estas pueden ser incluidas en un ser humano o realizado por software. Si el rol recae sobre un humano, entonces habrá un conjunto de competencias que la persona necesita, para llevar a cabo la función.

La ejecución de la función se rige por un conjunto de normas. Estas van desde la simple a la muy compleja.

A menudo, un proceso abarcará varios límites organizativos. Es importante, por tanto, que cada proceso tenga un propietario. Esta es otra función o rol.

El proceso propietario es el responsable de la definición del proceso en sí, que debería ser tratado como un elemento de configuración (CI), sujeta a todos los rigores de costumbre del Control de los cambios. El proceso propietario es

responsable de garantizar que todos los que están involucrados en la ejecución del proceso estén informados de cualquier cambio que se produce.

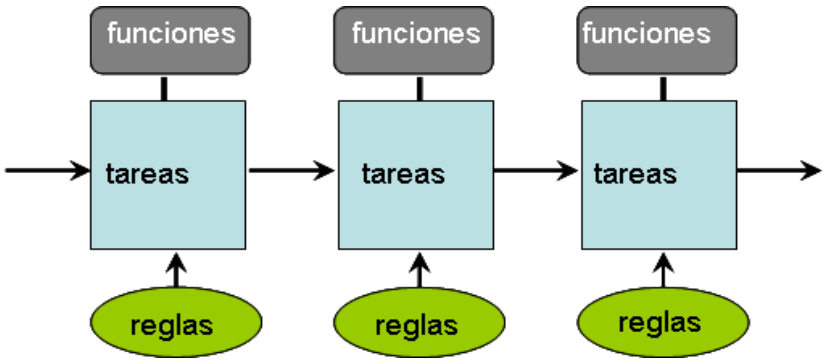

Figura 6 Componentes Físicos de la definición de un proceso

La implantación de medidas de control para mejora en los servicios es un proceso continuo, por lo que el Análisis y la Administración de los Riesgos, se integra como un proceso continúo para alcanzar los objetivos que sustentan la misión de la organización y los servicios que esta provee a sus cliente y usuarios.

4.6 Gestión de Niveles de Servicio como Proceso Continuo del Análisis y la Administración de Riesgos (Priorizar Acciones)

La misión de SLM, para la Gestión de Niveles de Servicio, es el de mantener y mejorar gradualmente la calidad de servicios de TI, a través de un ciclo constante para llegar a un acuerdo, sobre la supervisión y la presentación de informes en cuanto a los logros y los servicios de TI, induciendo acciones para erradicar el mal servicio; en línea con las empresas o la justificación de gastos. A través de estos métodos, debe desarrollarse una mejor relación entre las TI y sus clientes.

El concepto básico de la gestión de nivel de servicio, es el nombre dado a los procesos de planificación, coordinación, redacción, de acuerdos, concernientes a la vigilancia y presentación de informes sobre los acuerdos de nivel de servicio (SLA), y las negociaciones en curso para la revisión del servicio y los logros para garantizar que en función de costos es necesario y justificable mantener la calidad del servicio o donde es necesario mejorarlos gradualmente.

Cabe recordar que el SLA es un acuerdo escrito entre el proveedor de servicios de TI y el cliente o clientes de TI, definiendo los objetivos claves de servicio y las responsabilidades de ambas partes, debe hacerse énfasis en los acuerdos y los SLAs, no deben de ser usados como un medio para poner a alguna de las partes entre la espada y la pared, es decir, debe ser un acuerdo de mutuo beneficio entre el

cliente y el proveedor, de lo contrario el SLA rápidamente caerá en descrédito y de una cultura de culpa, impidiendo toda verdadera mejora en la calidad de los servicios que tienen lugar.

La Administración de riesgos es la estructuración de las acciones de seguridad para satisfacer las necesidades detectadas por el análisis y debe considerar, por lo menos, lo siguiente:

- Identificación.- Identificación de los riesgos (listado de riesgos)
- Clasificación.- categoría por la taxonomía
- Fecha de Identificación. Fecha sobre la cual el riesgo es definid
- Descripción.- Clara Descripción en "condición"-"consecuencia"-bajo un determinado formato
- Probabilidad La probabilidad de ocurrencia cualitativa o cuantitativamente
- Impacto.- El impacto en términos de severidad
- Exposición (probabilidad x impacto).- Producto de la probabilidad y el impacto
- Primer Indicador de Riesgo.-Condición o evento que indique que el riesgo se convierte en un problema
- Enfoque para la mitigación.- Enfoque para evitar o reducir el impacto del riesgo
- Asignación.- Persona (s) responsable(s) por la resolución del riesgo
- Fecha Objetivo.-Fecha para la cual se debe alcanzar una solución
- Plan de Contingencia.- Plan detallado para manejar la situación cuando un riesgo se convierte en un problema (aquí riesgos poco probables pero que si ocurrieran se convierten en un desastre) y seguir proporcionando un predeterminado y convenido nivel de Servicios de TI.
- Estatus- Activo (en tramite), Resuelto, Expirado (caducado).
- Seguimiento.- Proceso de resolución del riesgo; Seguimiento de la información.

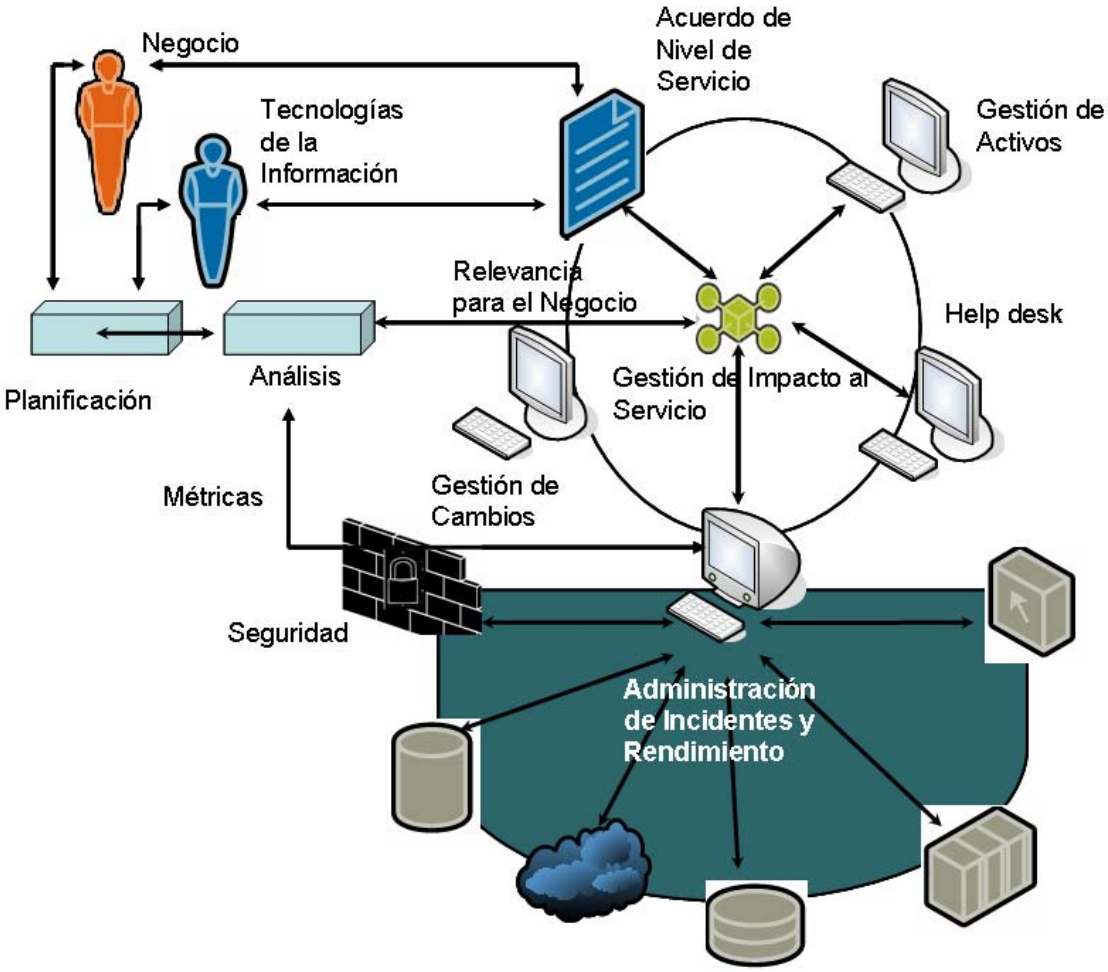

Figura 7 Gestión de Impacto al servicio

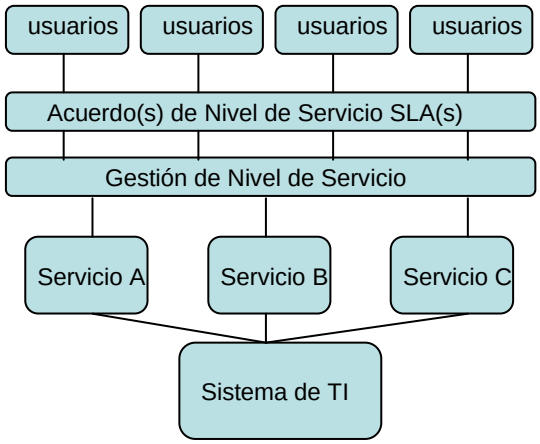

Figura 8 Relación entre la Gestión de Niveles de Servicio y los clientes

El conectar directamente la infraestructura y los servicios informáticos con los procesos de negocio – permitirá la gestión de servicios de negocio, como es:

- Planificar las relaciones entre sus elementos informáticos y los servicios de negocio.

- Administrar o gestionar el impacto que la tecnología de la información ejerce sobre el negocio en tiempo real (monitoreo) proporcionando al personal correspondiente la información necesaria para evaluar el impacto que las incidencias informáticas ejercen sobre el negocio y sobre los usuarios finales. Entonces se pueden establecer prioridades en las acciones informáticas y se pueden resolver las cuestiones del modo más eficaz posible.

- Establecer prioridades en las incidencias con el fin de asegurar la realización y disponibilidad de los servicios más críticos.

- Gestionar peticiones de servicio y cambios informáticos de acuerdo con su relevancia e impacto en el negocio.

- Analizar y optimizar la eficacia de los servicios informáticos en función de sus compromisos de nivel de servicio, de negocio, obteniendo soluciones. La Administración del Impacto en el Servicio ofrece información detallada y correlacionada para la gestión del negocio y los servicios de TI. Por tanto, el personal de TI cumple con rapidez y calidad, la exigencia de los clientes.

Para entender mejor la forma en que los procesos de Administración de Servicios (*Service Management*) se interrelacionan, examinemos el siguiente ejemplo del ciclo de vida de un incidente:

1. Un usuario llama al Centro de Servicio a Clientes (*Service Desk*) para reportar dificultades con el servicio en línea.

2. El proceso de Manejo de Incidentes acuerda que es un incidente

3. El proceso de Manejo de Problemas investiga que causa el incidente y en conjunto del proceso de Gestión de la capacidad para asistirse en la investigación.

4. La Gestión de Niveles de Servicio (SLM) alerta que un Acuerdo de Nivel de Servicio (SLA) no se ha cumplido.

5. El proceso de Manejo de Cambios plantea y coordina una solicitud de cambio (RFC), tomando en cuenta que este cambio será para dar solución a la incidencia.

6. El proceso de Gestión de las Finanzas de TI, con el costo en el caso de negocio, justifica la actualización del hardware.

7. El Proceso de Gestión de la Continuidad del Servicio de TI (*IT Service Continuity Management*) es involucrado en el proceso de Manejo de Cambios (*Change Management*) para asegurar que la recuperación es posible sobre el respaldo de la actual configuración.

8. El proceso de manejo de Software (*Release Management*) controla la implementación del cambio, es decir implantar el elemento de software y hardware a sustituir. El manejo de Software (*Release Management*) actualiza el Manejo de Configuración (*Configuration Management*) con los detalles de la nueva liberación y sus versiones.

9. EL proceso de Gestión de la Disponibilidad (*Availability Management*) es involucrado en la consideración de la actualización del hardware para asegurar que esto puede cumplir los requerimientos en los niveles de disponibilidad y fiabilidad.

10. El proceso de Manejo de Configuraciones (*Change Management*) asegura que la Base de Datos de Manejo de Configuraciones (CMDB) es actualizada durante todo el proceso.

4.7 Monitoreo de los Procesos de Negocio

El monitoreo de los procesos de negocio en la identificación de fallos en la infraestructura, es un aspecto fundamental, pero este monitoreo debe reflejar como es que se impacta un determinado servicio.

La monitorización en general del sistema permitirá determinar si los controles satisfacen con eficacia y eficiencia los objetivos propuestos.
Adoptar un planteamiento pro activo hacia la administración de los servicios de TI y la automatización de procesos.

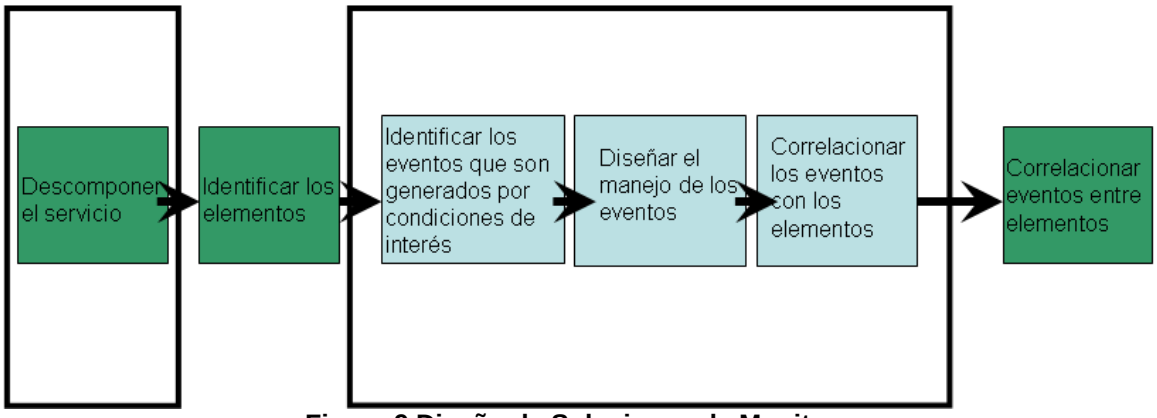

Figura 9 Diseño de Soluciones de Monitoreo

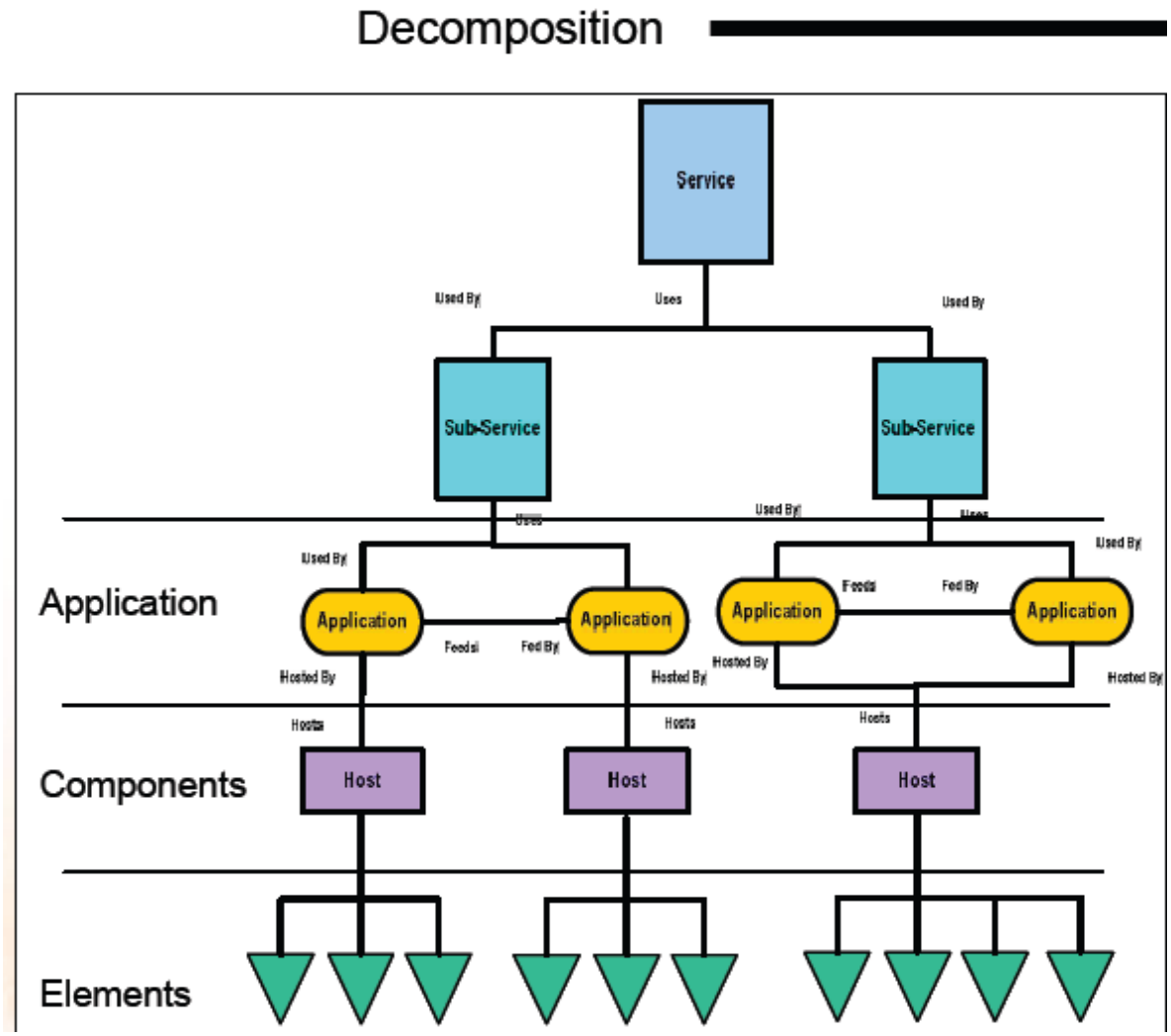

Figura 10 Descomposición del Servicio[5]

El cumplimiento de los SLA, para cada servicio proporcionado, es muy importante, como a continuación se explica.

4.8 Plan de Recuperación a Desastre (Disaster Recovery Planning)

También es necesario, tomar en cuenta la continuidad del servicio, con planes de recuperación de desastres, la Gestión de la continuidad del Negocio y los planes de contingencia considerados son algo esencial; sin embargo, la creación sólida de un plan de continuidad y contingencia es complejo, ya que involucra una serie de etapas y la participación en ciertas actividades.

