TRABAJO ESPECIAL DE GRADO

DISEÑO DE UN MODELO DE GESTIÓN DE RIESGO OPERACIONAL PARA LA IMPLEMENTACIÓN DEL SERVICIO IPTV EN CANTV

Ing. Palma Duque, Mary Dayana

Trabajo presentado ante la Ilustre
Universidad Central de Venezuela
para optar al Título de Especialista
en Telecomunicaciones Digitales

Caracas, 2012

TRABAJO ESPECIAL DE GRADO

DISEÑO DE UN MODELO DE GESTIÓN DE RIESGO OPERACIONAL PARA LA IMPLEMENTACIÓN DEL SERVICIO IPTV EN CANTV

Profesor Guía: Ing. Zeldivar Bruzual

Ing. Palma Duque, Mary Dayana

Trabajo presentado ante la Ilustre Universidad Central de Venezuela para optar al Título de Especialista en Telecomunicaciones Digitales

Caracas, 2012

CARTA DE APROBACIÓN

Caracas, 2012

Los abajo firmantes, miembros del Jurado designado por el Consejo de Escuela de Ingeniería Eléctrica, para evaluar el Trabajo Especial de Grado presentado por la Ing. Palma D., Mary D., titulado:

"DISEÑO DE UN MODELO DE GESTIÓN DE RIESGO OPERACIONAL PARA LA IMPLEMENTACIÓN DEL SERVICIO IPTV EN CANTV"

Consideran que el mismo cumple con los requisitos exigidos por el plan de estudios conducente al Título de Especialista en Telecomunicaciones Digitales, y sin que ello signifique que se hacen solidarios con las ideas expuestas por el autor, lo declaran APROBADO.

_____	_____
Prof. Neudith Morales	Prof. Ebert Brea
Jurado	Jurado

_____

Ing. Zeldivar Bruzual

Profesor Guía

DEDICATORIA

Quiero dedicar este trabajo a Dios por iluminar mi camino
A mis padres Gerardo y Mary Luz por apoyarme siempre
A mis hermanas Yermari y María Laura por su cariño
A José Angel por su compañía y por cuidarme siempre
Gracias a ustedes

AGRADECIMIENTOS

Con inmensa gratitud quiero expresar mis agradecimientos:

A mis padres, mis hermanas y a José Angel, por ser mi apoyo y mi motivación para alcanzar esta nueva meta

A mi profesor guía el Ing. Zeldivar Bruzual por brindarme su ayuda para la elaboración de este trabajo

A mis amigas Hilda y Mairina por su amistad, apoyo y ayuda siempre que la necesito.

A la Universidad Central de Venezuela por permitirme ser parte de esta casa de estudios y por los conocimientos adquiridos.

Palma Duque, Mary Dayana

DISEÑO DE UN MODELO DE GESTIÓN DE RIESGO OPERACIONAL PARA LA IMPLEMENTACIÓN DEL SERVICIO IPTV EN CANTV

Profesor Guía: Ing. Zeldivar Bruzual. Tesis. Caracas. U.C.V. Facultad de Ingeniería. Escuela de Ingeniería Eléctrica. Especialista en Telecomunicaciones Digitales. Institución: CANTV. 2011. 167 páginas, más anexos.

Palabras Claves: IPTV, ADSL, Riesgo, Calidad de Servicio.

Resumen. CANTV ha impulsado la implementación del servicio IPTV, el cual estará soportado en la tecnología de acceso ADSL e integrado a la actual red de acceso y transporte IP de la empresa, para lo cual debe asegurar la calidad de este nuevo servicio y el menor impacto sobre los ya soportados. Por ello surgió la necesidad de generar una estrategia integral de identificación de riesgo operacional, que permitiera identificar, analizar, evaluar y generar los planes de acción para la mitigación de estos eventos, y así garantizar la prestación del servicio con una plataforma robusta, integrada con la red de CANTV y de alta calidad. El trabajo se desarrolló en tres fases: 1.) Revisión teórica, donde se recopiló información referente al funcionamiento de la Plataforma IPTV a instalar en CANTV y se realizó la investigación de los estándares para la administración de riesgo; 2.) Identificación, análisis y cuantificación de los riesgos operacionales asociados a la implementación del servicio IPTV en CANTV, basado en la metodología del estándar ISO 31000; 3.) Diseño del mapa operacional, para el cual se utilizó la herramienta de Administración de Riesgos ERA adquirida por la Gerencia de Seguridad de la Operación de CANTV.

INDICE GENERAL

LISTA DE FIGURAS

LISTA DE TABLAS

LISTAS DE ACRÓNIMOS

ADSL: Asymmetric Digital Subscriber Line

ATA: Adaptador Telefónico Analógico (Analog Telephone Adapter)

CAS: Sistema de Acceso Condicional (Conditional Access System).

Core: Centro de Operaciones de la Red.

CPE: Customer Premise Equipment

cPVR: Grabador personal de video basado en el CPE. Ver también nPVR, PVR.

DCN: Red de gestión y monitoreo.

DRM: Digital Rights Management. Gestión de Derechos de Autor.

DSL: Digital Subscriber Line

EPG: Guía de Programación Electrónica.

HGW: Módem ADSLx.

IGMP: Internet Group Management Protocol

IETF: Internet Engineering Task Force

IGMP: Internet Group Management Protocol

IP: Internet Protocol

IPTV: Internet Protocol Tele-Vision

ITU-T: International Telecommunication Union – Telecommunication Standardization Sector

LAN: Red de área local.

MPEG: Motion Picture Experts Group

NOC: Centro de Operaciones de la Red.

nPVR: PVR basado en red.

PIM: Protocol Independent Multicast

PIM-SM: PIM-Sparse Mode

PIM-DM: Dense Mode

PIP: Picture In Picture

PLTV: Pause Live TV.

PVR: Grabador Personal de Video.

QoE: Calidad de la Experiencia (Quality of Experience).

QoS: Calidad de Servicio (Quality of Service).

SDTV: TV de definición estándar.

STB: Decodificador de IPTV (Set-Top Box).

Trick-play: Opciones de Pausa, Reanudación, Cámara Lenta, Adelantado Rápido (FF), Retroceso Rápido (RW), etc. sobre un contenido.

TSTV: Time-shifted TV

VoD Real: Servicio de VoD que ofrece al usuario “trick-play”.

VoD: Video bajo demanda.

WAN: Red de área extendida.

Zapping Time: Tiempo transcurrido desde el momento en que el usuario confirma un cambio de canal, hasta que la señal de video es desplegada en el TV.

INTRODUCCIÓN

La Compañía Anónima Nacional Teléfonos de Venezuela (CANTV), provee a sus clientes el servicio de internet de alta velocidad, haciendo uso de la tecnología de acceso ADSL (Asymmetric Digital Subscriber Line), la cual permite la transmisión de datos y el funcionamiento del servicio voz de manera simultánea, a través del mismo par de cobre de acceso telefónico. Por medio de este tipo de tecnología se pueden obtener velocidades de transmisión de datos de hasta 8 Mbps en dirección hacia el cliente (downstream), para accesos donde la distancia máxima entre el usuario final y la central telefónica no supere los 5 Km.

Considerando la posibilidad de ofrecer servicios convergentes (voz, video y datos) a altas velocidades, utilizando una sola infraestructura de red de datos o IP (Internet Protocol), CANTV ha impulsado la implementación del servicio IPTV (Internet Protocol Televisión), el cual estará soportado en la tecnología de acceso ADSL e integrado a la actual red de acceso y transporte IP de la empresa, así como a los diferentes sistemas que soportan todos los procesos relacionados con el servicio: aprovisionamiento, instalación, facturación y cobro (OSS/BSS Operations Support Systems/Business Support Systems).

El servicio de televisión por suscripción provisto por CANTV, se ofrecerá cumpliendo los estándares de calidad, con una variedad de planes de canales básicos (broadcast TV), canales Premium, canales a la carta, video bajo demanda, guía interactiva de programación, grabación personal de video, servicios de música digital, radio local e internacional.

En este sentido, la empresa contempla dentro de su mapa de objetivos estratégicos del año 2010-2015, integrar el aseguramiento de la calidad de

sus servicios, para satisfacer los requerimientos y demandas de telecomunicaciones en las comunidades venezolanas, haciéndose indispensable la atención y gestión de los posibles eventos que pudiesen afectar la calidad operacional en el otorgamiento del servicio de televisión por suscripción a través de la plataforma IPTV; por lo cual surge la necesidad de generar una estrategia integral de identificación de riesgo operacional, que permitirá identificar, analizar, evaluar y generar los planes de acción para la mitigación de riesgos, y de esta manera garantizar la prestación del servicio con una plataforma robusta, integrada con la red de CANTV y con una alta calidad.

Por lo antes mencionado y con el fin de proveer un nuevo servicio con altos estándares de calidad, se hace imprescindible el diseño de un modelo de riesgo operacional, que permita evaluar y gestionar aquellos eventos negativos tanto internos como externos, que puedan afectar o impedir el logro de los objetivos institucionales, así como también, la tipificación de los eventos positivos que coadyuve a identificar las oportunidades para un mejor desempeño del servicio, proporcionando de manera lógica y sistemática el establecimiento y la implantación de procesos para la administración del riesgo operacional.

La estructura de este trabajo se encuentra dividida en cinco capítulos, cada uno de los cuales contienen los siguientes puntos:

Capítulo I: Definición del Problema.

Se plantea, justifica y delimita el problema tratado en este trabajo, se definen el objetivo general, objetivos específicos y el desarrollo de la metodología empleada.

Capítulo II: Marco Teórico

Se definen y desglosan todos aquellos conceptos teóricos requeridos para el desarrollo del trabajo: funcionamiento del servicio IPTV, estándares para el diseño de sistemas IPTV, protocolos y tecnologías utilizadas para el despliegue de este servicio, arquitectura y funcionamiento de la plataforma IPTV implementada en CANTV, integración de este tipo de servicio sobre las redes de acceso, transporte y trocal IP de la empresa.

Capítulo III: Estándares de Administración Riesgo

Se describen los estándares de administración de riesgos aplicados en el ámbito de las telecomunicaciones, así como aquellas metodologías empleadas que permitan cumplir con la definición, análisis, evaluación y tratamiento de todos los riesgos operacionales asociados con la implementación de la plataforma IPTV en CANTV.

Capítulo IV: Metodología de Análisis de Riesgo Operacional

En este Capítulo se enumeran los eventos potenciales que colocan en riesgo la calidad operacional del servicio IPTV, a través de la definición de los agentes generadores, las causas y los efectos de su ocurrencia. Por otro lado, se analizan, cuantifican y definen los riesgos operacionales, en cuyo proceso son establecidos las probabilidades de su existencia y el impacto de sus consecuencias, con el fin de obtener información para establecer el nivel de riesgo y los planes de acción, que se implementaran en el mapa operacional a desarrollar, todo ello según los métodos evaluados en Capítulo III.

Capitulo V: Mapa Operacional de Riesgos

La propuesta y enfoque de este trabajo se presenta en el Capítulo V, con la

elaboración del mapa operacional de riesgos para la implementación del servicio IPTV en CANTV, en función del análisis realizado en el Capítulo IV.

Por último se presentarán las conclusiones y recomendaciones producto de la investigación realizada, la bibliografía consultada y los anexos que corresponden.

CAPITULO I

DEFINICION DEL PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

La Compañía Anónima Nacional Teléfonos de Venezuela CANTV, es el proveedor principal de servicios de telecomunicaciones en el país, y tiene como objetivo la administración, desarrollo y establecimiento de redes fijas y móviles para la prestación de servicios, entre los cuales destacan: la telefonía fija local y de larga distancia nacional e internacional, telefonía móvil, internet, y próximamente servicios de difusión por suscripción usando conexiones de banda ancha sobre protocolo IP (Internet Protocol), como lo es IPTV (Internet Protocol Televisión).

IPTV, es un servicio que viene a posicionarse dentro del portafolio de productos de CANTV, con la finalidad de ofrecer a sus clientes un mecanismo alternativo de distribución de video, que incluye contenidos almacenados, programación en directo y video bajo demanda, sumando de esta manera un nuevo servicio de video a sus ofertas de voz y acceso a internet disponibles actualmente. Todo ello, enmarcado dentro de los objetivos estratégicos de la empresa, en cuanto a ser líder en calidad del servicio, portafolio de productos y atención al usuario actual y potencial.

Así mismo, dentro de CANTV en la Gerencia de Seguridad de la Operación adscrita a la Gerencia General de Seguridad Integral, se llevan a cabo funciones como el aseguramiento de la calidad para las plataformas operativas Telco y Móvil, para lo cual se requiere establecer planes de riesgo operacional diseñados con indicadores y estrategias de acción, que permitan cuantificar y mitigar las brechas y vulnerabilidades identificadas, las cuales impactaran la disponibilidad de los servicios provistos por CANTV.

En este sentido, se planteó dentro de la Gerencia de Seguridad de la Operación como parte estratégica del Plan Operativo Anual, el establecimiento de los procesos para la administración de riesgo operacional enmarcado dentro de las recomendaciones y estándares internacionales existentes, a fin de asegurar el despliegue del servicio IPTV a través de la red de CANTV, así como también, el análisis de los factores que garanticen a la empresa un mejor desempeño en la administración de este nuevo servicio.

1.2 OBJETIVOS DEL PROYECTO

1.2.1 OBJETIVO GENERAL

Diseñar un modelo de gestión de riesgo operacional para la implementación del servicio IPTV en CANTV, con el fin de asegurar la calidad en el servicio a ofrecer a los usuarios finales.

1.2.2 OBJETIVOS ESPECIFICOS

1. Analizar los parámetros básicos de televisión por suscripción a través de la plataforma IPTV.
2. Comprender el funcionamiento de la plataforma IPTV a instalar en la red de CANTV.
3. Estudiar los estándares internacionales definidos para la administración de riesgo operacional, y su aplicación para la evaluación del servicio IPTV.
4. Identificar los procesos para la administración de riesgo operacional, asociados con la implementación del servicio IPTV en CANTV.
5. Analizar y cuantificar los riesgos operacionales para la implementación del servicio IPTV en CANTV, asegurando la calidad de servicio.
6. Definir los planes de acción, para la mitigación y gestión de los riesgos operacionales en el otorgamiento del servicio IPTV.

7. Diseñar un mapa, para establecer los procesos en la administración de riesgo operacional para la implantación del servicio IPTV en CANTV.

1.3 JUSTIFICACION DEL PROYECTO

Actualmente, una de las principales funciones que se llevan a cabo en la Gerencia de Seguridad de la Operación adscrita a la Gerencia General de Seguridad Integral de CANTV, es la identificación y análisis de riesgo operacional asociado a la implementación y puesta en marcha de las distintas plataformas y servidos (Telco y Móvil) disponibles en la empresa; y así definir planes de acción que permitan realizar la mitigación y el control de las brechas y vulnerabilidades identificadas, asegurando la calidad y efectividad en la operación de la red y los servicios de telecomunicaciones provistos.

La plataforma de IPTV que se encuentra en fase de implementación, requiere de la convergencia de distintos niveles de la red de CANTV como lo son: la red troncal IP, la red de transporte y la red de acceso; así como el modelaje de los distintos procesos de operación que existen actualmente, ya que se trata del otorgamiento de un servicio totalmente nuevo para la empresa, como lo es la difusión de video por suscripción.

El diseño de un modelo de gestión de riesgo operacional para la implementación del servicio IPTV en CANTV, permitirá realizar el análisis de cada uno de los eventos internos y externos que pudieran afectar la calidad de operación y limitar el despliegue del servicio.

1.4 ALCANCE DEL PROYECTO

El presente trabajo abarca la generación del mapa de riesgo operacional asociado a la implementación del servicio IPTV en CANTV, a través de la definición del procedimiento para la administración del riesgo que

permita realizar desde la identificación hasta el seguimiento y control de cada una de las brechas y vulnerabilidades identificadas.

1.5 LIMITACIONES DE LA INVESTIGACION

La implementación de los planes de acción definidos para la mitigación de los riesgos operacionales identificados en este trabajo, estará limitado por el tiempo de pase a producción de la plataforma en CANTV, así como también a la complejidad de las soluciones que sean requeridas técnica y económicamente para la ejecución de los mismos.