Por ejemplo, inicialmente es necesario para entender los riesgos y el impacto potencial de un desastre, que, por supuesto, dista mucho de ser trivial (véase el capitulo 2) debido a que es necesario obtener la información que permita saber el impacto en el negocio/ organización en diferentes escenarios. Teniendo el impacto, es igual de importante considerar la magnitud del riesgo, como resultado de determinado impacto. Otra vez, esto es una actividad critica y debe de comprender cuales son los escenarios y la probabilidad de ocurrencia, además de cuáles magnitudes atraen más atención durante el proceso de planeación.

Luego están las fases de mantenimiento y pruebas, para asegurar que el plan sigue siendo actual, se relaciona estrechamente con La Gestión de la Continuidad del Servicio de TI (*IT Service Continuity Management*), involucra los siguientes pasos básicos:

- Priorización de los negocios al ser recuperados mediante la realización de un Análisis de Impacto al negocio (BIA)
- Realizar una evaluación de riesgos para cada uno de los Servicios de TI para identificar los activos, las amenazas, vulnerabilidades y contramedidas para cada servicio.
- Evaluación de las opciones de recuperación
- Producir el Plan de Contingencia
- Examinación, seguimiento y revisión del plan en una base regular

La Gestión de la Continuidad del Servicio de TI (*IT Service Continuity Management*) se refiere a la capacidad de una organización de seguir proporcionando una predeterminado y convenido a nivel de Servicios de TI para apoyar el mínimo de los requerimientos del negocio tras una interrupción del negocio. Efectivamente La Gestión de la Continuidad del Servicio de TI (*IT Service Continuity Management*) requiere de un equilibrio de las medidas de reducción de riesgos, como la resistencia y las opciones de recuperación de los sistemas, incluido los respaldos (*back-up*). El manejo de Configuraciones (*Configuration Management*) tiene la obligación de facilitar los datos necesarios para la prevención y planificación. Los cambios de infraestructura y el negocio tienen que ser evaluados por su impacto potencial en los

planes de continuidad, y la tecnología de la información y los planes de trabajo deben estar sujetos a los procedimientos del manejo de cambios (*Change Management*). El Centro de Servicio a Clientes (*Service Desk*) tiene un importante papel que desempeñar si se invoca la continuidad del negocio. Por ejemplo, Centro de Servicio a Clientes (*Service Desk*) podría actuar como centro de coordinación para el Cambio solicitudes de los usuarios, la emisión de cambios de horarios en nombre del manejo de cambios (*Change Management*), y del mantenimiento de usuarios informando del progreso en los cambios. Manejo de cambios (*Change Management*), por lo tanto, debe asegurarse de que el escritorio del servicio (*Service Desk*) se mantiene constantemente al tanto de las actividades de Cambio.

El Centro de Servicio a Clientes (*Service Desk*) es la línea directa de fuego de cualquier impacto en los SLAs y, como tal, necesita un rápido flujo de información.

El Centro de Servicio a Clientes (*Service Desk*) puede delegársele la aplicación de cambios para eludir los incidentes dentro de su ámbito de autoridad. El alcance de tales cambios deben ser predefinidos y el manejo de cambios (*Change Management*) debe ser informado de todos los cambios.

Antes de la aprobación del manejo de cambios (*Change Management*), son fundamentales las especificaciones de los CIs a los que aplican los cambios.

En este capítulo se abordaron los factores de éxito en la implantación de controles, después de un Análisis de Riesgos, estos controles junto con la administración, la misión y los objetivos de la organización, permite la implementación de un plan de mejora continua, esto claro, como un proceso continúo de análisis y administración de riesgos resultado de los cambios realizados y que tiene la finalidad de mantener a una organización competitiva.

Para concluir este trabajo, el siguiente capítulo muestra los resultados de una aspecto particular y como puede disminuirse el riesgo con una administración efectiva, pero también, como una toma de decisiones basada en poca información puede alejar a la organización de sus objetivos.

Referencias Capítulo 4

[1] *Enyclopaedia Britannica*. **"Aglomeración de personas"**. Imagen obtenida y disponible en: http://cache.eb.com/eb/image?id=61610&rendTypeId=4 Leído el 20 Enero 2008.

[2] *Brigham Scully* **"Press Room Ingersoll Rand Security Technologies Schlage biometrics"**. Disponible en: http://www.brighamscully.com/photos/rsi/SFK-MongKok05.jpg Leído el 20 Enero 2008

[3] *L.I. Genny E. Góngora Cuevas, M.A.* **"Tecnología de la información como herramienta para aumentar la productividad de una empresa.¿qué es la Técnología de la información?"** Disponible en: http://www.tuobra.unam.mx/publicadas/040702105342-__191_Qu.html leído el 25 Agosto 2007.

[4] Geoff Senson Karl Bietsch. **"How To Enhance IT Monitoring to Enable Business Alignment Using ITIL"**. Image in Slide 14. ConsultingPortal Inc. 14 th February, 2007 Session 1523.

[5] *Geoff Senson Karl Bietsch.* **"How To Enhance IT Monitoring to Enable Business Alignment Using ITIL"**. Image in Slide 20. ConsultingPortal Inc. 14 th February, 2007 Session 1523.

Capítulo
5
Resultados y Conclusiones

Resumen

La información dispuesta a lo largo de este trabajo y referente al ITIL/BSM fue obtenida gracias a mi participación con un *partner* de la empresa BMC, lo cual permitió obtener el "*spider*" el cual muestra la aplicación de la metodología, en una forma gráfica, el *Business Service Management* BSM y que tiene un sustento tecnológico donde varias empresas se han dado a la tarea el desarrollar (aunque en la información obtenida, en el cuadrante mágico, ostenta a BMC como uno de los lideres en el mercado con la aplicación de diferentes herramientas en cada una de las partes del BSM) las herramientas, que son susceptibles a la convivencia con otras tecnologías de otras empresas, que tienen un sustento en la misma metodología consideran la unificación a pesar de no ser del mismo fabricante (como aspecto sumamente importante) ya que no se trata de ninguna forma incitar al lector para inclinarse a un proveedor, si no únicamente hacer hincapié en la metodología de *Business Service Management*, que parte de los Procesos de ITIL, particularmente ITSM, para la administración de riesgos y en conjunción con una metodología de Análisis de Riesgos, (ampliamente explicada en el capitulo 2 del presente trabajo) se pueda tener una visión enfocada a los objetivos del negocio y la misión, que es la base de estos objetivos, para la aplicación de controles dentro de una organización y lo relacionado con el impacto de su implantación, o no implantación, aceptación entre otros factores que repercuten directamente en la productividad y confiabilidad de la organización al exterior e interior de la misma.

---

5 Resultados y Conclusiones

La figura 1, *Forrester Wave™: Business Service Management*, Q1 2007*,* muestra un cuadrante con las empresas que utilizan la metodología de BSM con un sustento tecnológico, herramientas en *software*, propietarias de cada proveedor.

Es común que las organizaciones antes de adquirir infraestructura de TI se orienten con estos cuadrantes donde se ostenta la presencia en el mercado y otros factores como el soporte del proveedor, como información complementaria a dicho cuadrante, con la finalidad de que una determinada organización elija un proveedor que satisfaga sus necesidades de infraestructura, las cuales por supuesto, pretenden una mejora en procesos que se refleje en productividad, por ejemplo, o algún otro objetivo a alcanzar por la organización. Estos cuadrantes son desarrollados mediante un análisis y sometimiento a diferentes pruebas sobre diferentes productos, *Gartner* y *Forrester Wave* son un ejemplo de estas empresas, que analizan y ofrecen servicios de consultoría.

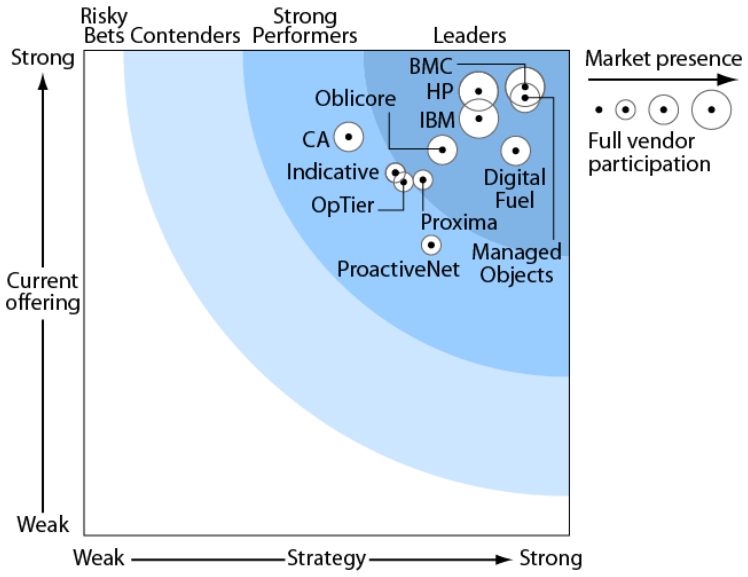

Figura 1 Forrester Wave™: Business Service Management, Q1 2007

La infraestructura de alto nivel basada en *best practices* y patrones para crear soluciones basadas en servicios, de alta cohesión y bajo acoplamiento se le conoce como SOA.

El ciclo de Vida de los Servicios, se refiere a una estrategia de servicio donde- entre otros- el mercado y el valor del servicio en éste es determinado. El portafolio de servicios y la propiedad debe ser administrado, además de que debe haber un modelo financiero para entregar y mantener el servicio.

Luego está el diseño del servicio, donde las soluciones son desarrolladas en términos de la arquitectura, tecnología, personas y procesos. Los procesos son desarrollados con respecto a la administración del catalogo de servicios, la continuidad, la seguridad, los niveles de servicio y mas.

El servicio incluye los procesos de transición, como la gestión del cambio, gestión de la configuración, versiones, esto en la planificación de las pruebas.

Por último la explotación de los servicios tiene que ser regido enfocándose en mantener los servicios en ejecución. Esto incluye, por ejemplo, Manejo de incidentes (*incident management*), manejo de problemas y administración identidades (accesos).

En la siguiente figura, ITIL-SOA, se muestra la relación que existe entre cada uno de los servicios del negocio los cuales, se relacionan entre si para solventar los objetivos de la organización, que son el sustento de la misión de la misma. Cada uno de los servicios de negocio pueden estar encadenados, lo que en un ambiente caótico, donde la administración está ausente, encontrar puntos de falla será un trabajo prácticamente artesanal.

La posibilidad de monitorear los procesos de negocio y los servicios permite, encontrar los puntos de falla de una manera más eficiente obteniendo tiempos mucho más precisos de solución(conforme a lo establecido en los Acuerdos de Nivel Operacional y los Acuerdos de Nivel de Servicio respectivos), que si se enfrentase a una búsqueda entre un mar de bitácoras, para localizar los eventos que puedan ser significativos en el entendimiento de la problemática y en el planteamiento de soluciones concisas que no repercutan en los otros servicios productivos. Se hace hincapié en este hecho debido a que una organización no debe optar por la monitorización de sus servidores críticos, a nivel infraestructura sin comprender el encadenamiento de servicios y todos los elementos que sustentan a éste, lo cual no es lo suficientemente robusto para encontrar fallas en servicios que dependen entre si, ya sea completamente o no, debido principalmente a que se carece de una centralización y correlación de eventos en un enfoque organizacional, lo que lleva, por ejemplo a tener un conjunto de servidores de un sistema operativo en particular en vez de un monitoreo que interrelaciones las partes de infraestructura con el negocio que es claramente una forma más estructurada del entendimiento de una falla, su impacto organizacional y su posible solución, temporal o definitiva dependiendo la criticidad del servicio, el impacto con los que se encuentra encadenado y la prontitud que se requiera para presentar una solución[1].

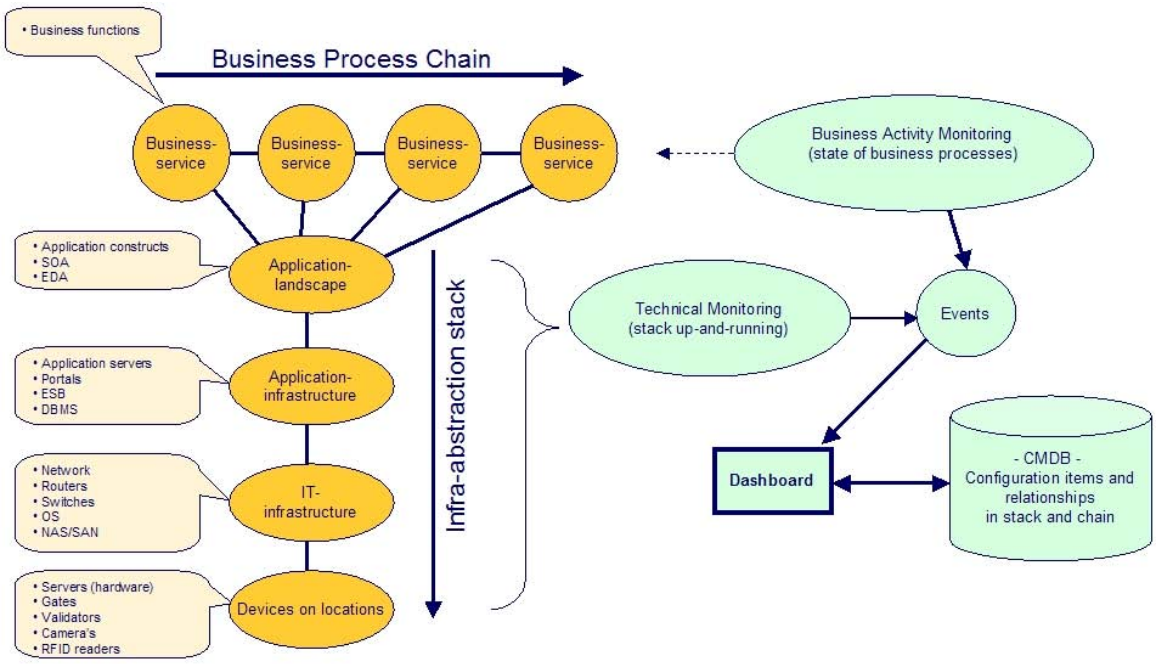

Figura 2 ITIL-SOA [1]

[1] Véase apartado de Manejo de Incidentes en el capítulo 3

Ahora bien en base a la información presentada a lo largo de este trabajo y con la finalidad de sustentar el análisis de las temáticas, se ejemplifica el siguiente caso de negocio, el cual después de realizado el análisis de riesgos , conforme a la metodología expuesta en el capítulo 2 , se obtiene los riesgos inherentes, relacionados con los aspectos de seguridad (servicios) que se pretenden alcanzar, no perdiendo de vista la concordancia con los objetivos del negocio que sustentan la misión de la organización.

Exposición de un caso ficticio:

La descripción que a continuación se realiza, expone la problemática a la cual se enfrenta una determinada organización y es sumamente importante retomar que independientemente que existan problemáticas afines entre una organización y otra no necesariamente la aplicación de acciones correctivas se llevarán acabo siguiendo una sucesión de pasos, debido a que existe una gran disparidad entre las organizaciones, así pertenezcan al mismo rubro o en esencia contemplen los mismos objetivos, estos factores son determinantes en la implementación de soluciones que mitiguen el riesgo:

El continuo mejoramiento es claro en la afinación de configuraciones como parte del aprendizaje continuo. Por ejemplo, un servicio de impresión que encola múltiples peticiones en diferentes servidores, que primeramente tienen que hacer una consulta o alguna transacción a una base de datos centralizada a través de la red corporativa y que sustenta información de clientes de diferentes regiones geográficas a nivel nacional y dentro del continente americano, particularmente Centroamérica y Sudamérica. Como parte de la posibilidad de dejar este servicio a una sola entidad encargada de las impresiones y que permita encolar una gran cantidad de peticiones de impresión, se cuestionan las capacidades del sistema y el riesgo que existe si el sistema falla, por lo que se divide la carga en varios sistemas afines; el monitoreo del funcionamiento (*performance*) de los sistemas y la identificación de su saturación en una determinada situación pueden auxiliar en la toma de decisiones, lo que hace que se cuestione si alguno de los sistemas deja de funcionar ¿puede distribuirse la carga de este a los otros sistemas afines sin saturarlos y que corran el riesgo de dejarlos indisponibles?. La distribución de la carga a otros sistemas afines ¿se realiza de una forma automática? (revisión de los OLAs y SLA, además del impacto en productividad y otros aspectos relacionados) o ¿en qué casos es conveniente realizarlo de forma manual?, dando el visto bueno a la realización de la(s) acción(es) de recuperación.

Las acciones de recuperación pueden ir desde reiniciar el servicio hasta un caso extremo (en sitio) reiniciar el sistema (tomando en cuenta todo lo que esto implica si se presenta un caso así). El reiniciar el servicio, también implica localizar los procesos relativos a este y darlos de baja, antes de reiniciar el servicio evitaría el riesgo de dejar colgados procesos que impidan reiniciar el servicio, en una situación así es conveniente tener monitoreados estos procesos (se refiere a la instancia en un programa de computo que se esta ejecutando) y que la acción de recuperación implique el primero darlos de baja antes de reiniciar el servicio.

Las mejoras que se pueden observar se relacionan con el filtrado de eventos (monitoreo de procesos) a acciones de recuperación en aras de mantener disponible el servicio.

Basándose en el ejemplo anterior, el servicio de impresión que interactúa con una base de datos transaccional y centralizada desde sus diferentes sucursales se descompondría en los sistemas y sus redundantes.

Identificar la problemática, la cual es el sustento del documento de caso de negocio, formato expuesto en el Anexo C del presente trabajo (o bien algún otro que permita hacer tangible a la alta gerencia de la organización, la problemática y la oportunidad de negocio que se manifiesta), con la finalidad de acometerla mediante la implementación de una solución tecnológica por parte de la organización, de forma independiente (con sus propios recursos materiales y humanos) o bien mediante el apoyo de un tercero (*outsourcing*), justificando la inversión económica, material y humana que de esta solución conlleve, evidenciando la ganancia efectiva sobre la prestación del servicio y el ROI (Retorno de Inversión) que para este caso se realiza.

Cabe destacar que la implementación de la solución para el caso de negocio, cualquiera que este sea, se apoya de una metodología de administración de proyectos, temática que queda fuera del alcance del presente.

El análisis de riesgos realizado en una fase previa y los resultados obtenidos de éste permitirán expresar claramente, en el documento de caso de negocio, la problemática y los riesgos inherentes de no implementar acciones correctivas. Para este caso es claro que para identificar los riesgos se necesita la interacción de los expertos en las aplicaciones e infraestructura, ya que son los únicos que podrán aportar una clara definición de la problemática al optar por un determinado control, los riesgos e incluso el impacto, mediante las acciones correctivas implementadas cuando se han presentado fallas, debido a la experiencia acumulada a lo largo de su interacción con las aplicaciones e infraestructura de la organización, se logrará, además, ampliar las posibilidades de empatía con los controles propuestos, esto debido a que la imposición de un control y la falta de concientización por parte de los usuarios son factores determinantes para el éxito del (los) control(es) en la mitigación de un riesgo.