1.6 METODOLOGIA EMPLEADA EN LA INVESTIGACION

1.6.1 TIPO DE INVESTIGACIÓN

El tipo de investigación aplicada al presente trabajo especial de grado se encuentra dentro de la modalidad de Proyecto Factible; según lo planteado en el Manual de Trabajo de Grado de Especialización y Maestrías y Tesis Doctorales de la UPEL del año 2006, donde se refiere a proyecto factible como: “La investigación, elaboración y desarrollo de una propuesta de un modelo operativo viable para solucionar problemas, requerimientos o necesidades de organizaciones o grupos sociales; puede referirse a la formulación de políticas, programas, tecnologías, métodos y procesos. El Proyecto debe tener apoyo en una investigación de tipo documental, de campo o un diseño que incluya ambas modalidades”. (UPEL 2010, p.21).

La propuesta planteada es de carácter factible ya que consiste en el diseño de un modelo de gestión de riesgo operacional para la implementación del servicio IPTV en CANTV. El método de investigación utilizado para su ejecución es de campo, ya que corresponde a la evaluación y análisis de eventos que pudiesen afectar la calidad operacional en el otorgamiento del servicio de televisión por suscripción a través de la

plataforma IPTV, haciendo uso de la metodología descrita en el estándar ISO 31000.

1.6.2 FASES METODOLÓGICAS

El desarrollo aplicado al presente trabajo especial de grado, correspondió a los pasos que se consideraron lógicos para cumplir con los objetivos planteados, las cuales se mencionan a continuación:

1.6.2.1 Recopilar información

El desarrollo de la primera fase se orientó hacia una extensiva consulta y análisis de los parámetros básicos de televisión por suscripción en plataformas IPTV, estudio de la arquitectura física y lógica de la solución de IPTV adquirida en CANTV, revisión de las especificaciones de los estándares internacionales de administración de riesgos y páginas web especializadas en este tipo de servicio. De la misma manera, se efectuaron entrevistas con el personal que actualmente implementa el proyecto en CANTV, las cuales permitieron comprender el funcionamiento y su interacción con la red, para la prestación del servicio de televisión por suscripción a través de la tecnología ADSL.

1.6.2.2 Identificación, análisis y cuantificación de los riesgos operacionales asociados a la implementación del servicio IPTV en CANTV.

Una vez conocida toda la información mencionada anteriormente, se llevo a cabo la segunda fase de la investigación, donde se identificaron los eventos, las causas y los efectos de su ocurrencia que colocaban en riesgo el despliegue del servicio IPTV. Posterior a ello, se realizó el análisis y cuantificación de los riesgos operacionales, definiendo las probabilidades de

ocurrencia y su impacto, con el fin de obtener información para definir el nivel de riesgo y las acciones a implementar para su mitigación.

Las aproximaciones usadas para identificar riesgos incluyeron: listas de chequeo, juicios basados en la experiencia, tormenta de ideas y análisis del entorno.

1.6.2.3 Diseño del mapa, a fin de establecer los procesos para la administración del riesgo operacional en la implantación del servicio IPTV en CANTV.

La fase final consistió en el diseño del mapa operacional de riesgos para la implementación del servicio IPTV en CANTV, el cual fue desarrollado utilizando la herramienta ERA (Entreprise Risk Assessor), la cual permite automatizar los aspectos del enfoque de riesgo en base a: los procedimientos especificados dentro del estándar de administración de riesgos ISO 31000, la información técnica y funcional de la plataforma IPTV adquirida en CANTV, y la necesidad de asegurar la calidad en el otorgamiento de este nuevo servicio por la empresa. Todo esto, con el fin de determinar el conjunto de brechas y vulnerabilidades que deben ser mitigadas para el óptimo desempeño de este servicio integrado en la red de CANTV, así como la definición de los responsables de ejecutar los planes de acción para la acciones de mitigación establecidas y el tiempo de respuesta de los riesgos a monitorear.

1.6.3 TÉCNICA DE RECOLECCIÓN DE DATOS.

De acuerdo al método de investigación aplicado, los datos de interés fueron recogidos en forma directa de la realidad; a través de la revisión de documentos (Informes y manuales), visitas a portales web en internet y

aquellas fuentes donde se indican las normas y estándares de riesgos en el área de telecomunicaciones.

Adicionalmente, se llevaron a cabo entrevistas con el personal que actualmente implementa el proyecto de IPTV, adscritos a las Gerencias Generales de: Servicios Audiovisuales, Proyectos Mayores, Tecnología y Operaciones, Planificación y Asuntos Corporativos y Seguridad Integral.

CAPITULO II

MARCO TEORICO

2.1 TELEVISIÓN SOBRE EL PROTOCOLO DE INTERNET-IPTV

UIT Focus Group (2010). Televisión sobre el Protocolo de Internet (IPTV), está definido por la Unión Internacional de Telecomunicaciones-Grupo Focal (UIT-T Focus Group) como un conjunto de servicios multimedia tales como: televisión, vídeo, audio, texto, gráficos y datos, los cuales son transportados a través de redes basadas en protocolo de internet (IP), proporcionando los niveles requeridos de calidad de servicio (QoS), calidad de experiencia (QoE), seguridad, interactividad y fiabilidad.

En otras palabras, IPTV es contenido televisivo que en lugar de ser transmitido por cable o satélite es transmitido al espectador a través de redes IP por un proveedor de servicio, tal y como se muestra en la siguiente figura.

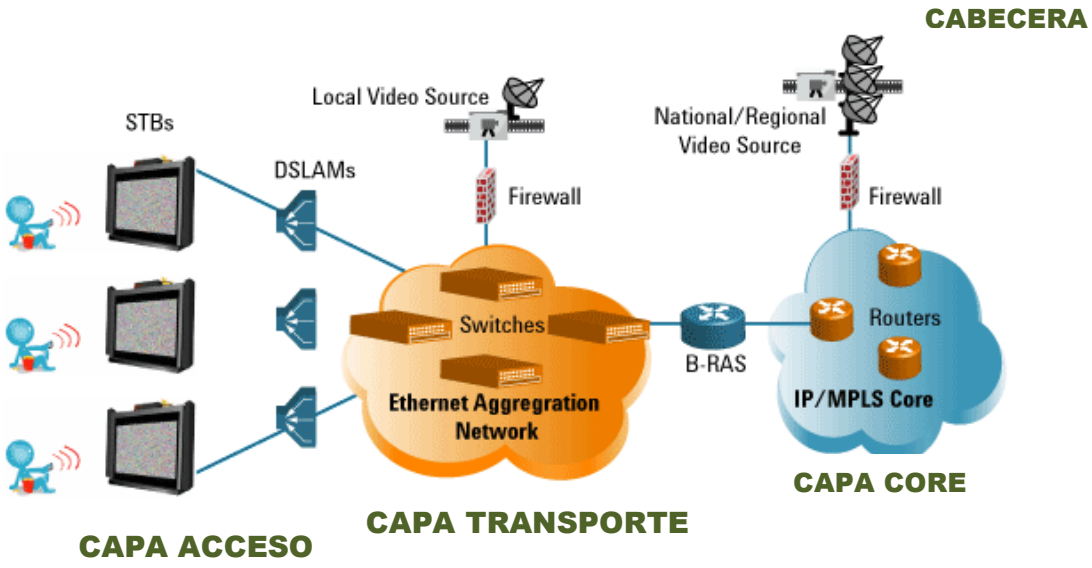


Figura 1. Arquitectura básica sistema IPTV. Fuente: TURBOTELTIC Cia. Ltda.

La característica principal que ofrecen las soluciones de IPTV, es que el transporte de la información (audio, video, datos asociados) se realiza mediante los protocolos IP sobre redes de banda ancha. El encapsulado de los contenidos de televisión se realiza sobre los protocolos RTP y UDP, utilizando para su distribución la tecnologías "multicast", mediante la cual cada canal de televisión se transmite una sola vez, y se replica en todos los puntos de la red para alcanzar a los usuarios que han sintonizado a ese canal (en terminología multicast, están 'suscritos' a ese canal).

En el caso de los contenidos en vídeo bajo demanda (VoD), el usuario tiene control completo sobre la reproducción del programa (parada, rebobinado, avance rápido, etc.), por lo que se utilizan para su distribución las técnicas habituales "unicast", ya que no es posible compartir el mismo flujo entre múltiples usuarios. Para ello, se colocan servidores de vídeo bajo demanda en puntos relativamente próximos a los usuarios, a fin de conseguir la adecuada escalabilidad del sistema.

Otra tecnología básica en IPTV es la codificación/compresión de las señales de televisión. En los primeros despliegues se utilizó MPEG 2, el mismo estándar de codificación que se usa en los DVD, que codifica una señal de video estándar en 4 Mbps y una de TV de alta definición en 20 Mbps. El avance tecnológico en el incremento de la compresión de los codificadores, de tal manera que el ancho de banda generado sea compatible con las tecnologías de acceso de banda ancha sobre pares de cobre (ADSL), ha llevado a que en los despliegues más recientes se utilice MPEG 4 que consigue la misma calidad de vídeo que en MPEG 2 con velocidades de codificación de aproximadamente, la mitad. Los decodificadores son un elemento clave en los sistemas IPTV. Estos elementos, además de realizar la decodificación de la señal de TV digital, realizan otras funcionalidades básicas como son presentar al usuario la interfaz de las aplicaciones.

2.2 FUNCIONALIDADES DEL SERVICIO IPTV

Entre las ventajas que ofrece IPTV frente a la televisión digital convencional, se pueden mencionar las siguientes:

- *Video bajo demanda (VoD)*, ya que cada usuario dispone de una televisión a la carta, y puede elegir qué película o programa desea ver y a qué hora.
- *Un mayor contenido,* ya que se pueden ofrecer los mismos canales disponibles en la televisión por cable convencional, satélite o TDT, pero además dentro de la oferta de contenidos se puede contar con un almacén de películas y/o programas de televisión, para ser vistas por los usuarios durante un tiempo mayor que las películas o eventos en emisión de una TV digital convencional.
- *Comodidad en la visualización*, a través del formato de video bajo demanda, un usuario puede disfrutar del contenido tantas veces como desee, es decir, puede parar una película en cualquier momento, rebobinar para volver a ver una escena.
- *Publicidad personalizada,* debido a que se trata de un canal bidireccional, los usuarios podrán determinar y seleccionar cuales son las áreas de interés sobre las que les gustaría recibir ofertas de publicidad, siendo así mucho más efectiva.
- *Servicios de valor añadido*, ya que es factible el acceso a todo tipo de información, no solo a contenidos televisivos sino también por ejemplo a contenidos de e-learning, buscadores, e-mail, etc.

2.3 DESPLIEGUE DEL SERVICIO IPTV

El servicio de IPTV se ha desarrollado rápidamente, siendo Europa la región que está liderando este crecimiento. Entre los despliegues más importantes conviene destacar el servicio Imagenio de Telefónica, lanzado en

España comercialmente en el año 2004 que cuenta en la actualidad con más de 300.000 usuarios. En España, a finales de 2005 Jazztel empezó también a prestar este tipo de servicios con el nombre Jazztelia TV. Otras ofertas audiovisuales en este sentido son la de Orange (Orange TV) y Superbanda.

Otros despliegues importantes en Europa son los de France Telecom con su servicio MaLigne TV lanzado en 2003 y con más de 400.000 usuarios en la actualidad, y FastWeb en Italia quienes superan los 350.000 usuarios, Deutsche Telecom y Telecom Italia. En líneas generales todas estas ofertas se presentan como Doble o Triple Play, ofertas donde, junto con Internet, se ofrece un servicio añadido de voz y/o contenidos audiovisuales.

En Alemania, la plataforma Premiere tiene implementado un STB híbrido con recepción por satélite y retorno e interactividad a través de red IP, mientras que en el Reino Unido, tanto British Telecom, con el servicio BTVision, como Orange están ofreciendo también servicios de IPTV.

Asia y el Pacífico están claramente a la vanguardia del movimiento de IPTV. Varios factores hacen de Asia un terreno atractivo para los servicios de IPTV, por ejemplo, muchos países de la región tienen sólidas redes de acceso de banda ancha con velocidades de conexión más elevadas que el resto del mundo. La infraestructura necesaria para el servicio de IPTV ya está presente, con un prometedor crecimiento de suscriptores que tienen lugar en países como China, Corea del Sur, Taiwán y Japón, convirtiendo a la región en el segundo mayor mercado de IPTV en el mundo.

De acuerdo al informe de investigación "Pronóstico Global de Mercado de IPTV para el año 2014" la región de Asia-Pacífico se prevé que representarán alrededor del 45% del global de suscriptores de IPTV en 2014. Según el informe, la penetración de este servicio en la mayoría de los mercados asiáticos es inferior al 10%. Sin embargo, Taiwán, Corea, Singapur

y Japón han sido testigos de importantes mejoras en la penetración de IPTV en los últimos dos años, y muestran un gran potencial para IPTV para convertirse en una plataforma de televisión de pagos similares.

En Estados Unidos, el mercado de suscriptores de IPTV en el año 2008 aumentaron un 113% desde 1.75 millones en 2007 a 3.84 millones en 2008, experimentándose en esta franja de tiempo el avance más espectacular hasta el momento.

2.4 IPTV EN LATINOAMERICA

De acuerdo con el estudio "Análisis del Mercado IPTV en América Latina" de Signals Telecom Consulting de enero 2011, IPTV en América Latina surge como una plataforma premium focalizada en clientes de alto poder adquisitivo. Dentro de este marco, Brasil, Colombia y México, los tres mercados más avanzados en la región, representarán más del 70% de los abonados de IPTV para 2015 en América Latina.

Según BNAmericas, en el último trimestre del año 2007 habían 8.991 subscriptores, número que creció a 58.440 en el último semestre de 2008. En estadísticas más actuales ofrecidas por Dataxis NexTV, en febrero 2011 proyectó que Latinoamérica alcanzaría unas 910.000 conexiones de IPTV para fines de año frente a los 400.000 registradas a fines de 2010. Esto marca un crecimiento agudo del IPTV en la región. El número total de conexiones de IPTV en la región llegará a unos 3,9 millones para fines del año 2015.

A pesar de que la tecnología está ganando fuerza dentro de América Latina, el principal problema que obstaculiza su expansión en ciertos países son marcos regulatorios que directamente prohíben la participación a los operadores con más potencial de hacerlo o dificultan su tendido, implementación y comercialización, como es el caso de Argentina para

quienes en este año, la Ley de Servicios de Comunicación Audiovisual puso fin a una vieja restricción legal permitiendo a las cooperativas brindar esta tecnología. De esta manera, ya son varias las entidades que se pusieron en marcha para lanzar el servicio.

Sin embargo, los marcos regulatorios no son el único frente que se debe atacar. Lo cierto es que en muchos países el tendido de cableado FTTH (Fiber-To-The-Home) no está disponible. "El problema es que pensamos que todas las telefónicas iban a implementar la última milla para las casas y tener un ancho de banda mucho más grande para las casas para implementar IPTV". (Álvaro Gazzolo, presidente y CEO de IPTV Américas)

Afortunadamente, muchas empresas de telecomunicaciones fijas han reevaluado los costos a largo plazo de tercerización de sus servicios de TV paga y han comenzado a ver la IPTV con otra perspectiva. Probablemente el protagonismo que esta plataforma está cobrando en otros mercados más avanzados tenga mucho que ver con esto. "Aquí en Estados Unidos, el DTH y los cables están perdiendo alrededor de 500.000 abonados mensuales a lo que es la IPTV, uno por ser una solución mucho más avanzada tecnológicamente, y dos, porque los costos han ido bajando". (Álvaro Gazzollo, 2011)

De este modo, se pueden ahora encontrar en América Latina varias iniciativas para implementar o mejorar la IPTV que, sin duda, está creciendo como plataforma masiva en el continente.