Es ampliamente recomendable dividir en diversos proyectos las oportunidades de negocio obtenidas del análisis de riesgos y considerar primeramente la dependencia de los servicios del negocio que se modelaran para su entendimiento, con la finalidad de establecer las políticas generales que en algunos casos podrán materializarse en políticas automatizadas en herramientas o aplicaciones particulares.

La figura 3, Afinación en configuraciones, muestra la descomposición del servicio entre los elementos que interactúan con el servicio, además de los aspectos relacionados con el spider de Business Service Management que permitirán la administración de riesgos mediante la monitorización de la infraestructura por medio de agentes en cada uno de los elementos que componen el servicio descrito anteriormente, el tunning de cada uno de los agentes de infraestructura, que hace referencia a la configuración del agente que envía eventos al Event Management este

tunning o afinación de las configuraciones de los agentes muestra mayor entendimiento de los servicios y desprecia en gran medida información de *logs* y bitácoras que se convierte en un a difícil tarea de lectura para la toma de decisiones precisas, concisas y en tiempo determinado en gran medida por el impacto hacia el negocio, *Impact Management*, lo que permite dar prioridad a las incidencias detectadas de acuerdo a lo establecido en los Acuerdos de Nivel de Servicio y los Acuerdos de Nivel Operacional.

El establecimiento de este orden permite que los afectados por alguna incidencia en un ambiente productivo y que recurran directamente al *Help Desk o Service Desk*[2] puedan ser informados sobre el estado de la problemática.

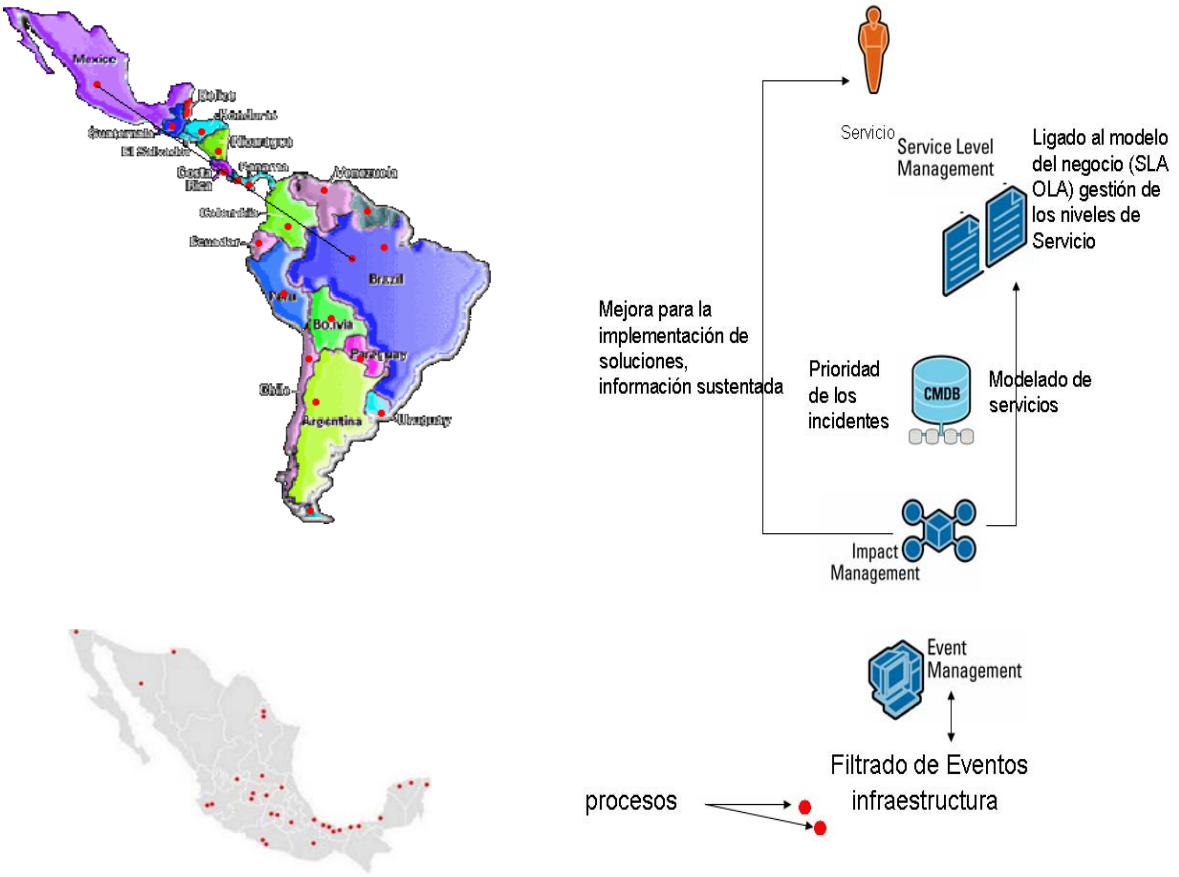

Figura 3 Afinación en configuraciones.

Las herramientas utilizadas para el monitoreo de las instancias de programas se afina mediante umbrales y alertas interfiriendo directamente con el filtrado de los eventos, estos cambios se ven reflejados en la CMDB

[2] Véase el apartado de Administración de Servicios en el capitulo 3.

Otro aspecto a considerar es la confidencialidad entre las sucursales hacia la central maestra.

Al utilizar la red corporativa (siguiendo el ejemplo anterior) y siendo muy costoso los enlaces dedicados hacia el Centro de Datos, puede optarse por VPNs por lo que la autenticación y otros factores, como la los dispositivos de filtrado de contenido, *firewalls,* deben armonizar y configurarse de una forma adecuada ya que una mala configuración (desición precipitada) puede causar una denegación del servicio. Para lograr esta armonización la realización de un análisis previo a la implantación de configuraciones y controles reducirá los fallos y protegerá los activos reflejándose en la continuidad del servicio.

Conclusiones

La toma de decisiones enfocada al negocio, objetivos que sustentan la misión de la organización es un factor fundamental en situaciones o estados críticos, por lo que prevenir estas situaciones de riesgo y ofrecer una base solida de información sustentará la toma de decisiones.

El objetivo de la Arquitectura Orientada a Servicios (SOA, por sus siglas en inglés) es habilitar el negocio para que alcance sus metas y objetivos a través de los procesos de negocio, soportado por la tecnología. Lo que cubre los siguientes aspectos en su implementación:

- Enfoque como una solución de negocio, no de tecnología.
- Demostración del Retorno de su Inversión (ROI, por sus siglas en inglés) en el tiempo.
- Aspectos críticos y visión global para la implementación, es decir, se debe tener noción de toda la empresa y de todas y cada una de las funciones.
- Esfuerzo multidisciplinario en la organización, esto es, involucrar a las áreas de negocio, operación y tecnología

Lo anterior se deriva por que los principales motivos que conducen a la transformación del negocio son los relacionados con la velocidad para ejecutar y entregar los procesos de negocio y que se dirigen a los esfuerzos de Tecnologías de Información (TI).

La reducción de tiempo y costos de los cambios adoptados o previstos mediante plataformas que permita los cambios eficientes a los procesos de negocio.

Reducir los costos de distribución y mantenimiento; soporte a las tecnologías existentes y compartirlas.

Además de la habilidad para reconocer y monitorear los beneficios y el Retorno de Inversión (ROI -*Return of Investment* por sus siglas en ingles) para incrementar el porcentaje para tecnologías en innovación del negocio.

SOA permite que toda la arquitectura, o componentes tecnológicos, ofrezcan agilidad para cambiar conforme se transforman los procesos de negocio, es decir, diseña un modelo de negocio basado en servicios, soportado por una arquitectura, de manera sencilla y ordenada, a través y alrededor de toda la empresa. Al Analizar el proceso ubica cuáles son los servicios y aplicaciones reutilizables, y de ahí se construye una capa que permite volver a usar los servicios las veces que sea necesario. Por ejemplo, el servicio de validación de crédito al cliente es una función utilizada por la mayoría de los departamentos en las organizaciones bancarias, por lo tanto, se crea una sola vez y es reutilizado por los diferentes procesos de negocio.

Para iniciar una implementación, se parte de identificar cuáles son las funciones críticas de negocio y de ahí se definen los servicios a implantar; esto se llama una “Estrategia y Diagnóstico de Agilidad”. Desde el punto de vista del negocio, se deben considerar los paquetes de servicios, funciones, procesos, clientes internos y externos, y soportar el negocio, de principio a fin. En la parte tecnológica, se debe observar la reducción de atrasos, **riesgos**, habilitar todo el proceso y evitar la duplicidad de aplicaciones. En tanto, la parte operativa debe verificar que todos los procesos operen eficientemente.

La realización de un plan de seguridad en cualquier organización no solo requiere del esfuerzo de los encargados de tecnologías de información, si no que además, de todas las áreas relacionas con la empresa. Cabe mencionar que la seguridad informática se hace presente desde los niveles más altos, como los dueños de la información, los cuales antepondrán, a está información, el valor de activo organizacional y las dependencias en la realización de las tareas cotidianas dentro de la organización que recaen directamente en la información y sus diferentes estados y procesos dentro de la estructura organizacional (responsables) así como la tecnología de la información para automatizar procesos y que se enlazan intrínsecamente con la productividad.

Por tal motivo es sumamente importante que cada una de las partes comprenda que la organización y su misión depende de las TI y de las funciones o roles de cada persona lleva cabalmente dentro de la organización, creando un proceso continuo.

La conciencia en cuanto a seguridad se refiere, es también considerada dentro del proceso de implementación de controles de todo tipo, esto es claro debido a que, en mayor parte, un control de seguridad se considera, en cierto modo, molesto por que con lleva el delimitar las responsabilidades, la escalación de toma de decisiones y una cohesión amplia en cuanto a lo que se refiere la realización y solución de problemas, el éxito de la implementación controles depende en gran medida de el personal dentro de la organización.

Es importante tomar en cuenta lo anterior, que la implantación de controles de seguridad es una tarea conjunta y que el objetivo a proteger es la misión de la Organización, teniendo en cuenta las diferentes dimensiones de la seguridad y las políticas como pilares sustentados de esta misión. Cuando las políticas no son seguidas se esta muy propenso a impactar la misión de la organización, por eso es

menester concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de atajarlos a tiempo.
Los conceptos de:

Disponibilidad o disposición de los servicios a ser usados cuando sea necesario y la comprensión de que la carencia de disponibilidad supone una interrupción del servicio, además de afectar este servicio de seguridad, la disponibilidad afecta directamente a la productividad de las organizaciones.

Integridad o mantenimiento de las características de completitud y corrección de los datos. Contra la integridad, la información puede aparecer manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de una Organización.

Confidencialidad o que la información llegue solamente a las personas autorizadas. Contra la confidencialidad o secreto pueden darse fugas y filtraciones de información, así como accesos no autorizados. La confidencialidad es una propiedad de difícil recuperación, pudiendo minar la confianza de los demás en la organización que no es diligente en el mantenimiento del secreto, y pudiendo suponer el incumplimiento de leyes y compromisos contractuales relativos a la custodia de los datos.

Autenticidad (de quién hace uso de los datos o servicios) o que no haya duda de quién se hace responsable de una información o prestación de un servicio, tanto a fin de confiar en él como de poder perseguir posteriormente los incumplimientos o errores. Contra la autenticidad se dan suplantaciones y engaños que buscan realizar un fraude. La autenticidad es la base para poder luchar contra el repudio y, como tal, fundamenta el comercio electrónico o la administración electrónica, permitiendo confiar sin papeles ni presencia física.
Ya que todas estas características pueden ser requeridas o no dependiendo de cada caso. Cuando se requieren, no es evidente que se disfruten sin más. Lo habitual que haya que poner medios y esfuerzo para conseguirlas.
El principio de la Evaluación de seguridad es determinar el estado o apego de las disposiciones y/o objetivos de la organización en dos áreas principales, técnica y no técnica.

No Técnica (Evaluación de Políticas)

Son 4 áreas claves en la evaluación de políticas:

- Control y Protección de la Información

Estas políticas rigen el control y clasificación de los activos de información. Esto también incluye revisar tanto las instrucciones así como las cuestiones relacionadas con el personal como el acuerdo de confidencialidad y deberes de segregación.

- Virus, Código Malicioso y Prevención contra virus

Estas políticas rigen la protección de los activos de información. Especificando el control periódico de información sobre la detección y las instrucciones para disuadir a las infecciones no intencionales de virus / troyanos.

- Prevención a Desastres

Estas políticas rigen la prevención de los desastres y la preservación de los activos de información. Sistema de Recuperación (*Failover*)[3], alta disponibilidad y capacidad de planificación son las medidas contra los desastres naturales o artificiales.

- Administración de la Continuidad del Negocio

Estas políticas rigen la continuidad del negocio en un evento de ruptura intencional o no intencional. La presencia de medidas de respaldo y las medidas suficientes para garantizar el ejercicio de planes de recuperación a desastres y su efectividad.

Los cuestionarios y entrevistas son un parte esencial de una evaluación de Políticas, esto es esencial para construir una lista de verificación (checklist) para satisfacer las áreas a un nivel aceptable para los objetivos de negocio. También es importante garantizar que todas las políticas son apoyadas por la administración y están al día con las actuales necesidades empresariales.

Evaluación Técnica

Debe cubrir las siguientes áreas con el principio específico de la política de seguridad corporativa en mente.

- Seguridad Física

¿Son las máquinas físicamente aseguradas únicamente teniendo acceso a ellas el personal autorizado?

Es acertado asegurar todos los cables y *switchs / hubs* para evitar el *sniffing*[4] el escaneo de puertos.

- Diseño de Redes y Seguridad

¿Existe el filtrado de trafico[5], el monitoreo y la separación de tráfico de la red con consideraciones basadas en una regla del menor privilegio? La presencia de un

[3] Tolerancia a fallos o también denominado *Failover*, Sistema de Recuperación

[4] Relativo al Análisis de Tráfico o Análisis de protocolos.

[5] Existen diversas situaciones en las que es conveniente o necesario filtrar determinado tráfico. Algunos ejemplos son los siguientes para filtrado de tráfico en un *router*:
• Un *host* está infectado por virus y para evitar que ataque o infecte a otras computadoras se quiere impedir que envíe tráfico. En este caso se deben filtrar los paquetes que tienen como origen esa dirección IP.
• Un *host* está distribuyendo ilegalmente música, películas o software (normalmente mediante programas *peer-to-peer*) y se quiere impedir que dicha distribución se lleve a cabo. En este caso se deben filtrar los paquetes que tienen esa dirección IP como origen o destino.
• Un servidor ofrece sus servicios por un puerto 'bien conocido' (por ejemplo el puerto 80 de TCP en el caso de un servidor web). Se supone que a dicho servidor solo deben llegar paquetes dirigidos al puerto 80. En estos casos suele ser buena práctica filtrar cualquier paquete dirigido a ese servidor que no vaya dirigido al puerto 80 de TCP, ya que en el mejor de los casos dicho tráfico es inútil y en el peor puede tratarse de intentos de ataque a ese servidor aprovechando vulnerabilidades accesibles por otros puertos o protocolos (ICMP, UDP, etc.).
• Un servidor tiene restringido su acceso a una serie de clientes externos autorizados que se identifican por una serie de direcciones IP. En este caso se debería filtrar cualquier petición de

sistema de registro y IDS (Sistema de Detección de Intrusos) ayudaría a identificar una buena cantidad de posibles intrusiones.

- En cuanto al personal y sus habilidades

¿El personal que manipula el sistema es capaz de detectar, responder y escalar cualquier Incidente? ¿Hay suficiente formación y capacitación en la tecnología de seguridad entre el personal?

La siguiente etapa de la evaluación técnica requiere la plena autorización de la administración y el propietario del sistema, ya que trata directamente sobre el sistema mediante pruebas de penetración.

"Lo que no se mide no se puede administrar.
Lo que no se administra no se puede asegurar."

conexión entrante que no provenga de una de las direcciones IP autorizadas.
• Se quiere impedir el establecimiento de conexiones TCP entrantes para todos los ordenadores de una red, excepto para un conjunto reducido de servidores que deben estar abiertos al exterior (y que se supone que estarán especialmente protegidos). En este caso se debe filtrar cualquier intento de conexión entrante que no vaya dirigido a los servidores.
• Se quiere impedir que los usuarios hagan uso de 'IP *spoofing*', es decir de direcciones IP falsas. Para ello se establece un filtro que comprueba que los paquetes recibidos en la interfaz LAN del *router* pertenecen a la red que está conectada a esa LAN. Análogamente se comprueba que por la interfaz WAN no lleguen paquetes con dirección de origen perteneciente a la LAN. Este filtro es aplicado de forma habitual por la mayoría de los ISPs.

Referencias Capítulo 5

[1] *Jack van Hook* **"SOA-ITIL"** Imagen Disponible en: http://bp0.blogger.com/_yL52t5KKXIo/R2KJ5aRLY1I/AAAAAAAAAFM/2K-gXD9EgvQ/s1600-h/ITIL-SOA.jpg Leído el 3 Febrero 2008.

ANEXO A Glosario de Términos

Acuerdo de Confidencialidad a menudo conocido también como Acuerdo de No Divulgación, *Confidential Disclosure Agreement*, CDA, Non Disclosure *Agreement*, NDA, Secrecy *Agreement*. Consta de un acuerdo legal entre al menos dos partes que delimitan los materiales confidenciales o el conocimiento de las partes del deseo de compartir con uno u otros para ciertos propósitos pero que deseen restringir el uso generalizado de dichos materiales confidenciales. En otras palabras, es un contrato mediante el cual las partes se comprometen a no revelar información cubierta dentro del acuerdo. Un acuerdo de confidencialidad crea una relación entre las partes para proteger cualquier tipo de intercambio secreto. Como tal, un Acuerdo de confidencialidad puede proteger información NO publica de la empresa.

Acuerdo de Nivel operacional (OLA) es un acuerdo interno que abarca la entrega de servicios los cuales soporta las TI de la organización en la prestación de sus servicios

Acuerdo de Nivel Operacional *Opertional Level Agreement* OLA, es un acuerdo interno que cubre la entrega de servicios, realizado entre un departamento de TI y la Gestión de Niveles de Servicio.

Acuerdos de Nivel de Servicio en inglés *Services Level Agrameent* (SLA´s). Son Contratos escritos entre un proveedor de servicio y su(s) cliente(s) en el que se documenta el nivel acordado para la calidad del servicio.

Acuerdo de No Divulgación véase acuerdo de confidencialidad**.**

Administración de la demanda Trabaja junto con el cliente para balancear cargas de trabajo y demanda. Ejemplo ejecutando ciertas tareas en horas “libres” (compilar, correr procesos en *batch* de trabajos de impresión largos); busca influenciar la demanda de capacidad, por lo general se realiza a corto plazo porque no hay capacidad suficiente, pero se puede utilizar en el largo plazo cuando es difícil justificar una actualización (*upgrade*).