En Chile, Movistar Chile lanzó durante junio del 2007 su servicio de IPTV, complementando su actual servicio de Televisión Satelital "Movistar TV Digital", para así ofrecer diversos servicios interactivos como Video on Demand entre otros. Por su parte, la empresa Telefónica del Sur es pionero en este tipo de transmisiones en Chile, quien a su vez es el tercer operador

de IPTV en América Latina, el cual contaba con 34.557 usuarios en diciembre 2010 (datos aportados por la Subsecretaría de Telecomunicaciones de Chile - Subtel).

Igualmente en Panamá, la empresa CTV Telecom desde agosto del 2007 brinda el servicio de IPTV a través de su red de última generación en fibra óptica, la cual hacen llegar hasta las residencias de sus clientes.

En Colombia, Empresas Públicas de Medellín, a través de su filial UNE-EPM Telecomunicaciones, dio inicio con la entrada en operación en julio de 2008, de la IPTV. De esta manera, UNE se consolida como la primera compañía en Colombia y cuarta en Latinoamérica en ofrecer el servicio de IPTV, ofreciendo sus servicios en la ciudad de Medellín y sus alrededores, así como en Bogotá a través de su filial EPM Bogotá. Para fines del tercer trimestre del 2010 contaba con cerca de 125.000 clientes de IPTV.

En Ecuador desde el año 2009 es ofrecido el servicio IPTV por parte de la Corporación Nacional de Telecomunicaciones (Amdinatel y Pacifictel).

Maxom es el segundo operador más importante de IPTV en América Latina detrás de Une en Colombia. Según datos de la CINIT (Centro de Investigación e Innovación en Telecomunicaciones) de abril 2011, la base de suscriptores de Maxcom creció 64% en 2010. Maxcom terminó el 2010 con 49.711 clientes, frente a los 30.371 que tenía en 2009. La operadora creció exactamente lo mismo (64%) entre 2008 y 2009.

En Uruguay, la empresa estatal ANTEL desde el año 2009 alcanzó las condiciones técnicas de brindar este nuevo servicio, bajo el nombre de adinet TV.

En República Dominicana la empresa Claro Codetel ha incorporado el servicio de IPTV, bajo el nombre de Claro TV.

En Venezuela, CANTV está desarrollando servicios de IPTV desde 2009 y se esperaba que el operador otorgue el servicio de forma pre comercial en el segundo trimestre del año 2012.

En Brasil, Telefónica es el principal proveedor de IPTV y lo hace a través de fibra óptica. Sin embargo, podrían producirse otros lanzamientos durante 2012, especialmente ahora que el gobierno planifica liberar las licencias y permitir a las telcos proveer de estos servicios sin necesitar la aprobación de su regulador local (Anatel).

En Paraguay, el servicio IPTV será ofrecida por la compañía estatal de telecomunicaciones COPACO (Compañía Paraguaya de Comunicaciones), para el año 2012.

2.5 ESTANDARES PARA EL DISENO DE SISTEMAS IPTV

2.5.1 FOCUS GROUP ON IPTV (FG IPTV)

Fue creado en abril del 2006, al final de la reunión de consulta para normalización de IPTV iniciada por la Oficina de Normalización de las Telecomunicaciones de la UIT-T (TSB), bajo la recomendación A.7. (FG IPTV, 2010).

La misión del FG IPTV es coordinar y promover el desarrollo de estándares globales para IPTV, teniendo en cuenta el trabajo actual de los grupos de estudio de la UIT, así como las normas de desarrollo de las organizaciones, foros y consorcios. Todo esto enfocado en los siguientes objetivos para la normalización de esta nuevo tipo de servicio:

- Definir IPTV e identificar los escenarios y las relaciones con otros servicios y redes, así como también la definición de los requisitos de arquitectura referencial.

- Revisar y analizar las deficiencias de las normas existentes y las obras en curso.
- Coordinar las actividades de normalización existentes.
- Concentrar la elaboración de nuevas normas para IPTV.
- Fomentar la interoperabilidad con los sistemas existentes donde sea posible.

El equipo formado a través del FG IPTV, inicio su labor en función de los objetivos antes mencionados y sus desarrollos son el resultado del despliegue e interoperabilidad a nivel mundial de este servicio. Fueron subdivididos seis grupos de trabajo para la estandarización y análisis de los siguientes tópicos:

- **Grupo de Trabajo 1 (GT1): Arquitectura y Requerimientos**

El objeto de este Grupo de Trabajo es realizar la definición del servicio, el usuario, los elementos que debe considerar la arquitectura referencial, tomando en cuenta los sistemas actuales que soportan este tipo de servicio. De esta manera, son evaluados escenarios con soluciones Redes de Próxima Generación (NGN) implementados y viceversa.

- **Grupo de Trabajo 2 (GT2): Calidad de Servicio (QoS) y Aspectos de Desempeño**

Este Grupo de Trabajo se enmarca en el desarrollo de las especificaciones de calidad de servicio (QoS) y de funcionamiento necesarias para garantizar la satisfacción del usuario final, y la aceptación del servicio de IPTV. De esta manera, se identifican y evalúan los parámetros ideales de Calidad de Servicio (QoS) y Calidad de Experiencia (QoE) ideales para la entrega del servicio de extremo a extremo.

- **Grupo de Trabajo 3 (GT3): Seguridad del Servicio y Protección del Contenido**

En el GT3 proporciona un enfoque para abordar los mecanismos que permitan garantizar la seguridad y protección del servicio IPTV en los siguientes aspectos: contenido, redes, elemento terminales y los suscriptores.

- **Grupo de Trabajo 4 (GT4): Red de Control para IPTV**

El GT4 tiene la misión de especificar los requerimientos funcionales de la red de control, las capacidades de direccionamiento multicast para la configuración de este servicio y la lista de protocolos requeridos para la integración dentro de la red.

- **Grupo de Trabajo 5 (GT5): Sistemas de Usuario Final y Aspectos de Interoperabilidad**

El ámbito de estudio del GT5 incluye la descripción de los dispositivos terminales y la red del usuario final que soportan el servicio IPTV, analizando los siguientes aspectos:

a. Dispositivos Terminales.
b. Red usuario final.

- **Grupo de Trabajo 6 (GT6): Mediador (Middleware), Aplicaciones y Plataformas de Contenido.**

En este último Grupo de Trabajo se lleva a cabo la definición de las plataformas del mediador (middleware), incluyendo las aplicaciones, formato de contenidos y sus usos, a fin de facilitar la efectividad e interoperabilidad

con los distintos sistemas y plataformas que interactúan para otorgar el servicio IPTV.

En la figura 2, se muestra la arquitectura del middleware, el cual representa el núcleo del sistema IPTV, realizando una administración integral del contenido, usuarios, proveedores de contenido, proveedores de servicios y guía de programación. Las entidades funcionales, que son relativamente independientes, están divididas en nueve subsistemas principales: sistema de administración de servicio (SMS), sistema de administración de derechos digitales (DRM), sistema de guía de programación (EPG), sistema de procesamiento de contenido, sistema de administración de contenido (CMS), sistema de librería de videos, sistema distribuido de streaming de contenidos, sistema de VAS (servicios de valor agregado) y la red de distribución de contenido (CDN).

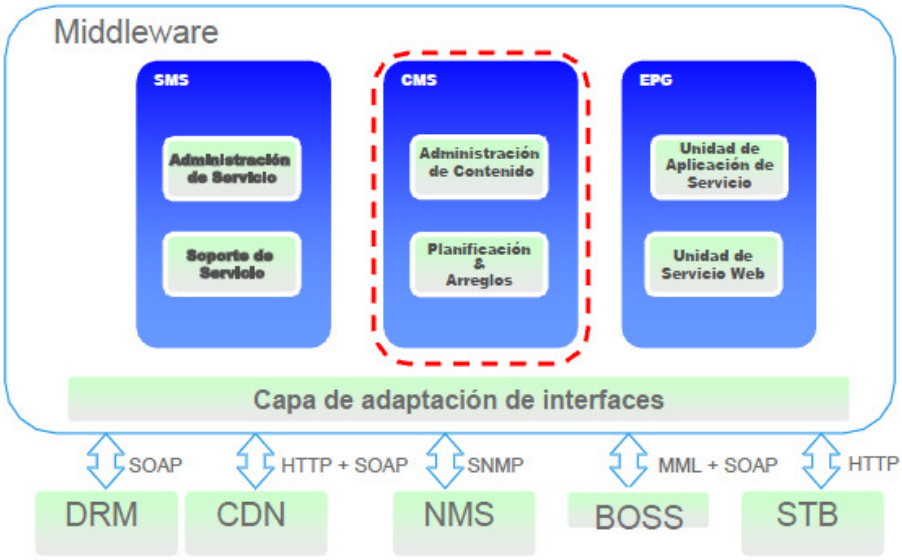


Figura 2. Arquitectura del Middleware del FG IPTV. Fuente: Ghassem Koleyni Nortel Networks Chairman (2006)

2.5.2 ALIANZA PARA LAS SOLUCIONES DE LA INDUSTRIA (ATIS) IPTV

Es una organización comprometida con el desarrollo y la promoción de normas técnicas y de operaciones para el sector de las telecomunicaciones y la industria relacionadas con tecnologías de la información en todo el mundo. De esta manera, en Junio del año 2005 esta organización creo el Foro de Interoperabilidad IPTV (FII), con la misión de permitir la interoperabilidad, interconexión y la aplicación de sistemas/servicios de IPTV mediante el desarrollo de normas ATIS. Este foro se desarrolló para su uso en América del Norte y las empresas miembros de la ATIS deben efectuar la coordinación con otras organizaciones para el desarrollo de estándares regionales e internacionales. (ATIS, 2008).

Para llevar a cabo lo antes expuesto se crearon cinco fuerzas de trabajo enfocadas en las siguientes áreas:

- **Comité Arquitectura FII,** dentro de este grupo se desarrolla la arquitectura estándar para el servicio IPTV, así como las especificaciones necesarias para permitir el despliegue de un sistema normalizado, interoperable, con un acceso independiente del servicio NGN.
- **Comité Soluciones Seguridad IPTV FII***,* en esta comisión se llevan a cabo trabajos con grupos de otras normas que participan en actividades de seguridad de contenido, con el objetivo de seleccionar un método único de seguridad, o el establecimiento de un marco en el que varios métodos puedan ser utilizados para el desarrollo de una solución de seguridad normalizada e interoperable para este servicio.
- **Comité de Metadata y Entrega de Transacciones FII,** en esta área se investiga la arquitectura de IPTV para identificar los elementos de metadata que requieren ser normalizados,

incluyendo aspectos de seguridad, conectividad, transporte y codificación. Adicionalmente, se analizan las métricas de desempeño necesarias para el transporte de la información sensible al tiempo de entrega.

- **Comité de Métricas de Calidad de Servicio (QoSM) FII,** dentro de este equipo se desarrollan las métricas, modelos, herramientas y técnicas para la medición de la QoS y QoE del servicio IPTV.
- **Comité de Pruebas e Interoperabilidad (T&I) FII,** es un grupo dentro del cual se realiza el análisis, planificación, pruebas, despliegue y operaciones de interoperabilidad del servicio IPTV. Además, se efectúan códigos y escenarios de prueba de las normas en desarrollo para mitigar así los problemas de despliegue en el campo. (Ocallaghan Daniel, 2008).

2.5.3 INSTITUTO EUROPEO DE NORMAS DE TELECOMUNICACIONES ETSI (EUROPEAN TELECOM STANDARDS INSTITUTE)

ETSI es un organismo para la producción de normas de aplicación mundial en las TIC (Tecnologías de Información y Comunicaciones), incluyendo los tópicos de telefonía fija, móvil, radio, servicios convergentes, de difusión y las tecnologías de Internet, y es oficialmente reconocida por la Unión Europea (UE) como la Organización Europea de las Normas. (etsi.org, 2010).

En una organización independiente, sin fines de lucro con sede en el parque de Sophia Antipolis, en el sur de Francia, con más de 700 organizaciones miembros procedentes de 62 países en todo el mundo, la cual engloba a: fabricantes, operadores de redes, administraciones nacionales, proveedores de servicios, organismos de investigación, grupos de usuarios y consultoras.

TISPAN (Telecoms and Internet-converged Services and Protocols for Advanced Networks), es una rama de la ETSI centrada en todos los aspectos relativos a la estandarización de la convergencia de redes, incluyendo la NGN, considerando aspectos de servicio, de arquitectura, de protocolos, de seguridad y de movilidad dentro de las redes fijas. De esta manera, es el órgano responsable de ETSI para la integración de IPTV en la NGN, a través de la combinación de múltiples servicios de telecomunicaciones y Web (voz, datos, presencia, mensajería, la comunidad, IPTV) mediante la reutilización de la misma IP basada en componentes NGN. (etsi.org, 2010).

En el Release 2-NGN, finalizado a principios de 2008, ETSI TISPAN definió la integración de los servicios de IPTV en una arquitectura, especificando dos soluciones, integrados y basados en IMS (IP Multimedia Subsystem), ambas incluyendo difusión broadcast de televisión, contenido bajo demanda y PVR, como se muestra en la siguiente figura.

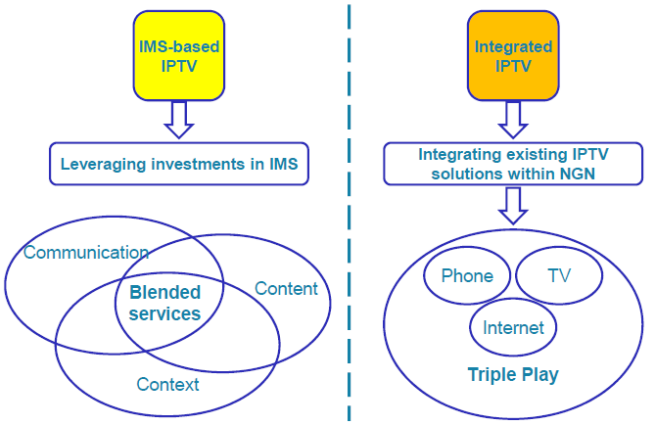


Figura 3. Especificación ETSI TISPAN IPTV. Fuente: etsi.org

En la figura 3, se ilustra que para las soluciones de IPTV integradas, el subsistema se centra en la convergencia de soluciones de mercado

existentes en un entorno de NGN, para la cual los proveedores de servicio de la red se benefician de las ventajas de costo que proporciona la integración del servicio IPTV sin modificaciones fuertes de su actual red de NGN. En el segundo escenario, de servicios IPTV basado en la arquitectura IMS, se puede obtener la mezcla de servicios de televisión con otros servicios de telecomunicaciones (por ejemplo voz y servicios de datos).

En el TISPAN-Release 3, se añaden nuevos tipos de servicios mediante la combinando las características de la red NGN (voz, datos, mensajería, PTV):

- Generación de contenido.
- Recomendaciones de los usuarios.
- Canales personalizados.
- Personalización de contenido.
- Servicios de control compartidos.
- Mensajería
- PVR avanzado.
- IPTV Roaming / Movilidad
- Sincronización de media

2.6 PROTOCOLOS Y TECNOLOGIAS UTILIZADAS PARA EL DESPLIEGUE DE SERVICIOS IPTV.

2.6.1 LÍNEA DIGITAL ASIMÉTRICA DE SUSCRIPTOR (ADSL)

La tecnología de línea de abonado digital asimétrica ó ADSL (estándar ANSI T1.413 y el ITU G-992.x), consiste en una línea digital de alta velocidad, apoyada en el par simétrico de cobre que lleva la línea telefónica convencional o línea de abonado. (Tanenbaum, 2003).

Es una tecnología de acceso a internet de banda ancha, lo que implica capacidad para transmitir más datos, y a su vez, se traduce en mayor velocidad. Esto se consigue mediante la utilización de una banda de frecuencias más alta que la utilizada en las conversaciones telefónicas convencionales (300-3.400 Hz) por lo que, para disponer de ADSL, es necesaria la instalación de un filtro (llamado splitter o discriminador) que se encarga de separar la señal telefónica convencional de la usada para conectarse con ADSL.