Ajuste en el rendimiento (*performance tuning*). Consiste en la mejora del rendimiento del sistema, el motivo de esta actividad es por un problema en el rendimiento, que puede ser real o previsto. Muchos sistemas responderán, para incrementar la carga, con algún acuerdo de disminución en el rendimiento. La capacidad de un sistema para aceptar una carga mayor es llamado escalabilidad y la modificación de un sistema para manejar una carga mayor es sinónimo de ese ajuste en el rendimiento. Un ajuste sistemático sigue los siguientes pasos: 1) Evaluar el problema y establecer los valores numéricos que clasificar una conducta aceptable. 2) Medir el rendimiento del sistema antes de la modificación. 3) Identifique la parte del sistema que es fundamental para mejorar el rendimiento. Esto se llama el cuello de botella.4) Modificar esa parte del sistema

para eliminar el cuello de botella. 5) Medir el rendimiento del sistema después de la modificación.

Alteración de paquetes de internet (*internet Spoofing*) Un ataque utilizando las direcciones alteradas o simuladas de paquete de Internet fuente (IP). Esta técnica explota aplicaciones que utilizan autenticación basada en direcciones IP. Esta técnica también puede permitir a un usuario no autorizado tener acceso de raíz en el sistema en cuestión.

Análisis de rendimiento (*performance analysis*), comúnmente denominado perfil, es la investigación del comportamiento de un programa usando información recogida por este cuando se ejecuta (es decir, es una forma de análisis dinámica del programa, en contraposición de un análisis de código estático).El objetivo habitual de el análisis de rendimiento es determinar cuales partes de un programa optimizan la velocidad o el uso de memoria.

Analizador de Protocolo o también conocido como Analizador de tráfico en red o sniffer es un programa de captura de las tramas de red. Es algo común que, por topología de red y necesidad material, el medio de transmisión (cable coaxial, UTP, fibra óptica etc.) sea compartido por varias computadoras y dispositivos de red, lo que hace posible que una computadora capture las tramas de información no destinadas a él. Para conseguir esto el *sniffer* pone la tarjeta de red o *Network Interface Card* (NIC) en un estado conocido como "modo promiscuo" en el cual en la capa de enlace de datos (ver modelo OSI Anexo B) no son descartadas las tramas no destinadas a la MAC *address* de la tarjeta; de esta manera se puede obtener todo tipo de información de cualquier aparato conectado a la red como contraseñas, e-mail, conversaciones de chat o cualquier otro tipo de información personal. La cantidad de tramas que puede obtener un *sniffer* depende de la topología de red, del nodo donde esté instalado y del medio de transmisión.

Aprobación de la Autoridad Designada (DAA por sus siglas en ingles *Designated Approving Authority*) en el departamento de defensa de los Estados Unidos es el funcionario con autoridad para asumir oficialmente la responsabilidad del funcionamiento de un sistema a un nivel aceptable de riesgo.

Ataque DDOS (*Distributed Denial Of Service Attack*) o Ataque de Denegación de Servicio Distribuido es un tipo especial de DoS (*Denial of Service* es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos) consistente en la realización de un ataque conjunto y coordinado entre varios equipos (que pueden ser cientos o miles) hacia un host víctima. Esto es posible gracias a un cierto tipo de malware (software que tiene como objetivo infiltrarse en o dañar una computadora sin el conocimiento de su dueño y con finalidades muy diversas ya que en esta categoría encontramos desde un troyano hasta un spyware.) que permite obtener el control de esas máquinas y que un atacante ha instalado previamente en ellas, bien por intrusión directa o mediante algún gusano. Los DDoS consiguen su objetivo gracias a que agotan el ancho de banda de la víctima y sobrepasan la

capacidad de procesamiento de los *routers*, consiguiendo que los servicios ofrecidos por la máquina atacada no puedan ser prestados. A las máquinas infectadas por el malware mencionado anteriormente se las conoce como máquinas *zombie* (zombis, en español), y al conjunto de todas las que están a disposición de un atacante se le conoce como *botnet* (red de *bots* normalmente es un gusano que corre en un servidor infectado con la capacidad de infectar a otros servidores de forma automatizada).

Base de Datos de Gestión de la Configuración (*Configuration Manager Data Base*) véase CMDB.

Baseline es una línea o un estándar imaginario por el cual las cosas son medidas o comparadas. Especificaciones iniciales establecidas.

BCM Business Continuity Management, por sus siglas en ingles, mediante el análisis y administración de riesgos se intenta garantizar que una organización pueda continuar operando a un nivel mínimo predeterminado. La gestión de la continuidad del negocio (BCM) reduce riesgos y desarrolla planes para restaurar las actividades del negocio si son interrumpidas por un desastre

Biblioteca de software definitivo es la Biblioteca lógica (repositorio) en la cual se tiene las versiones autorizadas de todo el software que está almacenado y protegido, es una/varias bibliotecas físicas donde se tienen las copias maestras de las versiones de software, debe estar separada de la biblioteca de pruebas e incluir software autorizado y aceptado bajo un control estricto de *Change & Release Management*. Puede incluir un lugar físico en donde se almacenan las copias físicas de las copias maestras de manera protegida (Ejemplo acondicionada a prueba de incendios).

Bombas lógicas son en cierta forma similares a los troyanos: se trata de código insertado en programas que parecen realizar cierta acción útil. Pero mientras que un troyano se ejecuta cada vez que se ejecuta el programa que lo contiene, una bomba lógica sólo se activa bajo ciertas condiciones, como una determinada fecha, la existencia de un directorio con un nombre dado, o el alcance de cierto número de ejecuciones del programa que contiene la bomba; así, una bomba lógica puede permanecer inactiva en el sistema durante mucho tiempo y por tanto sin que nadie note un funcionamiento anómalo hasta que el daño producido por la bomba ya está hecho.

BSM Forrester Research, Inc. Lo define como: Administración de Servicios de Negocio a los enlaces dinámicos de negocio enfocados en los servicios de TI sostenidos por la infraestructura Tecnológica. El enfoque de los negocios en los servicios de TI puede ser un servicio específico de estas Tecnologías o parte de un proceso de negocio, pero es un soporte más significativo y visible a la métrica del negocio por el propietario del mismo.

Business Case. Véase caso de negocio

Business Service Management véase BSM

Caballo de Troya (también llamado Troyano) es una pieza de software dañino disfrazado de software legítimo. Los caballos de Troya no son capaces de replicarse por sí mismos y pueden ser adjuntados con cualquier tipo de software por un programador o puede contaminar a los equipos por medio del engaño. Su nombre es dado por su peculiar forma de actuar como los Troyanos de la historia, entrando en la computadora, ocultos en otros programas aparentemente útiles e inofensivos pero que al activarse crean problemas a la computadora al desarrollar la acción de estos archivos infecciosos.

Caso de negocio se utiliza para obtener el compromiso de la administración y la aprobación para la inversión en cambios en el negocio, a través de la justificación de la inversión, El caso de negocio propone un marco de trabajo para la planificación y administración de los cambios en el negocio. La viabilidad del proyecto en curso deberá ser monitoreado contra el caso del negocio, este debe de contener información que cubre cinco aspectos fundamentales: ajuste estratégico, las opciones de evaluación, aspectos comerciales, el que pueda conseguirse o alcanzarse y la adecuación.

Catálogo de Servicio es un listado completo de todos los servicios disponibles para los clientes y usuarios.

CDA siglas de *Confidential Disclosure Agreement* véase Acuerdo de confidencialidad

Certificado digital, en criptografía llave publica certificada, es un identificador que contiene información de su propietario, es decir, estos certificados relacionan la llave pública con algunos de sus atributos. Es avalado por una tercera entidad confiable. Su autenticidad es garantizada por el hecho que solo un organismo oficial puede expedirlo, utilizado para transacciones electrónicas.

CI véase Elemento de Configuración

Cliente es quien en general recibe el servicio; usualmente el administrador responsable por el costo / pago del mismo, ya sea a través de un cargo directo o de manera indirecta en términos de necesidades. (Ejemplo: el Departamento de Ventas).

CMDB es una base de datos que contiene detalles relevantes de cada *Configuration Item* CI y de la relación entre ellos, incluyendo equipo físico, software y relación entre incidentes, problemas, cambios y otros datos del servicio de TI. La CMDB no es una base de datos para los programas de administración ni es una herramienta de auditoria que proporciona información limitada acerca del software y hardware.

Código Malicioso es software que tiene como objetivo infiltrarse o dañar las funciones de una computadora sin consentimiento de su dueño y con finalidades muy diversas como espiar, o permitir un acceso no autorizado por ejemplo.

Compromiso es exponer o poner a riesgo a alguien o algo en una acción o caso aventurado.

Configuration Item véase Elemento de Contiguración.

Conocimiento es la capacidad de convertir datos e información en acciones efectivas, por lo que el conocimiento puede ser explícito (cuando se puede recoger, manipular y transferir con facilidad) o tácito. Este es el caso del conocimiento heurístico resultado de la experiencia acumulada por individuos.

Contratos de Servicio Acordado véase Contratos externos

Contratos escritos entre un proveedor de servicio y su(s) cliente(s) en el que se documenta el nivel acordado para la calidad del servicio.

Contratos externos o contratos de servicios acordados, donde un proveedor externo mediante un contrato, cubre la entrega de los servicios hacia TI.

Control de Acceso Discrecional o DAC por sus siglas en ingles, el usuario que desarrolla, adquiere u obtiene un archivo (programa, aplicación dispositivo, etc.) se considera como su dueño, y como tal es el único con la capacidad de asignar derechos sobre el archivo para otros usuarios.

Control de Acceso Mandatario u Obligatorio también denominado MAC por sus siglas en ingles, los usuarios reciben un nivel de autorización de acceso y la información se clasifica según su sensibilidad. Estos dos parámetros se combinan para crear Clases de Acceso.

Control es una descripción de cómo la GESTIÓN DE LA SEGURIDAD será organizada y la forma en que será administrada.

Control Objectives for Information and related Technology, COBIT, es un conjunto de mejores prácticas para el manejo de información creado por *Information System Audit and Control Association*, ISACA y IT *Governance Institute*, ITGI, en 1992.

Controles de detección son asignados para reservar o dilatar para otro tiempo los errores e irregularidades que se están llevando acabo y asegurar su pronta corrección. Estos controles representan una continuidad de gastos operativa son con frecuencia costoso, pero necesarios, Los controles de detección suministran los medios para corregir errores de datos, además de modificar los controles existentes o la recuperación de los activos perdidos.

Cortex es el manto de tejido nervioso que cubre la superficie de los hemisferios cerebrales, tales redes neuronales, se distinguen en tres tipos básicos de corteza: Isocortex (o Neocortex), que es el último en aparecer en la evolución del cerebro, es el encargado de los procesos de raciocinio; paleocortex, comprende el cerebro olfatorio; Arquicortex, constituido por la formación del hipotálamo, esta es la parte "animal" o instintiva, es la parte del cerebro que se encarga de la supervivencia, las reacciones automáticas y los procesos fisiológicos. Dentro del cortex, se pueden distinguir áreas con capacidad de procesar la información, más eficaces, las áreas del neocortex, asiento o soporte principal del Registro de Lo Simbólico. En los lóbulos como el temporal (las neuronas captan cualidades

sonoras en la corteza auditiva primaria, además de contener neuronas que se relacionan con la comprensión del lenguaje, memoria y aprendizaje), el frontal (contiene la corteza primaria aquí las neuronas controlan los músculos del cuerpo, se distribuye en la corteza cerebral en función de las partes del cuerpo), el parietal (corteza somato sensorial primaria, compuesta por neuronas relacionadas con el tacto, también se organiza en función de las partes del cuerpo), y el occipital (contiene la corteza visual primaria, localizada en la parte posterior, procesa la información visual que llega de la retina) .

Costo Real costos históricos que se han incurrido en un periodo anterior.

Cracker es alguien que viola la seguridad de un sistema informático por un beneficio particular o para hacer daño, como la modificación de código fuente de un programa (denominado cracking). También se les denomina hackers a los aficionados a la informática que buscan defectos, puertas traseras. *Cracker* es aquel individuo que se especializa en saltar las protecciones anti-copia de software, de ahí el nombre crack para definir los programas que eliminan las restricciones en las versiones de demostración de software comercial.

DAA véase Aprobación de Autoridad Designada

DAC véase Control de Acceso Discrecional

DDOS véase ataque DDOS

Declaración de políticas son los documentos que se exponen los requisitos específicos o normas que deben cumplirse. En el ámbito de seguridad de la información, las políticas son generalmente un punto específico, que abarca un espacio único. Por ejemplo, el "Uso Aceptable" la política abarcaría las normas y reglamentos para el uso adecuado de las instalaciones de computo.

Degaussing (borrado seguro) es el proceso de disminuir o eliminar un comportamiento no deseado en un campo magnético. Lleva el nombre de Carl Friedrich Gauss, uno de los primeros investigadores en el campo del magnetismo. Debido a la histéresis magnética, generalmente no es posible reducir un campo magnético completamente a cero, de modo *degaussing* normalmente inducido por un muy pequeño, pero conocido, campo magnético.

Delitos informáticos son actos cometidos mediante el uso indebido de las tecnologías de información cuando tales conductas constituyen el único medio de comisión posible -o el considerablemente más efectivo- para lograr el efecto dañoso que vulnera bienes jurídicos cuya protección es necesaria. Los delitos informáticos de resultado, se refiere a conductas que vulneran los sistemas que utilizan tecnologías de información, es decir, que lesionan el bien jurídico constituido por la información, lo que implica que legislaciones penales conciban como bien jurídico la protección de los sistemas que la contienen, procesan, resguardan y transmiten, puesto que la información no es más que el bien que subyace en ellos. Los delitos informáticos de medio, recoge las conductas que se valen del uso indebido de las tecnologías de información para atentar contra

bienes jurídicos tradicionales, distintos de la información contenida y tratada en sistemas automatizados.

Desastre natural tal es el caso de un movimiento sísmico, un huracán o cualquier otro fenómeno extremo de la naturaleza que se convierte en desastre o catástrofe cuando ocasiona pérdidas humanas o económicas. Es decir, se denomina desastre natural sólo cuando el problema social o económico es detonado por un fenómeno de la naturaleza.

Designated Approving Authority, DAA por sus silgas en ingles, en el Departamento de Defensa de los estados unidos, es el funcionario con autoridad para asumir oficialmente la responsabilidad de la explotación de un sistema a un nivel aceptable de riesgo.

Dimensionamiento de aplicaciones es la evaluación de los requisitos de capacidad (almacenaje, ancho de banda, soporte) necesario para las nuevas aplicaciones o los cambios en estas referentes a software.

Elemento de Configuración (*Configuration Item*) es un componente de la infraestructura que está o estará bajo el control de la Gestión de la Configuración (*Configuration Management*). Pueden variar en complejidad, tamaño y tipo – desde un sistema entero hasta un módulo o un componente menor de hardware.

Error conocido es un problema del que se conoce la causa raíz y se tiene identificada la falla en el Elemento de Configuración (CI). Un error conocido cuenta con una solución temporal o una alternativa permanente. A partir de un error conocido puede generarse un Requerimiento para cambio *Request For Change* [RFC]. Sin embargo, la situación permanecerá como error conocido hasta que el cambio se haya implantado y sea definitivo.

Escáner de puertos o escaneo de puertos se emplea para designar la acción de analizar por medio de un programa el estado de los puertos de una máquina conectada a una red de comunicaciones. Detecta si un puerto está abierto, cerrado, o protegido por un firewall.
Se utiliza para detectar qué servicios comunes está ofreciendo la máquina y posibles vulnerabilidades de seguridad según los puertos abiertos. También puede llegar a detectar el sistema operativo que está ejecutando la máquina según los puertos que tiene abiertos.

Evaluación clasificación y control de documentos en un inventario exhaustivo de los bienes con la responsabilidad asignada para asegurar que protección eficiente es mantenida.

FTP Véase Protocolo de transferencia de archivos

Gadget es aquel dispositivo que tiene un propósito y una función específica, generalmente de pequeñas proporciones, práctico y a la vez novedoso. También es el término que se le ha dado a la nueva categoría de mini aplicaciones, diseñada para proveer de información o mejorar una aplicación o servicio de una computadora, o bien cualquier tipo de interacción a través de la Internet, por ejemplo una extensión de alguna aplicación de negocios, que provea información en tiempo real del estatus del negocio u organización.

Gestión de la continuidad del negocio Véase BCM.

Gestión de sistemas, aplicaciones y procesos productivos alineada a objetivos de negocio

Gestión Total de Calidad TQM por sus siglas en ingles *Total Quality Manegement* es una estrategia de gestión encaminada a la sensibilización de la introducción de la calidad en todos los procesos organizacionales. La Calidad Total proporciona un paraguas bajo el cual todos los miembros de la organización puede procurar la satisfacción de los clientes y crear continuamente inferior a los costos reales.

Guerra de la información es el uso y la gestión de la información en la búsqueda de una ventaja competitiva sobre un rival. La guerra de la información puede incluir la recolección de información táctica, la garantía de que la propia información es válida, la difusión de la propaganda o la desinformación para desmoralizar al enemigo y a la opinión pública, lo que socava la calidad de oponerse a la fuerza de información y la denegación de la recopilación de información de oportunidades a las fuerzas de oposición.

Hacker es un experto en alguna o varias ramas de las Tecnologías de Información y las telecomunicaciones: programación redes de computadoras, sistemas operativos, hardware. Hacker de la palabra inglesa hace referencia a divertirse con el ingenio. Hacker es toda aquella persona con elevados conocimientos informáticos independientemente de la finalidad con que los use.

Hacking es la técnica o arte de encontrar los límites de los productos, aparatos y servicios digitales de informática o comunicaciones y compartirlo con otros y/o los fabricantes mismos de ésos productos.

Herramientas de escaneo tienen la finalidad de someter mediante algún mecanismo a una exploración con la finalidad de producir una representación mayormente detallada del objeto o situación en cuestión.

Host en términos generales es una computadora con una posición especifica en una red de computadoras (network), También puede denominarse nodo.

ICC véase tarjeta inteligente

ICT (*Information and Communications Technology*) incluye tecnologías como computadoras de escritorio y portátiles, software, periféricos y conexiones hacia Internet que son previstos para satisfacer procesamiento de información y

funciones de las comunicaciones.

ICT (*Information and Communications Technology*)Tecnologías de la información y las comunicaciones. ICT incluye tecnologías como computadoras de escritorio y portátiles, software, periféricos y conexiones hacia Internet que son previstos para satisfacer procesamiento de información y funciones de las comunicaciones.

ICT es un acrónimo de tecnología de la información y las comunicaciones

Identificar y evaluar tecnologías que proporcionen economía de escala (procesamiento paralelo, arreglos de almacenamiento).Monitorear e informar las tendencias de uso de recurso y desempeño a corto, mediano y largo plazo, es parte de la administración de los recursos.

Incidente es cualquier desviación de la operación estándar, que causa o puede causar una interrupción o reducción de la calidad del servicio de TI.

Indicadores clave de rendimiento, del inglés Key Performance Indicators (KPI), miden el nivel del desempeño de un proceso, enfocándose en el "como" e indicando que tan buenos son los procesos, de forma que se pueda alcanzar el objetivo fijado

Indicio inminente considérese como un evento próximo a suceder y que tiene la posibilidad de con llevar un riesgo (origen de una amenaza). Cualquier intento y método con un objetivo de explotación intencional de una vulnerabilidad o también como una situación o método que puede accidentalmente desencadenar una vulnerabilidad.

Informática es la disciplina que estudia el tratamiento automático de la información utilizando dispositivos electrónicos y sistemas computacionales. Lo que hoy conocemos como informática es la interacción de muchas de las técnicas y de las máquinas que a lo largo de su historia el hombre ha desarrollado para ayudarse y aumentar sus capacidades de memoria, de pensamiento y de comunicación.

Infraestructura de TI es el conjunto de hardware, software y documentación asociada, que se utiliza como soporte a las metas del negocio.

Ingeniería social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Un ingeniero social usará comúnmente el teléfono o Internet para engañar a la gente y llevarla a revelar información sensible, o bien a violar las políticas de seguridad típicas. Con este método, los ingenieros sociales aprovechan la tendencia natural de la gente a confiar en su palabra, antes que aprovechar agujeros de seguridad en los sistemas informáticos. Generalmente se está de acuerdo en que "los usuarios son el eslabón débil" en seguridad; éste es el principio por el que se rige la ingeniería social.

ITSM es una disciplina basada en procesos, enfocada en alinear los servicios de Tecnologías de Información proporcionados con las necesidades de las

empresas, poniendo énfasis en los beneficios que puede percibir el cliente final, además propone cambiar el paradigma de gestión de TI, por una colección de componentes enfocados en servicios "end-to-end" usando distintos marcos de trabajo con las "mejores prácticas", como por ejemplo la Information Technology Infrastructure Library (ITIL) o el eSCM (enabled Service Capability Model).

ITSM es una disciplina basada en procesos, enfocada en alinear los servicios de Tecnologías de Información proporcionados con las necesidades de las empresas, poniendo énfasis en los beneficios que puede percibir el cliente final, además propone cambiar el paradigma de gestión de TI, por una colección de componentes enfocados en servicios "end-to-end" usando distintos marcos de trabajo con las "mejores prácticas", como por ejemplo la Information Technology Infrastructure Library (ITIL) o el eSCM (enabled Service Capability Model). Entre los que se destacan para ITIL Entrega de Servicios (Service Delivery) y Servico de asistencia (Service Support).

ITT por las siglas en ingles Information Technology Tender, Licitaciones referentes a TI.

Kerberos es el nombre de un protocolo de autenticación en redes de computadoras, el cual permite comunicaciones individuales sobre redes no seguras, probando su identidad de manera segura. Esto es también una suite de software libre del MIT que implementa este protocolo. Este diseñado con el propósito del modelo cliente servidor y proveyendo una autenticación mutua, ambos el usuario y el servidor verifican la identidad del otro, los mensajes del protocolo Kerberos son protegidos contra los ataques de replicación e intercepción o escucha. Kerberos se basa en criptografía de llave simétrica y requiere una tercera parte confiable Extensiones de Kerberos puede prever el uso de la criptografía de clave pública durante ciertas fases de la autenticación.

Key Performance Indicators véase indicadores clave de rendimiento.

KPI véase indicadores clave de rendimiento.

La declaración de los requisitos o SoR por sus siglas en ingles de *Statements of Requirement*

Los receptores sensoriales son los órganos capaces de captar los estímulos del medio ambiente (órganos de los sentidos) y del medio interno (receptores viscerales) En los receptores sensoriales la energía del estímulo se transforma en el lenguaje informático del organismo, mientras que en los estímulos ambientales de distinto tipo inducen en los receptores sensoriales ubicados en la cabeza y en la piel, la generación de señales eléctricas que viaja por vías específicas hasta centros nerviosos también específicos donde se generan sensaciones particulares. Normalmente tenemos conciencia de este tipo de información. Del mismo modo, estímulos del medio interno actúan sobre sistemas sensoriales específicos, pero la información que transportan, al actuar sobre los centros que les corresponden, no siempre generan sensaciones. La conciencia que tenemos

de este tipo de información es limitada

MAC véase Control de Acceso Obligatorio

Marco de trabajo en la gestión de la seguridad es el marco de referencia donde se establece la administración para iniciar y controlar la implementación de la seguridad de l a información dentro de una organización y poner en curso la disposición de la seguridad de la información.

Market Intelligence (MI) – es la información relativa a los mercados de una empresa, se reúnen y analizan específicamente con el fin de precisar y confiar en la toma de decisiones en la determinación de oportunidades de mercado, en la estrategia de penetración en el mercado, en el desarrollo de los mercados y las nuevas cifras, es decir, es el proceso de adquirir y analizar la información a fin de comprender el mercado (tanto los clientes actuales y potenciales), para determinar las necesidades actuales, futuras y las preferencias, además de las actitudes y el comportamiento del mercado, y Evaluar los cambios en el entorno empresarial que pueden afectar el tamaño y la naturaleza del mercado en el futuro.

Medición del rendimiento es el proceso de evaluar el progreso hacia el logro de objetivos predeterminados. La gestión del rendimiento se basa en este proceso, añadiendo la comunicación pertinente y la adopción de medidas sobre los progresos realizados contra los objetivos predeterminados

Mesa de Servicio (*Service Desk*) Punto único de contacto de clientes y usuarios, en el apartado de Servicios de Asistencia (*Service Support*) se hondará más en esta función característica de la metodología de ITSM (Administración o Gestión de servicios de TI) de donde se desprenden las buenas prácticas y procedimientos de ITIL.

MI véase *Market Intelligent.*

Modelación mediante Técnicas y/o herramientas para predecir y optimizar los recursos, a partir de predecir el comportamiento de los servicios de TI, bajo cierto volumen y variedad de trabajo (desde estimar hasta hacer prototipos de prueba).

Modelo de Capacidad y Madurez o CMM (*Capability Maturity Model*), es un modelo de evaluación de los procesos de una organización. Fue desarrollado inicialmente para los procesos relativos al software por la Universidad Carnegie-Mellon para el SEI (*Software Engineering Institute*)

NDA véase acuerdo de confidencialidad

Neguentropía, la podemos definir como la fuerza opuesta al segundo principio de la termodinámica, es una fuerza que tiende a producir mayores niveles de orden en los sistemas abiertos, y la podemos relacionar con la conservación de la Energía, que predice que ésta ni disminuye ni aumenta, simplemente se transforma constantemente, y, en el caso de sistemas abiertos, con cualidad negantrópica, aumentando su nivel de organización. En tal sentido se puede considerar la neguentropía como un mecanismo auto-regulador con capacidad de sustentar, es decir con una capacidad y un poder inherente de la energía de manifestarse de incontables formas y maneras. La neguentropía favorece la subsistencia del sistema, usando mecanismos que ordenan, equilibran, o controlan el caos. Mecanismo por el cual el sistema pretende subsistir y busca estabilizarse ante una situación caótica.

Non Disclosure Agreement véase acuerdo de confidencialidad

Objeto del Mundo Real la encontramos por sus siglas en ingles como RWO (*Real Word Object*) Objetos identificados en los componentes de un proceso donde el objeto (tangible) tiene una forma física (pieza de papel o meramente información en formato electrónico) como auxiliar en la realización de tareas.

OLA véase Acuerdo de Nivel Operacional

Operacional Level Agreement véase Acuerdo de Nivel Operacional.

Outsourcing pasó a formar parte del léxico de negocios durante la década de 1980 y se refiere a la delegación de las operaciones no esenciales de la producción interna a una entidad externa especializada en la gestión de esta operación. *Outsourcing* es la utilización de expertos de fuera de la entidad para llevar a cabo tareas específicas que la entidad una vez realizadas las tomara a su cargo.

PDU (*Protocol Data Unit*) que especifica los datos que serán enviados a la capa del protocolo par en el extremo de recepción.

Performance Analysis véase Análisis de Rendimiento

Performance tuning véase Ajuste en el rendimiento.

PMF por sus siglas en ingles, *Process Maturity Framework*, Marco de Referencia en el Proceso de Madurez

Política de liberación define los roles y responsabilidades, las guías y detalles para cada sistema o servicio; incluyendo su nombramiento, numeración, criterios para determinar el impacto, estatus de emergencia, ventanas de mantenimiento y activación de su plan de reversa (*back out*).

Prioridad es la secuencia en la cual un incidente o problema requiere ser resuelto, se acuerdo a su impacto y urgencia.

Problema es una condición identificada en múltiples incidentes que exhiben síntomas comunes y de la cual no se conoce la causa (y se confirma que un Ítem

de Configuración (CI) falla).

Protocolo de transferencia de archivos (FTP) proporciona los elementos básicos de la compartición de archivos entre máquinas. FTP utiliza TCP para crear una conexión virtual para la información de control y, a continuación, crea una conexión TCP para las transferencias de datos. La conexión utiliza el control de una imagen del protocolo Telnet para el intercambio de comandos y mensajes entre hosts.

Pruebas de Penetración están diseñadas para detectar vulnerabilidades y brechas de seguridad que puedan ser utilizadas por personas malintencionadas para atacar y penetrar en la red interna de una organización.

Pruebas y evaluaciones de seguridad, también abreviado como ST&E por sus siglas en ingles *Security Test and Evaluation* es la examinación o análisis de las medidas proactivas que son interpuestas en un sistema de información una vez este plenamente integrado y funcional. Los objetivos del ST&E son descubrir los desperfectos en las fases de diseño, implementación y operación que podrían permitir la violación de la política de seguridad; determinar los mecanismos adecuados de seguridad, las garantías y otras propiedades para hacer cumplir las políticas de seguridad; Evaluar el grado de consistencia entre la documentación del sistema y su implementación.

Puerto en los protocolos de TCP y UDP usados en computadoras en red, un puerto es un número especial que se presenta en la cabecera de un paquete de datos. Los puertos son típicamente usados por los asociar datos a un particular proceso corriendo en una computadora.
Los puertos se pueden explicar fácilmente con una analogía: pensar en las direcciones IP como la dirección postal de un edificio de apartamentos, y el número de puerto como el número de un apartamento dentro de ese edificio. Si una carta (un paquete de datos) se envía al edificio de apartamento (IP) sin el apartamento número (número de puerto) en él, entonces nadie sabe quién (qué servicio) es para. A fin de que entregue el trabajo, el remitente tiene que incluir un número de apartamento junto con la dirección para garantizar la carta llegue a la residencia.
A modo de ejemplo, un servidor utilizado para enviar y recibir correo electrónico puede proporcionar tanto un SMTP (para el envío) y un POP3 (para recibir); estos se canalizarán a través de diferentes procesos de servidor, y el número de puerto que se utilizará para determinar qué datos Que se asocia con el proceso. Por convenio, el servidor SMTP se escucha en el puerto 25, mientras que POP3 escuche en el puerto 110, aunque es posible utilizar diferentes puertos.

RBAC por sus siglas en ingles *Role Based Access Control*, control de acceso basado en roles, se basa en tres aspectos. Grupos y usuarios, roles donde los usuarios y grupos son asignados y privilegios, los atributos de cada rol o capacidades de acceso la granularidad de este control de acceso permite asignar un grupo de privilegios característicos de un rol y otros mas específicos con el

objetivo del menor privilegio.

Release véase también versión.

Requerimientos de Nivel de Servicio *Service Level Requirement* SLR, son una lista de los servicios solicitados por los clientes, son una parte integral del criterio de diseño de los servicios, donde la especificación funcional es parte de estos requisitos, cubre las definiciones detalladas de las necesidades del cliente y son usados para desarrollar, modificar e iniciar servicios. Puede servir como una base para diseñar un servicio y su *Service Level Agreement* SLA.

Requermiento de Cambio Solicitud de cambio en algún elemento de Configuración, infraestructura, etc.

Request for Change véase Requerimiento para cambio

RFC véase Requerimiento para cambio

RWO *Real Word Object* véase Objeto del Mundo Real

Salvaguarda cosa que asegura o protege contra algún riesgo o necesidad también se refiere a un control con la finalidad de asegurar o proteger contra algún riesgo o necesidad.

Sección de seguridad de los acuerdos de Nivel de seguridad. Es el párrafo de los acuerdos de seguridad por escrito entre un proveedor de servicios y el cliente que los documenta de acuerdo con el nivel de servicio en sí

Secrecy Agreement véase Acuerdo de Confidencialidad

Secure Socket Layer es un protocolo criptográfico que provee comunicaciones seguras en una red, como Internet, para aspectos como la navegación Web, el correo electrónico, mensajes instantáneos (*messenger*) y otros datos transferidos.

Service Desk véase Mesa de Servicio

Service Level Requirements véase Requerimiento de Nivel de Servicio.

Service Pack es una colección de actualizaciones, reparaciones y/o mejoras desarrolladas en la forma de un sencillo e instalable paquete.

Sistema de Archivos o por la palabra en ingles *filesystem* se refiere al método para almacenar y organizar los archivos de una computadora y los datos que estos contienen para hacer más fácil el acceso a ellos.

Sistema de Gestión de Calidad QMS que significa en ingles *Quality Management System*

Sistema Operativo es el software que administra la compartición de los recursos en una computadora.

SLA véase Acuerdos de Nivel de Servicio

SLR véase Requerimientos de Nivel de Servicio.

Solución Temporal en inglés *Workaround* es un método para “atacar” un incidente o problema, sea por una solución temporal o a través de una técnica, Se deben presentar y elaborar los detalles para soluciones temporales.

SSH es un protocolo de red que permite el intercambio de datos entre dos computadores sobre un canal seguro. SSH utiliza criptografía de llave publica para autenticarse con la computadora remota y permitir a la computadora remota autenticar a l usuario si es necesario.

SSL véase *Secure Socket Layer*

ST&E Véase Pruebas y evaluaciones de Seguridad.

sniffer véase Analizador de Protocolos

Tarjeta inteligente, tarjeta con chip o tarjeta con un circuito integrado (ICC *Integrated Circuit Card*) es definido como una tarjeta de bolsillo con un circuito integrado incrustado el cual puede procesar información. Esto indica que puede recibir entradas que se procesa, por medio de la solicitud en la aplicación de la tarjeta con el circuito integrado (ICC), y entregado como una salida. Las tarjetas de memoria contienen únicamente memoria no volátil, la memoria que almacena los componentes, y algunos periféricos específicos para la seguridad lógica. Las tarjetas con microprocesador contienen memoria volátil y componentes de microprocesador. Las tarjetas inteligentes son normalmente hechas de plástico, PVC, la tarjeta presenta también en algunos casos un holograma que impide la falsificación.

Tecnologías de Información o también denominado simplemente TI, se encargan del estudio, desarrollo, implementación, almacenamiento y distribución de la información mediante la utilización de *hardware* y *software* como medio de sistema informático y otros relativos al tratamiento de la información en los estados que esta se encuentre. Las tecnologías de la información son una parte de las tecnologías emergentes que hacen referencia a la utilización de medios informáticos para almacenar, procesar y difundir todo tipo de información o procesos de formación educativa.

Telnet es un protocolo de la pila de TCP/IP que emula una Terminal, la emulación se da por que el procesamiento realizado no se hace en la maquina del usuario si no que en una maquina remota también denominada Terminal tonta por este hecho, Telnet tiene la posibilidad de transferir datos en formato binario, emular terminales graficas, y transmitir información para ayudar en la administración centralizada de las Terminales. Telnet consigue una conexión virtual entre el cliente y el servidor.

TI véase Tecnologías de Información.

Tolerancia a fallos o también denominado *Failover*, Sistema de Recuperación; es la capacidad de cambiar automáticamente a un equipo redundante o de respaldo de el servidor, el sistema, o de la red sobre la falla o terminación anormal del servidor activo anteriormente, el sistema, o de la red. El sistema de recuperación ocurre sin la intervención humana y, en general, sin previo aviso, a diferencia de cambiarse.
Los diseñadores de sistemas suelen proporcionar la capacidad de tolerancia a fallos de en los servidores, sistemas o redes que requieren disponibilidad continua y un alto grado de fiabilidad.
En algunos casos, el sistema informático de fallos no se desea automatizarlo, sino que se requiere la intervención humana para efecto del sistema de recuperación. Esto se llama "automatizado con la aprobación manual", ya que la actividad es automática una vez que se da la aprobación.

Token es un único identificador el cual es generado y enviado desde un servidor a un software cliente para identificar una interacción, también denominada sesión *token.* Los *tokens* denominados de seguridad, también conocidos como *tokens* en hardware, *token* para autenticación o *token* criptográfico, es un dispositivo físico que un usuario autorizado de los servicios de computo se le da para auxiliar en el proceso de autenticación. En cuanto al *token* de acceso, se refiere a un objeto del sistema representando al sujeto a las operaciones de control de acceso.

TQM véase Gestión Total de Calidad

Underpinning Contrats es un contrato con un proveedor externo que cubre la entrega de Servicios que apoyan a las TI de la organización en su prestación de servicios, véase contratos de servicio acordado.

Unidad de datos de servicio, SDU por sus sigla es inglés *Service Data Unit* es un sistema de datos que son enviados por un usuario de los servicios de una capa dada, y se transmite a un usuario de servicio del par semántico sin cambiar. El SDU es básicamente los datos que cierta capa pasará hacia una capa inferior.

Usuario es la persona que recibe los servicios día con día (Ejemplo: el vendedor del departamento de ventas)

Versión (*release*) es una colección de nuevos y/o cambios de *Configuration Items* CIs de una unidad de versión, los cuales fueron probados e introducidos en el ambiente de producción.

Virus son programas que se replican y ejecutan por sí mismos, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en una computadora, además tienen, básicamente, la función de propagarse, replicándose, pero algunos contienen también una carga dañina (*payload*) con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando tráfico inútil.

White paper es un documento de informe. Los *White papers* son utilizados para educar a los clientes, recogiendo un conjunto de indicios o señales que pueden conducir a la averiguación de algo por parte de una compañía o ayudan a las personas en la toma de decisiones, pueden ser también un informe de gobierno delineando una política.

Workaround véase solución temporal.

ANEXO B Transmisión de mensajes en red

B.1.Telefonía. Conmutación de circuitos

La conmutación de circuitos tiene como característica principal que al establecer una comunicación el canal, es decir el medio, esta dedicado para esa comunicación hasta el termino de la sesión.