Entre los objetivos principales del ADSL destacan:

- ADSL debe funcionar sobre los circuitos locales existentes de par trenzado categoría 3.
- ADSL no debe afectar el funcionamiento de máquinas de fax, ni teléfonos existentes.
- ADSL debe superar la velocidad de 56 Kbps

Esta tecnología se le llama asimétrica porque del 80 al 90 % del canal se dedica al enlace descendente (downstream) y de un 10 a 20 % al enlace ascendente (upstream). En este tipo de servicio, la calidad de la línea telefónica es muy importante y se ajusta automáticamente la capacidad de transmisión.

El esquema que se maneja en ADSL, como se muestra en la figura 4, es instalar un Dispositivo de Interfaz de Red (Modem ADSL) en el lado del usuario para acceder al servicio, éste es el límite entre la propiedad de la compañía telefónica y la propiedad del usuario. Junto al modem ADSL se suele instalar un filtro para dividir la señal de datos con la de voz. La mayoría de los módems ADSL son externos y se conectan al computador del cliente por medio de redes Ethernet o cable USB.

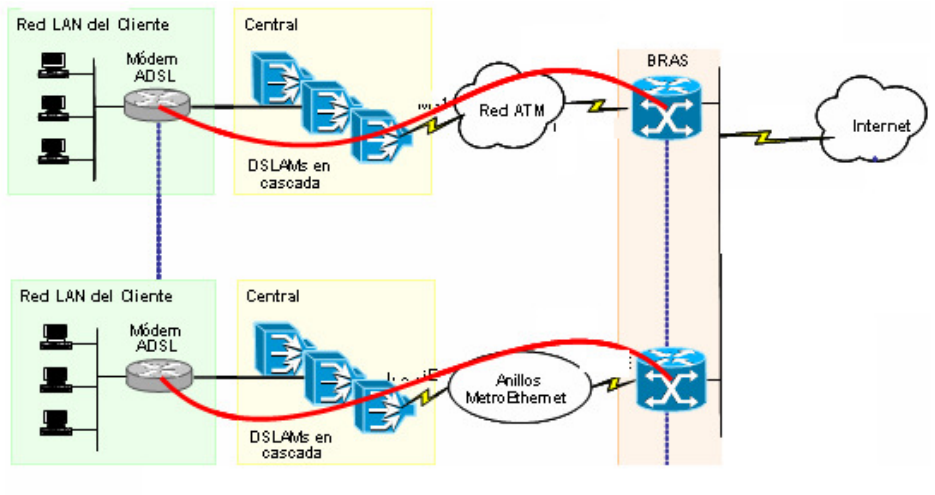


Figura 4. Arquitectura ABA CANTV. Fuente CANTV 2006

Actualmente, existen versiones mejoradas de esta tecnología como ADSL2 y ADSL2+, las cuales fueron desarrolladas para ofrecer servicios que requieren mayor capacidad de ancho de banda como por ejemplo televisión y video de alta calidad por el par telefónico. La principal diferencia con respecto a un sistema ADSL es que la cantidad de espectro que se puede usar sobre el cable de cobre del bucle de abonado es mayor, con lo cual se alcanzan tasas de transferencia superiores a las proporcionadas por el ADSL convencional, utilizando la misma infraestructura telefónica basada en cables de cobre. De esta manera, con ADSL se obtienen tasas máximas de bajada/subida de 8/1 Mbps, con ADSL2 se consigue 12/2 Mbps y con ADSL2+ 24/2 Mbps. En la tabla 1, se muestra las versiones disponibles para la tecnología ADSL y las velocidades de transferencia disponibles para cada uno de estos.

Tabla 1. Tecnologías ADSL y estándares asociados

Tecnología	*Estándar*	*Velocidad Máxima bajada*	*Velocidad Máxima subida*
ADSL	ANSI T1.413-1998	8 Mbps	0.8 Mbps
ADSL2	ITU G.992.3	12 Mbps	1.0 Mbps
ADSL2+	ITU G.992.5	24 Mbps	1.0 Mbps

El servicio de IPTV a ofrecer por CANTV, estará soportado en el transporte Metro Ethernet y acceso ADSL2+ a través de los DSLAM IP. Para ello, el equipo terminal del cliente (CPE) será un modem ADSL2+ que se conectara al nodo de acceso DSLAM IP a través del mismo par de cobre de acceso telefónico (ver figura 5), con una comunicación asimétrica, es decir, en dirección hacia la red (upstream) la velocidad de transmisión de datos será alrededor de los 800 Kbps y en dirección hacia el cliente (downstream) será de 6 Mbps mínimo. (CANTV, 2009).

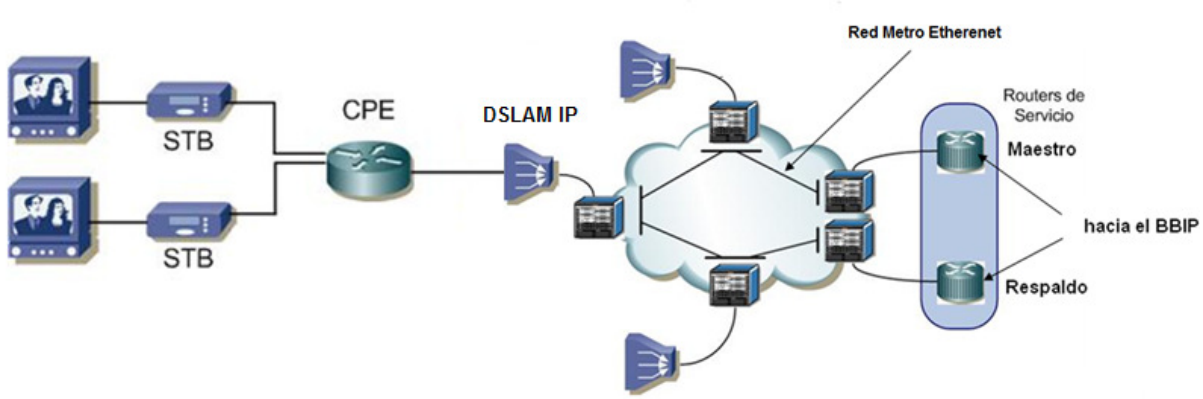


Figura 5. Arquitectura Red Acceso y Transporte para el Servicio IPTV de CANTV. Fuente: CANTV (2009)

2.6.2 METRO ETHERNET

Las Metro Ethernet (ME), son redes metropolitanas basadas en tecnología Ethernet sobre fibra óptica, con lo cual se elimina la capa ATM/SDH de las redes metropolitanas tradicionales. Soportan servicios de

capa 2 tales como VPN-L2 (Virtual Private Networks Layer 2), VPLS (Virtual Private LAN Services) y VLL (Virtual Lease Lines). (CANTV, 2006).

Los nodos Metro Ethernet son switches Ethernet que se interconectan utilizando directamente fibra óptica en topologías de anillo o bus, garantizando calidad, escalabilidad y protección de los servicios mediante MPLS (Multi Protocol Label Swiching).

En términos generales, todos los servicios de usuarios finales son transportados por la ME como servicios MPLS, con las siguientes ventajas intrínsecas a MPLS:

- Aseguramiento de QoS sobre toda la ME.
- Alta confiabilidad tanto para la red como para los servicios transportados, con tiempos de restauración del orden de los milisegundos.
- Escalabilidad basada en MPLS.
- Gestión de red y servicios extremo a extremo.

La arquitectura de las redes Metro Ethernet de CANTV está basada en anillos de acceso, los cuales se interconectan a través de un "switch" de cabecera, con un anillo Metro Ethernet de la red de distribución del troncal IP, los cuales implementan enrutamiento "capa 3" entre los anillos de acceso. El anillo Metro Ethernet se conecta con el resto de la red a través de un par de routers del Core de la red troncal IP, los cuales implementan protocolo de enrutamiento BGP (Border Gateway Protocol) para acceso a Internet. (CANTV, 2006).

En la figura 6 se muestra, como ejemplo, la arquitectura de los anillos Metro Ethernet de CANTV.