Figura 1 Conmutación manual de circuitos[1]

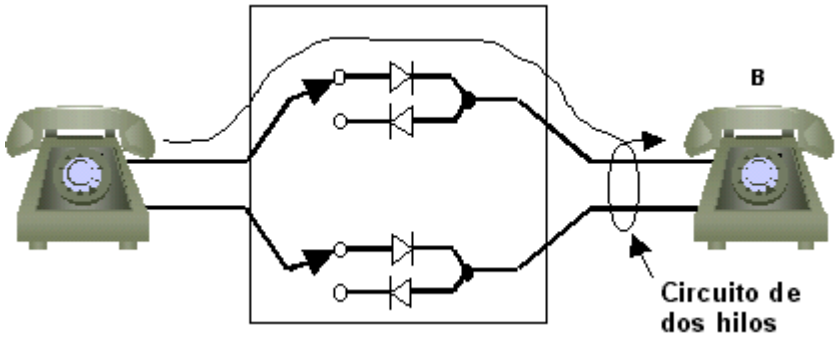

Figura 2 Conmutación automática de circuitos[2]

La conmutación de circuitos de forma manual, lo hacia un operador que interconectaba a las partes que deseaban establecer una comunicación mediante

previa petición de alguno de los interlocutores. Mientras que en la conmutación de circuitos de forma automática, no el operador, ya no necesita establecer el medio para una comunicación si no que los circuitos se cierran automáticamente, la aplicación más usada hoy en día en nuestro país que es la telefonía.

B.2. Internet- Protocolos de Conmutación de paquetes

La conmutación de paquetes se caracteriza por dividir en paquetes los datos o información a transmitir y se envían de forma individual.
El medio por donde se transmite no se dedica a una sola comunicación si no a varias, es decir, por el mismo medio se transmiten comunicaciones de diferentes usuarios,
El medio de transmisión, por lo anterior, es compartido por los usuarios permitiendo con esto que la información o datos a transmitir puedan seguir diferentes rutas hasta llegar a su destino.
Los paquetes recibidos son reagrupados.

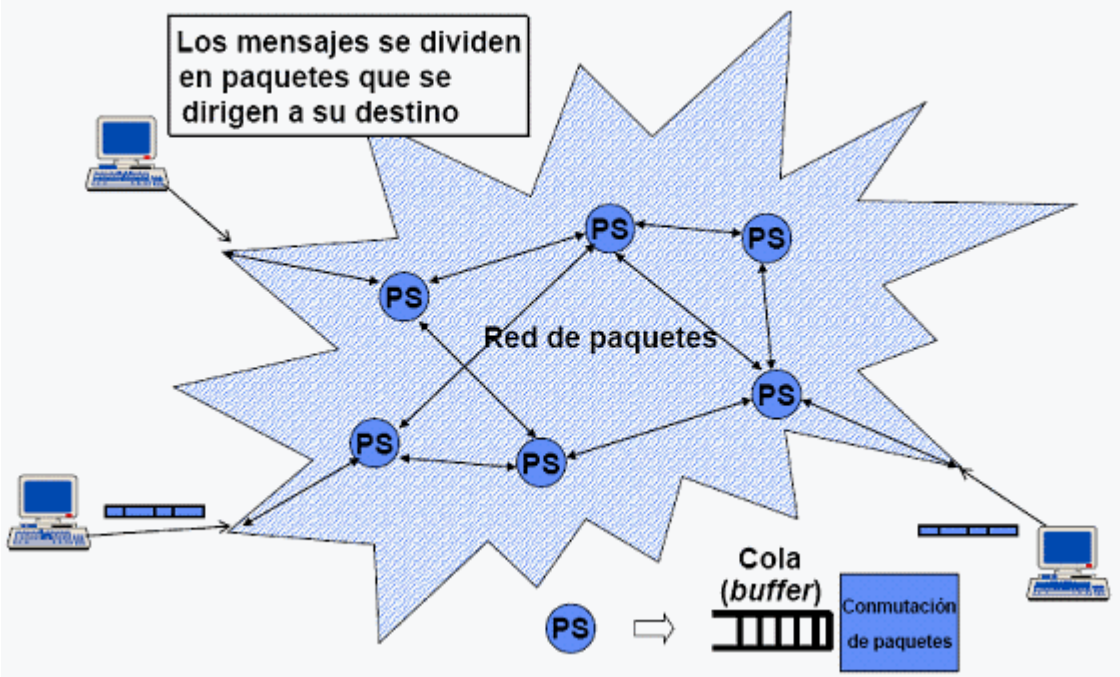

Figura 3 Envío de paquetes en una Red[3]

Como puede observarse en la imagen anterior, Envío de paquetes en una Red, el emisor realiza una segmentación de la información o de los datos en paquetes, los que se des agrupan para su envío, paquete por paquete, en un buffer y posteriormente en el punto de destino se vuelven a agrupan.

Principales diferencias entre la conmutación de circuitos y la conmutación de paquetes						
Conmutación de Circuitos	**Medio**	**Enlace**	**Forma**	**Velocidad**	**Ancho de Banda**	**Prioridad**
	Línea física dirigida de principio a fin. Una sola ruta	**Físico**	**Se cierran circuitos**	**Máxima**	**Desperdiciado (se dedica la línea a una sola comunicación hasta el termino de está aunque existan intervalos sin envío)**	**La primera en llegar se atiende**
Conmutación de Paquetes	**No hay línea física. Múltiples rutas**	**Lógico**	**Decisión por software**	**Depende de la cantidad de paquetes a enviar**	**Comparten el ancho de Banda varias comunicaciones**	**Jerárquica**

Tabla 1 Conmutación de circuitos/ Conmutación de paquetes

B.3. Modelo OSI-

Open System Interconection (OSI)	**No depende de la arquitectura**	
	Esta constituido de siete capas	**7 Aplicación** **6 Presentación** **5 Sesión** **4 Transporte** **3 Red** **2 Enlace de datos** **1 Física**
	Las capas superiores proporcionan información a las capas inferiores en forma secuencial	
	Cada capa es independiente, es decir, no "sabe " más que lo correspondiente a su capa	

Tabla 2 Modelo OSI

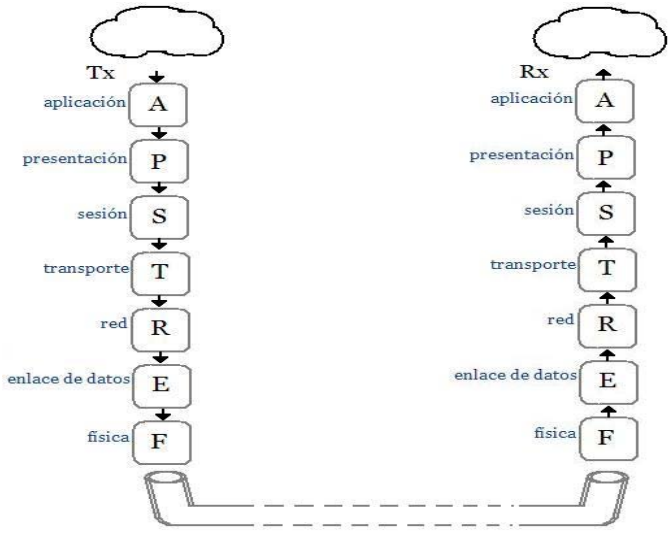

Figura 4 Transmisión/Recepción en el modelo OSI

En la producción en serie hay varias etapas para la elaboración de un determinado producto, etapas de proceso que se llevan acabo de manera sincronizada, de manera análoga, en el modelo OSI hay varias capas, cada una de las cuales complementa a la que le precede.
En esta figura, Transmisión/Recepción en el modelo OSI, puede observarse como se realiza la transmisión, Tx, de datos desde la capa superior, aplicación, y va descendiendo hasta la capa física, en donde los datos viajan por la red.
El receptor, Rx, al obtener los datos por medio de la capa inferior, va ascendiendo por este modelo en capas.

Del descenso de los datos a través de cada una de las capas se desprende otro concepto primordial que permite comprender cómo es que se logra una comunicación basando esta en el modelo OSI, este concepto es conocido como encapsulamiento. Mientras que de la ascensión de los datos a través de cada una de las capas se desprende el concepto de desencapsulamiento.

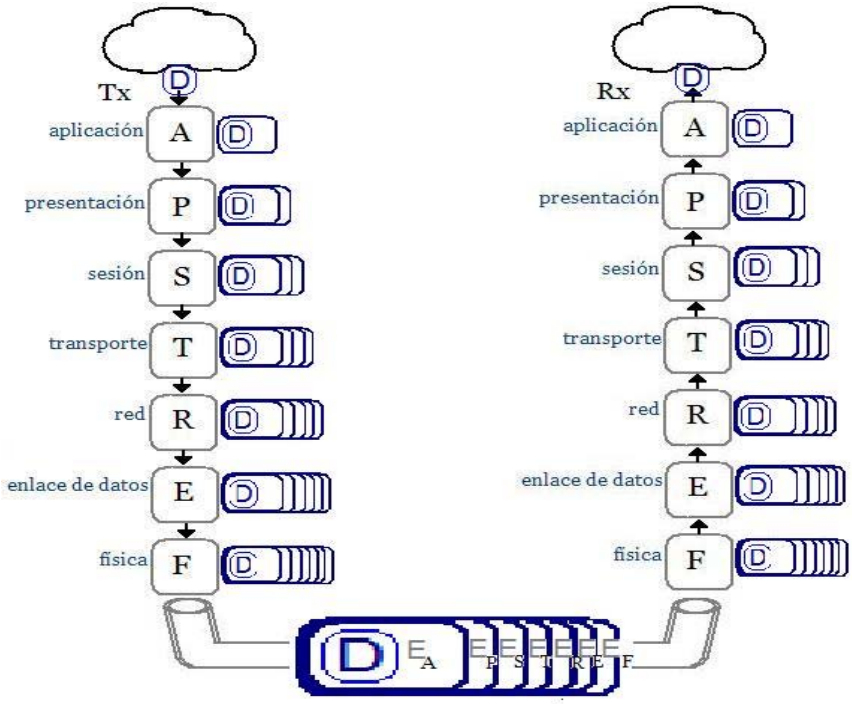

Figura 5 Encapsulamiento/Desencapsulamiento y Encabezados en OSI

Al escribir una carta para enviarla por correo, es primero puesta en un sobre, donde se agregan los datos propios para que llegue a su destino, para después ponerle el sello postal.

De manera análoga ocurre con el encapsulamiento, al descender por cada capa le agrega un encabezado que le dará las directivas para su proceso; E_A, Encabezado de la capa de Aplicación, E_P, Encabezado de la capa de presentación, E_S, Encabezado de la capa de Sesión, E_T, Encabezado de la capa de Transporte, E_R, Encabezado de la capa de Red, E_E, Encabezado de la capa de Enlace de Datos, E_F, Encabezado de la capa Física.

Al recibir la carta, en el buzón, se verifica el destinatario para que este la extraiga de su envoltorio y pueda leerla.

También ocurre algo similar con el desencapsulamiento pasando por una serie de intermediarios que extraen lo que a cada uno le corresponde hasta el tope de este modelo en capas. También puede verse que conforme va escalando el modelo se elimina el encabezado, por la misma capa, pero del lado de la recepción. De lo anterior se desprende que la comunicación en el Modelo OSI se realiza a un mismo nivel, es decir Capa Física del que transmite, se comunica con la Capa Física del que recibe, y así sucesivamente para todas las capas.

B.4.Capas del Modelo OSI

Aplicación	**Se encarga de definir todos los aspectos relacionados con una aplicación**
Presentación	**Toma una presentación estándar (Código ASCII, ABCD). En esta capa solo conoce dos diferentes codificaciones la propia y la estándar lo que le permite hacer la decodificación y codificación de la estándar a la suya y viceversa.**
Sesión	**Se encarga de controlar la sesión, abrirla y cerrarla.**
Transporte	**En esta capa se forman segmentos, además de verificar la integridad de los datos.**
Red	**Toma la decisión de la ruta a tomar para llegar a su destino.**
Enlace de Datos	**Parte de Software y Hardware que nos permiten el acceso al medio**
Física	**Cableado, voltajes e Impedancias**

Tabla 3 Capas del Modelo OSI

Tecnologías y protocolos de red*	
Nivel de aplicación	DNS, FTP, HTTP, IMAP, IRC, NFS, NNTP, NTP, POP3, SMB/CIFS, SMTP, SNMP, SSH, Telnet, SIP, *ver más*
Nivel de presentación	ASN.1, MIME, SSL/TLS, XDR, *ver más*
Nivel de sesión	NetBIOS, ONC RPC, DCE/RPC *ver más*
Nivel de transporte	SCTP, SPX, TCP, UDP, *ver más*
Nivel de red	AppleTalk, IP, IPX, NetBEUI, X.25, *ver más*
Nivel de enlace	ATM, Ethernet, Frame Relay, HDLC, PPP, Token Ring, Wi-Fi, STP, *ver más*
Nivel físico	Cable coaxial, Cable de fibra óptica, Cable de par trenzado, Microondas, Radio, RS-232, *ver más*
* según el **Modelo OSI**	

Figura 6 Protocolos[4]

B.5. Capas o Niveles del TCP/IP

En TCP/IP se distinguen cuatro capas, las cuales tienen una equivalencia, en cuanto a funcionalidad, con las capas del modelo OSI. La capa de Aplicación, Transporte e Inter Red en TCP/IP están bien definidos a diferencia de la capa inferior, Host a Red que no esta definida, es decir, es independiente de software o hardware alguno proveyendo una base de construcción y evitando limitantes.

Al transmitir datos pasan por las diferentes capas desde la superior, Aplicación hasta llegar a la de Host a Red, también denominada Acceso al Medio.

Capa 4 - Aplicación [Asimilable a las capas 5 (sesión), 6 (presentación) y 7 (aplicación) del modelo OSI]
Capa 3 - Transporte [Asimilable a la capa 4 (transporte) del modelo OSI]
Capa 2 – Inter Red o también denominada Internet [Asimilable a la capa 3 (red) del modelo OSI]
Capa 1 – Host a Red o también denominada Acceso al Medio [Asimilable a la capa 1 (física) y 2 (enlace de datos) del modelo OSI]

En la capa de Enlace, está el control de enlace Lógico (LLC) y el Control de Acceso al Medio (MAC), especificado en el estándar de la IEEE 802.2 y 802.3 respectivamente, y la Capa Física implementadas a nivel software en *drivers* o controladores para los diferentes conectores. Para cada capa MAC existen otras capas Físicas.

TCP/IP es una pila de protocolos entre los que se pueden enlistar TCP, UDP, IP, etc. Dichos protocolos tiene su funcionalidad en un determinado nivel, o capa de estos modelos.

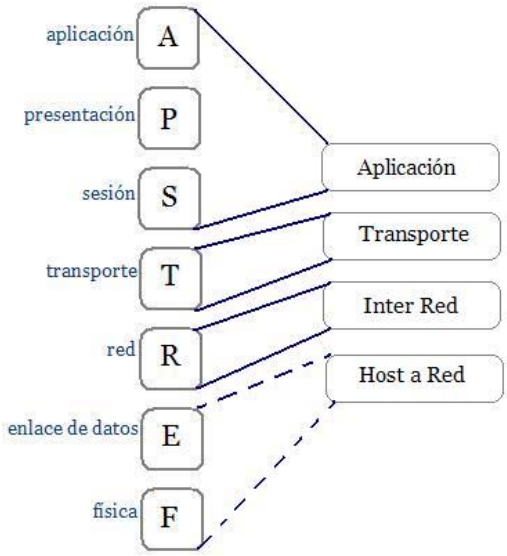

Figura 7 Comparativa del Modelo OSI con TCP/IP

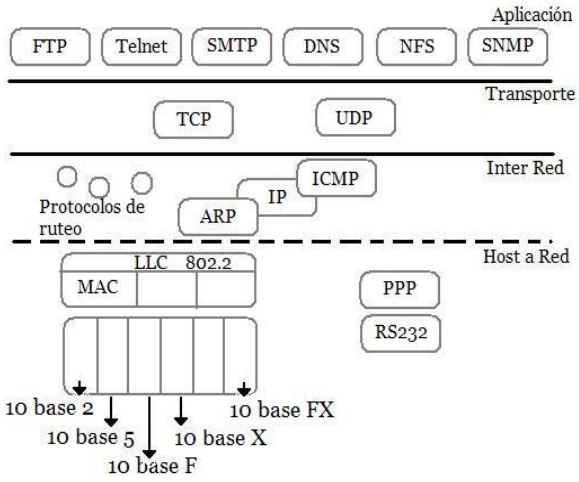

Figura 8 Protocolos Modelo de cuatro capas

Por ejemplo protocolos en la capa de Aplicación se pueden mencionar FTP, Telnet, SMTP, DNS, SNMP, entre otros.

Referencias Anexo B

[1]*Colegio Oficial Asociación Española ingenieros de telecomunicación.* **"Foro Historico de las Telecomunicaciones"** Imagen Disponible en: http://www.coit.es/foro/pub/img/1876_la_telefonia_190_x_289_a45557e8.jpg Leído el 10 Junio 2007.
[2]*Supertel Superintendencia de Telecomunicaciones* **"Telecomunicaciones"** Imagen Disponible en: http://www.supertel.gov.ec/images/telecomunicaciones/t_fija/image002.gif Leído el 10 Junio 2007.
[3] *Monografías* **"Telecomunicaciones"** Imagen Disponible en: http://www.monografias.com/trabajos33/telecomunicaciones/Image7173.gif Leído el 10 Junio 2007.

[4] *Wikipedia La Enciclopedía libre*. **"Modelo OSI"**. Disponible en: http://es.wikipedia.org/wiki/Modelo_OSI Leído el 12 de Junio 2007.

ANEXO C Formato de Caso de Negocio (Business Case)

[Nombre del Departamento] [Dirección del Departamento]

Caso de Negocio

[Nombre del Proyecto]

NOTA HACIA EL LECTOR:

“Los Casos de Negocio utilizan directrices” tienen que ser desarrolladas para acompañar este formato.

Tabla de Contenido

Sección 1

1.Resumen Ejecutivo

[Nombre Del Proyecto]

El Propósito de un Resumen Ejecutivo:

La razón para escribir en un resumen ejecutivo es para proveer una síntesis concisa de los puntos destacados en un caso de negocio. El lector debe ser capaz de entender el proyecto, sobre el rol de éste en el negocio, la PLANEACIÓN/ DIRECCIÓN del departamento, y la justificación para el negocio de la realización de el proyecto. El lector debe comprender la forma en que el proyecto mejora la eficiencia general y / o la eficacia administrativa.

Descripción:

Mientras el Resumen Ejecutivo aparece al inicio del caso de negocio, este se escribe al último.

El Resumen Ejecutivo describirá el objetivo del proyecto, el estado actual de la problemática y las consiguientes oportunidades. Si está fuera del alcance del proyecto en términos generales, y brevemente describir el ambiente competitivo, por ejemplo otra jurisdicción(es) administrativa(s) o actividad(es) en otra(s) empresas. El Resumen ejecutivo también provee de una breve descripción del impacto en el negocio, y el riesgo de llevar acabo el proyecto. Finalmente, este concluye con las recomendaciones y el impacto financiero del proyecto. Este Resumen debe también ser escrito tomando en cuenta los medios de comunicación, es decir la forma en que las partes que interactúan en el proyecto y los afectados por la implantación de éste se comunicarán. El Resumen Ejecutivo es también utilizado para la preparación de un comunicado.

El Resumen ejecutivo debe ser máximo de 2 páginas.

Revisión para un Resumen Ejecutivo:

1. Será el lector teniendo un entendimiento de las razones para la realización del proyecto y los resultados para delimitar el “¿Quién?, ¿Qué?, ¿Cuándo? y ¿Cómo?” del proyecto
2. ¿Contiene alguna información que no este contenida en el cuerpo del caso de negocio? (No debería)
3. ¿Es el Resumen ejecutivo menor que 2 paginas?
4. ¿Puede el Resumen Ejecutivo ser tratado como un documento autónomo?

Sección 2

2.Antecedentes

[Nombre Del Proyecto]

Propósito de la Sección de Antecedentes:

La razón para escribir la Sección de Antecedentes es para proveer al lector de una introducción de lo que se trata el caso de negocio. Esta sección describe la historia y estado actual de los asuntos que dan lugar a, o relacionados hacia la problemática general del negocio, o lo oportuno que es el tema con el caso de negocio.

Problema / Oportunidad

Descripción:

Proporciona una breve descripción del problema del negocio o la oportunidad que el proyecto esta intentando dirigir.

Ejemplos de un problema general del negocio son:

- No conocer las expectativas de los niveles de servicio
- Escalación de los costos de un servicio
- Cambios en los requerimientos del negocio.
- Cambio en la legislación

Situación Actual

Descripción:

Esta sección proporciona una sinopsis de que esta pasando actualmente, si es aplicable, que fue lo que condujo a la situación actual, y que es probable que ocurra si la situación se mantiene. La situación actual puede ser definida en términos de relevancia en cuanto a requerimientos legislativos, estructuras organizacionales y responsabilidades, recursos humanos, procesos y tecnología.

Revisión para la Sección de Antecedentes:

1. ¿Definido en términos generales, es un problema de negocio o una clara oportunidad?

2. ¿Son los hechos relevantes? Indicando al lector que tiene una comprensión clara de la historia y la situación actual y los consiguientes problemas u oportunidades
3. En caso necesario, ¿la situación actual incluye información estadística disponible?

Sección 3

3.Descripción del Proyecto

Propósito de la Sección Descripción del Proyecto:

La razón para escribir una sección de la Descripción del Proyecto es la de proporcionar al lector una definición clara de lo que el proyecto logre (objetivo) de lo que el proyecto incluirá y no incluirá (alcance), cuales son los resultados esperados (expectativas) y quien son los participantes (responsables).

Descripción del Proyecto

Esta sección proporciona una explicación de como el proyecto dirigirá los problemas/oportunidades del negocio identificados en la sección 2.

Objetivos

Describe lo que el proyecto logrará, en términos claros y mensurables en un plazo determinado. Estos objetivos pueden ser utilizados en una revisión posterior a la ejecución para examinar y evaluar el éxito del proyecto. Los objetivos deben formularse de manera lo suficientemente amplia para que las alternativas relevantes sean consideradas y que los costos y beneficios puedan ser formulados. Los objetivos deben centrarse en las metas, no en las operaciones, y en el producto a la salida, no en la producción.

Ejemplos de objetivos incluyen:

- Reducir el tiempo de procesamiento de una hora a 30 minutos, para Marzo del 2003
- Reducir los costos de administración de $1.2 a $1.1 millones para el año fiscal del 2003

Alcance

Esta sección define los parámetros del proyecto. Específicamente, este describe los márgenes de tiempo, departamento/organización, funciones y tecnología.

Márgenes de tiempo (periodos): Explica detalles específicos sobre cuando el proyecto iniciará y terminará

Departamento/Organización: Detalla los lugares específicos, si es aplicable y los departamentos o grupos de departamentos quienes serán involucrados en el proyecto.

Funciones: Describe que funciones del departamento/Organización involucra el proyecto.

Tecnología: Define las fronteras dentro de las cuales el proyecto debe trabajar, por ejemplo uso del sistema existente en cumplimiento de las normas establecidas.

Fuera del Alcance

Esta sección incluye elementos que son específicamente excluidos desde el proyecto.

Resultados Previstos

Esta sección enumera de forma especifica y mesurablemente los entregables del proyecto. Cada resultado incluye un plazo estimado de cuando los resultados / entregables serán completados (en términos del tiempo transcurrido desde el inicio del proyecto).

Resultados/Entregables	Finalización estimada
Documento Detallado de los Requerimientos del Negocio	3 Semanas
Documento del Diseño del Proyecto	6 Semanas

Partes Interesadas

Lista todas las partes interesadas que pueden ser impactadas (positiva o negativamente) internos (Una parte dentro de la administración) o externos (parte externa de la administración) y primaria (los directamente afectados e involucrados en el proyecto) y / o secundaria (impactados, pero no están directamente implicados en el proyecto). Para cada una de las partes incluyen una visión general de sus necesidades comerciales en el proyecto.

Partes Interesadas:	Visión General de los Requerimientos del Negocio
Primaria – Interna	
Parte Interesada 1	Requerimiento 1 Requerimiento 2…
Parte Interesada 2	Requerimiento 1 Requerimiento 2…
Primaria – Externa	
Parte Interesada 1	Requerimiento 1 Requerimiento 2…
Secundaria – Interna	
Parte Interesada 1	Requerimiento 1

	Requerimiento 2…
Parte Interesada 2	Requerimiento 1 Requerimiento 2…
Secundaria – Externa	
Parte Interesada 1	Requerimiento 1 Requerimiento 2…
Parte Interesada 2	Requerimiento 1 Requerimiento 2…

Lista de Revisión para la Sección de Descripción del Proyecto:

1. ¿Está claro que el proyecto se cumplirá?
2. ¿Es claro lo que no está incluido en el proyecto y lo que no se va a lograr?
3. ¿El lector conoce que todas las partes que serán impactadas por el proyecto?
4. ¿Son los requisitos generales, de cada uno de los interesados, claramente establecidos?
5. ¿Son los plazos de los proyectos claramente definidos?
6. ¿El caso de negocio menciona las consultas que se han llevado a cabo con las partes interesadas?.

Sección 4

4.Alineación Estratégica

Propósito de la Sección de Alineación Estratégica:

La razón para escribir la sección de Alineación estratégica es para proporcionar al lector un entendimiento del cómo el proyecto se alinea con el total del plan del negocio y la forma en que pueden llegar a afectar otras iniciativas.

Descripción:

Revisar el plan de negocio para todos los interesados internos e identificar las metas especificas que el proyecto ayudará a realizar. Identificar los niveles de impacto que el proyecto tiene sobre la realización de las metas de varios planes de negocio por ponderar el impacto alto, medio o bajo, utilizando la siguiente guía:

Alto indica que el proyecto es crítico para la realización de las metas
Medio indica que el proyecto impacta directamente la meta pero esto no es crítico para su logro.
Bajo indica un impacto indirecto para la realización de las metas

Metas para El plan del Negocio	Nivel de Impacto	Explicación (si es requerida)

Lista de Revisión para la Sección de Alineación Estratégica:

1. Para las metas que se les han asignado a un nivel alto de impacto, ¿es el proyecto verdaderamente crítico para lograr la meta?
2. ¿La explicación apoya a la evaluación de cómo el proyecto impacta la meta?
3. ¿El proyecto se alinean con el plan de negocios? ¿Habrá apoyo para este proyecto?

Sección 5

5.Análisis del Ambiente

El Propósito de la sección de Análisis del Ambiente:

La razón para escribir la sección de Análisis del Ambiente es proporcionar al lector, en el entendimiento de que otras organizaciones (internas y externas), lo que tienen que hacer o están haciendo para resolver tipos similares de problemas. El lector puede usar esta sección para comparar lo propuesto para el caso de negocio hacia las tendencias de las organizaciones y de las industrias.

Descripción:

El Análisis debe incluir que esta sucediendo en otros departamentos administrativos, otras jurisdicciones administrativas y en la industria privada, que directamente se relaciona con el alcance del proyecto. La investigación puede incluir información:

- La duración del proyecto
- Los resultados específicos del proyecto.
- Factores Críticos de Éxito
- Costos del Proyecto
- Logros
- ¿Qué habrían de hacer las diferente organizaciones?
- Lecciones aprendidas

Esta sección incluye cualquier conclusión de los estudios de investigación que identifican las tendencias de la industria y las mejores prácticas.

Lista de Revisión para el Análisis de Ambiente:

1. ¿Son las organizaciones elegidas para el Análisis de Ambiente representativas de la situación, específicamente en términos de tamaño y complejidad?
2. ¿Son las fuentes de la investigación fiable y han sido verificados los datos?
3. ¿Es el período de tiempo del estudio de investigaciones aplicables a la situación actual?
4. ¿Las conclusiones se han hecho a partir de la investigación?
5. ¿Como es la investigación incorporada o considerada en el caso de negocio?

Sección 6

6. Alternativas

Propósito de la Sección de Alternativas:

La razón para escribir la Sección de Alternativas es para proporcionar al lector un esbozo de la gama de posibilidades de que se dispone para hacer frente al problema o la oportunidad. Ofrece al lector, con razón, de por qué algunas alternativas consideradas viables se han eliminado. Finalmente, esto proporciona una descripción detallada de las opciones viables que dirigirán el problema u oportunidad del negocio. Una opción viable usualmente incluye la opción “el no hacer nada” (status quo).

Descripción:

Lista de todas las posibles soluciones que puede encontrar el problema u oportunidad de negocio. Basado en el análisis practico y con sentido común, reduciendo la lista para incluir únicamente alternativas viables, exponiendo la razón para excluir una alternativa. Alternativas validas no debe ser simplemente excluidas debido a las limitaciones de financiación. Únicamente las alternativas viables serán detalladas y llevadas a las siguientes secciones del caso de negocio.

Para cada alternativa viable, explicar las características clave incluyendo personas, procesos y sistemas. Discutir como cada alternativa viable llevará a la solución de los problemas del negocio y conocerá los objetivos del proyecto con la delimitación del alcance como se indica en la sección 3- Descripción del Proyecto.

Cada alternativa debe ser definida con suficiente detalle para permitir la identificación de impactos específicos (Sección 7- Impactos Operacionales y al Negocio), los riesgos del proyecto (Sección 8 Evaluación de Riegos en el Proyecto) y los beneficios y costos (Sección 9 Análisis Costo Beneficio). Incluir las oportunidades de sociedades y servicios compartidos que pueden aumentar el resultado del negocio de una alternativa.

Incluir cualquier análisis de requerimientos detallado en un apéndice.

Lista de Revisión par alas Alternativas

1. ¿Todas las soluciones posibles han sido identificadas?
2. ¿Todas las alternativas viables han sido determinadas? ¿Las razones de exclusión son suficientes?
3. ¿Son las alternativas verdaderamente distinguibles?
4. ¿Son viable las alternativas definidas a un nivel suficiente de detalle para definir los costos y los beneficios?
5. ¿Donde es posible, de estas alternativas, tomar ventaja de oportunidades de asociaciones y compartición de servicios?
6. ¿Se han destacado para cada alternativa cualquier factor crítico de éxito?
7. ¿Han sido identificadas todas las limitaciones para cada alternativa dada?

Sección 7

7.Impactos Operacionales y al Negocio.

Propósito de la Sección de Impactos Operacionales y al Negocio:

La razón para escribir la sección de Impactos Operacionales y al negocio es proporcionar al lector una lista de todos los impactos operacionales y al negocio para cada parte interesada. Cada impacto es descrito y analizado para cada alternativa viable.

Descripción:

Para cada persona interesada (delimitado en la sección 3) identificar todos los negocios (estratégicos enfocados a largo plazo)e impactos operacionales (procedimientos detallados) que pueden derivarse del proyecto.

Ejemplos de impactos al Negocio son:

- Cambio en el servicio y / o productos que se prestan.
- Cambio en el foco o la dirección del departamento

Ejemplos de impactos operacionales son:

- La capacitación del personal necesario
- Reducción de los recursos de personal

Para cada impacto identificado se antepondrá su magnitud (alto, medio, bajo o ninguno) para cada alternativa usando las siguientes directrices:

> Alto indica que la magnitud del impacto es significativa y que se necesita de las partes interesadas apoyo y preparación para el éxito de la alternativa.
> Medio indica que el impacto es manejable para las partes interesadas.
> Bajo indica que la alternativa tendrá un impacto menor para las partes interesadas

Ninguno indica que las partes interesadas no serán impactadas por la alternativa.

Si es necesario, documentar la justificación de la evaluación

Impacto y Descripción	**Alternativa 1**	**Alternativa 2**	**Alternativa 3**
Parte Interesada 1:			
Impacto 1 – una descripción del impacto 1	Alto	Medio	Alto
Impacto 2 – una descripción del impacto 2	Medio	Medio	Medio
…			
Parte Interesada 1:			
…			
…			

Lista de Revisión para los Impactos Operacionales y al Negocio

1. Para cada parte interesada, ¿todos los impactos del negocio y operacionales han sido identificados?
2. ¿Ha sido evaluado con precisión la magnitud del impacto para cada alternativa evaluada?
3. ¿Han sido consideradas todas las partes interesadas?
4. ¿Se han incluido los riesgos específicamente relacionados a cada alternativa?

Sección 8

8.Evaluación de Riesgos del Proyecto

El propósito de la sección de Evaluación de Riesgos del Proyecto:

La razón para escribir la sección de Evaluación de Riesgos del Proyecto es proporcionar al lector el entendimiento de los riesgos que son relativos al proyecto y como estos riesgos pueden variar por la viabilidad de la alternativa Esta sección incluye una estrategia de mitigación de riesgos, para cada riesgo.

Los Riesgos de un Proyecto y cada Alternativa Viable (No incluye el estado actual de las cosas/ Status Quo)

Descripción:

Identificar todos los riesgos que puedan relacionarse con el proyecto. Un riesgo es un factor o evento que puede poner en peligro el alcanzar los beneficios previstos o aumentar el costo del proyecto.

Ejemplos de Riesgos del proyecto son:

- Falta de Apoyo de la Gerencia Administrativa
- Cambios en la legislación
- Capacitación insuficiente
- Comunicación inadecuada
- Los conflictos de prioridades
- Incapacidad para desbloquear recursos críticos del negocio

Para cada riesgo del proyecto, identificar la probabilidad de que el riesgo se materialice y el impacto que este puede tener en cada alternativa, utilizando la siguientes directrices:

Probabilidad de Riesgo

Alto indica que el evento es altamente probable que ocurra
Medio indica que el evento es probable que ocurra
Bajo indica que el evento no es probable que ocurra

Impacto del Riesgo

Alto indica que el evento tiene un impacto significativo para el proyecto
Medio indica que el evento impactará el proyecto
Bajo indica que el impacto es relativamente menor en el proyecto
Ninguno indica que el riesgo no impactara al proyecto

Si es necesario documente la justificación de la evaluación

Evaluación de Riesgos del Proyecto	**Alternativa Viable 1**		**Alternativa Viable 2**		**Alternativa Viable 3**	
	Probabilidad	Impacto	Probabilidad	Impacto	Probabilidad	Impacto
Riesgo 1 –una descripción del riesgo 1	Alto	Medio	Bajo	Bajo	Medio	Bajo
Riesgo 1 Estrategia General de Mitigación	*Estrategia Especifica*		*Estrategia Especifica*		*Estrategia Especifica*	
…						
Riesgo 2 –una descripción del riesgo 2	Bajo	Medio	Medio	Bajo	Medio	Medio
Riesgo 2 Estrategia General de Mitigación	*Estrategia Especifica*		*Estrategia Especifica*		*Estrategia Especifica*	
…						

Riesgo de No Proceder con el Proyecto (Status Quo)

Evaluación de Riesgos del Proyecto	Status Quo (estado actual)	
	Probabilidad	Impacto
Riesgo 1 –una descripción del riesgo 1	Alto	Medio
Riesgo 1 Estrategia General de Mitigación	*Estrategia Especifica*	
…		
Riesgo 2 –una descripción del riesgo 2	Bajo	Medio
Riesgo 2 Estrategia General de Mitigación	*Estrategia Especifica*	
…		

Lista de Revisión para la Evaluación de Riegos del Proyecto

1. ¿Han sido identificados todos los riesgos generales del proyecto?
2. ¿Han sido identificados todos los riesgos específicos para cada alternativa?
3. ¿Se han tomado en cuenta, cuando se evaluaron la probabilidad y el impacto, los riesgos específicos de cada alternativa?
4. ¿La estrategia de mitigación ha sido identificada para niveles de riesgo no aceptables?
5. ¿Han sido identificados los riegos relativos al estado actual de las cosas/ Status Quo?

Sección 9

9. Análisis Costo/Beneficio

Propósito de la sección de Análisis Costo/Beneficio:

La razón para escribir una sección de Análisis Costo/Beneficio es proporcionar al lector las alternativas viables asociadas con su respectiva evaluación de costos y beneficios. El lector puede fácilmente entender y comparar los gastos iniciales y permanentes de los beneficios financieros y no financieros esperados, para cada alternativa viable.

Análisis Cuantitativo – Beneficio y Costo Financiero:

Descripción:

Análisis Completo de los Costos
Siempre que sea posible todos los costos y beneficios esperados como resultado de esta oportunidad deben ser analizados para cada alternativa viable (incluyendo los costos y beneficios del status quo) Esta metodología proporciona al lector la perspectiva total de los costos y es mucho más informativo que un enfoque incremental. Cualquier hoja de trabajo detallada debe ser adjuntada como anexo.

Análisis de Costo Incremental
Si no es posible o práctico para analizar plenamente la totalidad de los costos o cuando el incremento de los costos de los proyectos, son relativamente pequeños a la totalidad de los mismos, se puede utilizar un enfoque incremental. Esta metodología implica la identificación de los cambios o diferencias entre cada alternativa, utilizando las proyecciones de los costos / beneficios de la situación actual como una base alternativa.

Periodos de Tiempo:

Identificar los periodos de tiempo apropiados en el proyecto a través de los costos y beneficios analizados. Los periodos de Tiempo deben ser apropiados para el ciclo de vida del proyecto previsto, hasta incurrir en los costos para el logro de los beneficios previstos.

Costos:

Identificar todos los gastos efectuados por todos los interesados sobre los periodos de tiempo elegidos:

- Costos Directos
- Costos Indirectos
- Costos Iniciales
- Costos Permanentes
- Los costos del Capital

Debería Considerarse la posibilidad de:

- ¿Cuando se incurrirá en gastos?
- ¿Quién va a incurrir en los costos?
- Certeza de los costos.

Beneficios:

Identificar todos los beneficios cuantificables relacionados con todos los interesados, durante el plazo de tiempo del proyecto elegido.

Debería considerarse la posibilidad de:

- ¿Cuando se lograrán los beneficios?
- ¿Quién va a ser el ser el destinatario de los beneficios?
- Certeza de los beneficios

Un ejemplo de un formato de Resumen de Costo Beneficio:

Resumen Cuantitativo de Costo/Beneficio	**Alternativa Viable 1**	**Alternativa Viable 2**	**Alternativa Viable 3**
Valor Presente del Total de Beneficios:	**$**	**$**	**$**
Valor Presente de los Costos Totales:	**$**	**$**	**$**
Valor Neto Actual del Proyecto	**$**	**$**	**$**

Ejemplo de un Formato de Calculo de los Costos para cada alternativa viable:

Análisis Cuantitativo - Alternativa Viable 1	**Año 0**	**Año 1**	**Año 2**	**Año 3**	**Año 4**	**Año 5**
Beneficios:						
Ingresos	$	$	$	$	$	$
Costos:						
Análisis	$	$	$	$	$	$
Diseño	$	$	$	$	$	$
Implementación	$	$	$	$	$	$
Gastos Operacionales en curso:						
Recursos Humanos	$	$	$	$	$	$
Administración	$	$	$	$	$	$
Beneficios Netos o Costo de la Alternativa Viable 1	**$**	**$**	**$**	**$**	**$**	**$**
Valor Actual Neto (xx% Tasa de Descuento)	**$**					

Análisis:

Un calculo “Valor Actual Neto” es utilizado para tener en cuenta el hecho de que $ 1 de hoy no es el mismo que el valor de $ 1 cinco años a partir de ahora, debido a la inflación y los tipos de interés. El uso de un cálculo de “Valor Actual Neto” debería utilizarse para tomar en cuenta el valor temporal del dinero, independientemente de que enfoque se utiliza para la totalidad o los gastos adicionales.

Si hay algunas hipótesis que tienen un impacto significativo en el costo o beneficio, un análisis de sensibilidad se debe presentar. Contingencia a subsidios de tipos de interés o las primas que deben utilizarse para tener en cuenta las diferencias entre la certeza / riesgo. El análisis de costo / beneficio debe ser revisado para racionalizar a través de la utilización de puntos de referencia, la experiencia de otra organización, datos de la industria, etc. Esto incluiría el uso de una comparación del sector público para la asociación público-privada de proyectos.

Análisis Cuantitativo - No Financieros; Beneficios y Costos:

Algunos de los costos y los beneficios pueden no ser cuantificables (difícil atribuir un valor en dólares, pesos, etc.). Por ejemplo Beneficios no cuantificables pueden ser: mayor satisfacción del cliente o el aumento de la moral del personal. Costos no cuantificables pueden ser: la reducción de la imagen corporativa o la percepción pública adversa. Cuando sea razonable, estos deben traducirse en beneficios cuantificables es decir. Aumento de la moral del personal, pueden dar lugar a una alta productividad, lo que puede conducir a una disminución considerable en tiempo. Sin embargo, los costos y beneficios no cuantificables que no pueden ser traducidos costos / beneficios cuantificables deben resumirse de la siguiente manera:

Alternativa Viable 1

Resumen Cuantitativo	**Descripción**	**Parte(s) Interesada (s) Impactada(s)**
Beneficios:		
Beneficio 1	Descripción del Beneficio 1	
Beneficio 2	Descripción del Beneficio 2	
Costos:		
Costo 1	Descripción del Costo 1	
Costo 2	Descripción del Costo 2	

Supuestos

Todas las hipótesis utilizadas para determinar costos tanto cuantitativos como cualitativos y los beneficios deben ser claramente documentados. Esto incluiría las premisas generales, así como supuestos específicos de cada alternativa.

Lista de Revisión para la sección de Análisis de Costo/Beneficio

1. ¿Han sido identificados todos los costos cualitativos y los beneficios?
2. ¿Han sido identificados todos los costos cualitativos y los beneficios?
3. ¿Es apropiado el periodo de tiempo considerando, la expectativa de vida prevista del proyecto?
4. ¿Puede alguno de los elementos no financieros convertirse en elemento financiero?
5. ¿Todos los supuestos son claramente identificados?
6. ¿Tienen todas las premisas comunes / generales que se aplican de manera coherente a cada alternativa?
7. ¿Han sido revisados los supuestos para identificar la sensibilidad de su estimación sobre el impacto de los resultados?
8. ¿Se tienen puntos de referencia, la experiencia de otras organizaciones, datos de la industria que hayan sido utilizados para validar los costos y los beneficios?

Sección 10

10. Conclusiones y Recomendaciones

Propósito de la Sección de Conclusiones y Recomendaciones:

La razón para escribir la sección de Conclusiones y Recomendaciones es para proporcionar al lector en la alternativa seleccionada, basada en una evaluación global de las alternativas, la información en términos de impacto riesgo y costo/beneficio. Se presentan también las recomendaciones específicas para avanzar en el proyecto.

Conclusiones

Descripción:

En esta sección se recapitularan cada una de las alternativas basadas en su impacto Operacional y al Negocio, Evaluación de Riesgos del Proyecto y el Análisis Costo/Beneficio. Basado en estos resultados, una conclusión sobre cualquier alternativa o variante que sea elegida o hecha.

Alternativa	Impacto Operacional y al Negocio	Evaluación de Riesgos del Proyecto	Análisis Costo/Beneficio
Alternativa 1	Describe la evaluación global	Describe la evaluación global	Describe la evaluación global
Alternativa 2	Describe la evaluación global	Describe la evaluación global	Describe la evaluación global
Alternativa 3	Describe la evaluación global	Describe la evaluación global	Describe la evaluación global

Elegir las alternativas recomendadas basado en la recapitulación, seleccionando la alternativa que maximice la eficacia y eficiencia mientras minimice el riesgo y los costos.

Recomendaciones

Descripción:

Esta sección hará recomendaciones específicas sobre si seguir adelante con el proyecto.

El alcance de la recomendación puede ir desde la recomendación de aprobación para la plena implementación de los proyectos a la recomendación mas detallada en un análisis de los requisitos para validar algunos de los principales componentes de negocio.

Responsabilidad del Proyecto

Descripción:

Recomendar quienes deben Administrar el Proyecto y como tal, responsabilizar en la implementación y administración de éste. Ésta Sección deberá incluir cualquier aspecto administrativo adicional relacionado a los proyectos administrativos.

Rendición de Cuentas del Proyecto

Descripción:

Recomendar quien debe ser el patrocinador del Proyecto y, como tal, tiene la responsabilidad general de garantizar que el proyecto se termine. Esta sección incluiría todos los aspectos de la gobernabilidad adicionales vinculados a los proyectos Administrativos.

Sección 11

11. Estrategia de Implementación

Propósito de la sección de la Estrategia de Implementación:

La razón para escribir una sección de Estrategia de Implementación y una sección de Recomendaciones es asegurar que estos aprueban el caso de negocio entendiendo los recursos que se deben asignar (personas, tiempo y dinero) para completar los siguientes pasos recomendados para el proyecto.

Descripción:

El esbozo propuesto del plan de implementación para los siguientes pasos recomendados en un nivel alto. Debe estar previsto de suficiente detalle a fin de que se apruebe el caso de negocio entendiendo los recursos que se deben asignar (personas, dinero, tiempo) para completar los siguientes pasos recomendados para el proyecto.

Esta sección debe incluir:

- Las principales fases del proyecto
- Alto nivel del plan de trabajo, entregables y fechas objetivo previstas
- Costos ($) requeridos para llevar acabo el plan de implementación
- Personal requerido (departamentos, roles)
- Estructura propuesta del proyecto
- Asignación de responsabilidades para implementación y monitoreo las estrategias de mitigación de riesgo (Sección 8).

Sección 12

12. Revisión y Aprobación de Procesos

Propósito de la Sección de Revisión y Aprobación de Procesos:

La Razón de escribir una sección de Revisión y aprobación de Procesos es para presentar claramente al lector con quien y como ha sido revisado y aprobado el caso de negocio. Esta sección también contendrá los resultados finales del caso de negocio. Si el caso de negocio no es aprobado, la decisión del negocio de tras de cualquier rechazo del proyecto o diferencia en este debe ser documentada.

Revisión de Procesos

Descripción:

Quienes revisarán el caso de Negocio

Aprobación de Procesos

Descripción:

Cual es el proceso aprobado y quien esta involucrado

Caso de Negocio Signoff

Descripción:

El caso de negocios debe ser firmado y fechado por la(s) persona(s) que dieron su aprobación, indicando si efectivamente el caso de negocio es aprobado. Si procede, las condiciones de aprobación deben ser identificadas. Si el caso de negocio no es aprobado, las razones para esta decisión deben ser documentadas.

Bibliografía

Martinez Evelio. "**Conmutación de circuitos y paquetes"**. Disponible en: http://www.eveliux.com/telecom/cpswitching.html Leído el 25 Julio 2007.

Hernández Carlos Alejandro. Universidad Iberoamericana Campus Cuidad de México. **"Metodología ITIL. El objetivo de usar ITIL en la Administración de Servicios"**. Disponible en: http://www.monografias.com/trabajos31/metodologia-itil/metodologia-itil.shtml Leído el 15 Agosto 2007.

Green Christopher D. York University, Toronto,Ontario. **"Classics in the History of Psychology. CONDITIONED EMOTIONAL REACTIONS"** By John B. Watson and Rosalie Rayner(1920) First published in Journal of Experimental Psychology, 3(1), 1-14. Disponible en: http://psychclassics.yorku.ca/Watson/emotion.htm Leído el 17 Agosto 2007.

Wikipedia La Enciclopedía libre. **"Ivan Pavlov"**. Disponible en: http://es.wikipedia.org/wiki/Ivan_Pavlov Leído el 19 Agosto 2007.

Wikipedia La Enciclopedía libre. **"Condicionamiento clásico"**. Disponible en: http://es.wikipedia.org/wiki/Condicionamiento_cl%C3%A1sico Leído el 19 Agosto 2007.

Wikipedia La Enciclopedía libre. **"Psicología conductista"**. Disponible en: http://es.wikipedia.org/wiki/Psicolog%C3%ADa_conductista Leído el 20 Agosto 2007.

Wikipedia La Enciclopedía libre. **"Pequeño Albert"** Disponible en: http://es.wikipedia.org/wiki/Peque%C3%B1o_Albert Leído el 20 Agosto 2007.

L.I. Genny E. Góngora Cuevas, M.A. **"Tecnología de la información como herramienta para aumentar la productividad de una empresa ¿Qué es la Técnología de la información?"** Disponible en: http://www.tuobra.unam.mx/publicadas/040702105342.html Leído el 25 Agosto 2007.

Wikipedia La Enciclopedía libre. **"Información"**. Disponible en: http://es.wikipedia.org/wiki/Inform%C3%A1tica Leído el 25 Agosto 2007.

Ruiz Antón J. Carlos. Depto. de Traducción y Comunicación, Universitat Jaume. **"Lingüística Teórica y Aplicada (k37) Capítulo 11 de Bernárdez ("Lenguaje y cerebro") Un gen que afecta específicamente al lenguaje"**. Disponible en: http://www3.uji.es/~ruiz/k37/k37-5.pdf Leído el 25 Agosto 2007.

Tortosa Gil, F. (1998) **"Una historia de la psicología moderna"**. Madrid: McGrawHill Varela, F., Thompson, E., Rosch, E. (1992) De cuerpo presente. Las ciencias cognitivas y la experiencia humana. Barcelona: Gedisa.

Wikipedia La Enciclopedía libre. **"Corteza Cerebral"**. Disponible en: http://es.wikipedia.org/wiki/Corteza_cerebral Leído el 30 Agosto 2007.

Passig Villanueva. "**Los Sistemas de memoria"**. Revista de Psicología – Vol. V Años 1994-1995, p.27. Depto. Fisiología y Biofísica, Facultad de Medicina, Universidad de Chile. Disponible en: http://csociales.uchile.cl/publicaciones/psicologia/docs/Los_sistemas_de_memoria.pdf Leido el 30 Agosto 2007.

Belmar Jorge. **"Estructura Desarrollo y Funciones del Sistema Nervioso"**. Organización y Estructura. Facultad de Ciencias Biológicas. Pontíficia Universidad Católica de Chile. Disponible en: http://www.puc.cl/sw_educ/neurociencias/ Leído el 30 Agosto 2007.

M. Reichart, **"Psiquiatría general y especial"**, Madrid 1958; A. M. FREEDMAN, Narcotics addicts in New York: characteristics and management, en Excepta Medica, IV Congreso Mundial de A. C. *Pacheco E Silva*,**"Psiquiatría"**, Amsterdam 1966; Dintoxication chronique en Amérique Latine, en Actas del IV Congreso Internacional de Psiquiatría, Madrid 1966; D. WANDREY y V. LEUTNER, Los neuropsicofármacos en la clínica y en la práctica, Madrid 1967. Ediciones Rlalp S.A. Enciclopedia GER. Canal Social Noticias. Alucinaciones. Disponible en: http://www.canalsocial.net/GER/ficha_GER.asp?id=9612&cat=medicina Leído el 30 Agosto 2007.

Airala et al. Instituto Argentino de Normalización. **"Esquema 1 de Norma IRAM-ISO IEC 17799. Tecnología de la Información. Código de práctica para la administración de la seguridad de la Información"**. Año 2002.

Encyclopedia of Mental Disorders :: Py-Z. **"Rorschach technique"**.Disponible en: http://www.minddisorders.com/Py-Z/Rorschach-technique.html Leído el 31 Agosto 2007.

Wikipedia La Enciclopedía libre. **"Esteganografía"**. Disponible en: http://es.wikipedia.org/wiki/Esteganograf%C3%ADa Leído el 4 septiembre 2007.

Hernández Leobardo y E. Daltabuit 2006. *"Diplomado de Tecnologías de Información"*, Centro Educativo Multidisciplinario Polanco, México, D.F 30 Junio-14 Julio 2006. En el módulo 4: Seguridad Informática, Centro Educativo Multidisciplinario Polanco, México, D.F.

Villalón Huerta Antonio.Seguridad en UNIX y en Redes. **"Esteganografía"**. 2002. Disponible en: http://es.tldp.org/Manuales-LuCAS/SEGUNIX/unixsec-2.1-html/node320.html Leído el 4 Septiembre 2007.

VSantivirus No. 787 - Año 6 - Martes 3 de setiembre de 2002. **"Orígenes de la esteganografía"**. Disponible en: http://www.vsantivirus.com/esteganografia.htm Leído el 4 Septiembre 2007.

Charles P. Pfleeger, Shari Lawrence Pfleeger. **"Security in Computing"**. Third Edition Printed in the United States of America Pub. December 02, 2002. Prentice Hall.

Wikipedia La Enciclopedía libre. **"Sistema informático"**. Disponible en: http://es.wikipedia.org/wiki/Sistema_inform%C3%A1tico Leído el 6 Septiembre 2007.

*Solano Ronald.***"Teoría de Sistemas. Características de los sistemas"**. Disponible en: http://www.monografias.com/trabajos11/teosis/teosis.shtml Leído el 7 Septiembre 2007.

Wikipedia La Enciclopedía libre. **"Teoría de Sistemas. Entropía y neguentropía"**. Disponible en: http://es.wikipedia.org/wiki/Teor%C3%ADa_de_sistemas Leído el 31 Agosto 2007.

Martínez Bustamante Sandra. **"La termodinámica y el concepto de entropía"**. Monografías.com Disponible en: http://www.monografias.com/trabajos/termoyentropia/termoyentropia.shtml?interlink Leído el 7 Septiembre 2007.

Guyton Pamela. " **Bussines Service Management. Introduction to Business Service Management == Business Service Management (BSM) is a goal for businesses, and a promise from potential providers. A good BSM"** .The 6 April 2007. Wikipedia the free Encyclopedia. Disponible en: http://en.wikipedia.org/wiki/Business_Service_Management Leído el 27 Septiembre 2007

Wikipedia the free Encyclopedia.**" Information Technology Infraestructure Library"**. Disponible en: http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library Leído el 27 Septiembre 2007.

Steven Weil. **"How ITIL Can Improve Information Security. Security Focus"** December 22, 2004. Disponible en: http://www.securityfocus.com/infocus/1815 Leído el 12 Agosto 2007.

Johnson D. et al **"Capacity Management"** From Wikipedia, the free encyclopedia. Disponible en: http://en.wikipedia.org/wiki/Capacity_management Leído el 8 Octubre 2007.

Supremo Tribunal de Justicia del Estado de Sinaloa. **"Delitos Informáticos"** Disponible en: http://www.stj-sin.gob.mx/Delitos_Informaticos2.htm Leído el 16 Octubre 2007. Lázaro Cárdenas y 16 de septiembre. Unidad Administrativa Edificio "B", Col. Centro, Culiacán, Sinaloa, México.

Alison Et al. **"Cyberstalking".** From Wikipedia, the free Encyclopedia. Disponible en: http://en.wikipedia.org/wiki/Cyberstalking Leído el 16 de Octubre 2007.

Wayne Petherick **" CYBER-STALKING: OBSESSIONAL PURSUIT AND THE DIGITAL CRIMINAL"** Disponible en: http://www.crimelibrary.com/criminology/cyberstalking/ Leído el 16 de Octubre 2007.

Farmbrough Rich Et al. **"Information warfare"** from Wikipedia, the free encyclopedia Disponible en: http://en.wikipedia.org/wiki/Information_warfare Leído el 16 Octubre 2007.

International Standard ISO 7498-2 First Edition 1989-02-15 **"Information processing systems- Open systems Interconnection- Basic Reference Model- Part 2: Securyty Architecture".**

Grance Tim et al. **"NIST National Institute of Standards and Technology. Technology Administration U.S. Departament of Commerce. Guide to Information Technology Security Services. Recommendation of the National Institute of Standards and Technology. Special Publication 800-35".** Computer Security Division. Information Technology Laboratory. National Institute of Standards and Technology. Gaithersburg, MD 20899-8930. October 2003.

Villalon Huerta Antonio.**"Gestión de la seguridad de la información: UNE 71502, ISO 17799"**. Junio 2004. Universidad de Verano Campus TI Ciencia y Tecnología & S2 grupo. Vilanópo Valencia España.

Philip L. Campbell, Jason E. Stamp. **"A Classification Scheme for Risk Assessment Methods. SANDIA REPORT SAND2004-4233"** Unlimited Release. Printed August 2004. Sandia National Laboratories Albuquerque, New Mexico 87185 and Livermore, California.

Chou Sean. **"Beyond Procedurement: Use Technology to Manage the Complete Service Life Cycle March 2004. Management Contract** ". Disponible en: http://www.fieldglass.com/news/pdf/2004/3-04_BeyondProcurement.pdf Leído el 17 Septimebre 2007.

Marian Swanson et al. " **NIST National Institute of Standards and Technology. Technology Administration U.S. Departament of Commerce.Contingency planning Guide for Information Technology Systems. Recommendation of the National Institute of Standards and Technology. Special Publication 800-34"**. Government Printing Office Internet: bookstore.gpo.gov Washington, DC 20402-0001. June 2002.

Marian Swanson. **"Guide for Developing Security Plans for Information Technology Systems NIST Special Publication 800-18"**.National Institute of Standards and Technology. December 1998.