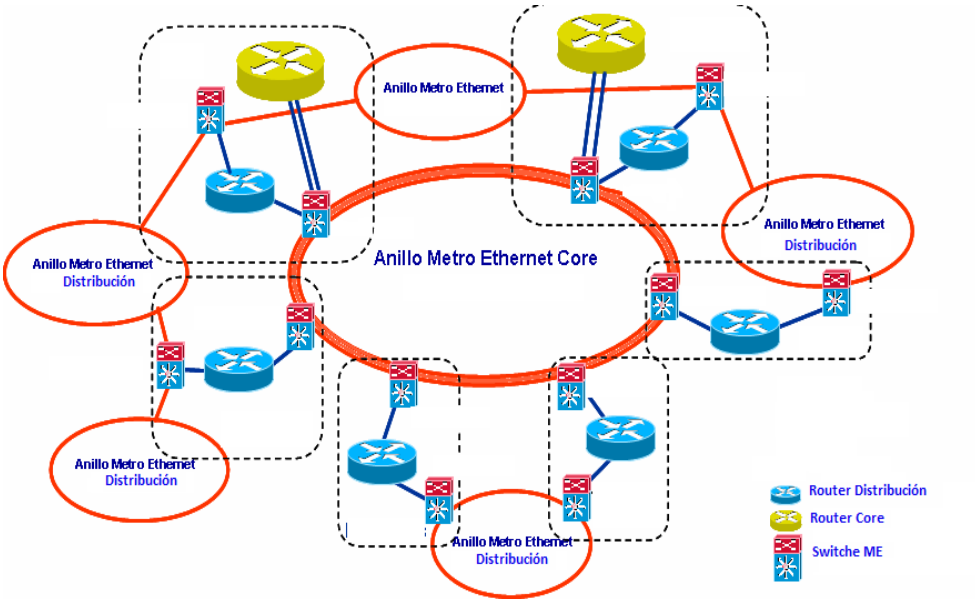


Figura 6. Arquitectura Red Metro Ethernet CANTV. Fuente: CANTV 2006

Los usuarios finales se conectan a los anillos de acceso a través de los DSLAM los cuales se conectan a los "swiches" Metro Ethernet vía enlaces Gigabit Ethernet (GE). Los suscriptores se conectan a los DSLAM utilizando un CPE (modem ADSL).

En la figura 7, se puede observar que para el servicio IPTV, la red Metro Ethernet se encarga de interconectar los DSLAM IP con los enrutadores de servicio, y de allí hacia la red troncal IP. Los enrutadores de servicio se encargaran de realizar la agregación capa 3 del servicio de video, además de ser la puerta de enlace por defecto de los usuarios del servicio (STB). En este equipo se definen los protocolos de video multidifusión (Multicast) para la recepción de las señales de video provenientes de la red troncal IP y la entrega de las señales de video hacia los clientes a través de la red Metro Ethernet y los DSLAM IP.

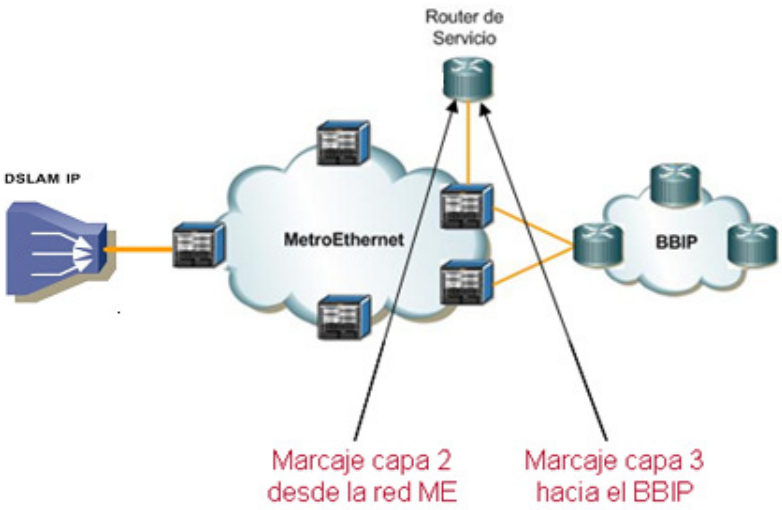


Figura 7. Red Troncal IP "Enrutador de Servicio" para IPTV. Fuente: CANTV 2007

2.6.3 SERVICIOS MULTICAST

El término multicast se refiere a la transmisión de una señal de vídeo única a varios usuarios de forma simultánea. Como ocurre con la técnica broadcast, todos los usuarios reciben la misma señal al mismo tiempo, pero en este caso no hay un stream distinto para cada receptor. (Ver figura 8)

La ventaja más significativa de su uso en redes IP es la reducción del ancho de banda necesario para transmitir contenidos de alta calidad a través de la red. Esto es así porque sólo se envía un stream a cada router, que se encarga de realizar una copia para cada dispositivo receptor conectado. También se reduce la carga de procesado del servidor de contenidos ya que sólo transmite una copia del stream al router de distribución. La tecnología de IP multicast provee un eficiente sistema de transferencia de datos punto a multi punto en redes IP, reduciendo el consumo de ancho de banda en la red. Es comúnmente aplicado en transferencia de datos en tiempo real, video conferencia, copia de datos, juegos, etc.

Entre las ventajas que ofrece la tecnología multicast están:

- Mejora la utilización del ancho de banda, eliminando el tráfico redundante de los enlaces.
- Se tiene menos carga de utilización en el host (Fuente de Multicast) y en los routers, ya que el tráfico sólo se genera una vez y llega sólo a los usuarios que lo solicitan.
- Permite una red en la que no se conozcan las IPs de los destinatarios, en la cual cualquiera puede participar del grupo de multicast sin necesidad de darse de alta en el servidor por un administrador de sistemas.

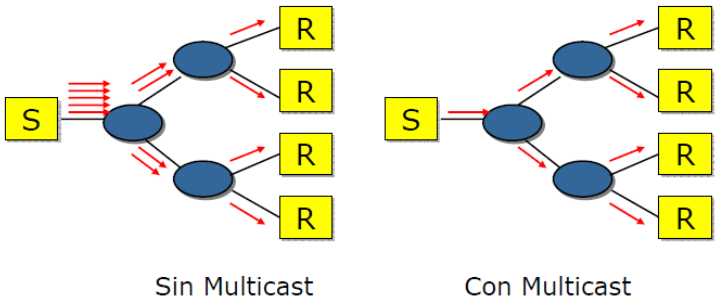


Figura 8. Tecnología IP Multicast. Fuente: elaboración propia

La técnica multicast se suele utilizar para emitir programaciones IPTV en vivo y es una técnica eficiente para su uso en infraestructuras IPTV. Sin embargo, la transmisión multicast presenta algunos inconvenientes:

- No da soporte a los controles VCR. No es posible realizar las acciones de rebobinar, pausa o avance rápido de los contenidos.
- Incrementa la carga de trabajo y procesado de los routers. Los routers deben realizar copias de los streams para enviarlos a todos los clientes conectados.
- Todos los componentes, desde la fuente de contenidos hasta el decodificador de usuario, deben soportar la tecnología multicast.

Un grupo de distribución de multicast implica una fuente (S) y uno o varios receptores (R) desconocidos, en el cual un receptor puede solicitar en cualquier momento participar de un grupo multicast ofrecido por una fuerte S. Esto lo hará mediante mensajes de IGMP (Multicast de L2) que envía a su router local.

En este caso la red tiene que ser capaz de responder ante esta petición, haciendo llegar al cliente estas tramas del grupo de multicast que ha solicitado, mediante los protocolos de routing (Multicast de L3).

El protocolo IGMP (Internet Group Management Protocol), es un "lenguaje" que utilizan los receptores para registrarse en un grupo de multicast, es decir, comunicarle a su router local que desea recibir tramas de ese grupo determinado. Además, también servirá para borrarse de un grupo o para decir que está todavía interesado en recibir estas tramas de multicast.

Gracias a la información recopilada mediante IGMP, los routers mantienen una lista de los grupos multicast en los que están interesados los hosts que están conectados a sus interfaces. Dado que generalmente los hosts se conectan a redes locales, el funcionamiento de IGMP afecta normalmente a las interfaces LAN de los routers.

Entre las características de los grupos multicast, destacan:

- IP multicast permite el envío de datagramas a un grupo concreto de nodos.
- El grupo completo de nodos se identifica por una única dirección IP (una dirección multicast).
- Los grupos son dinámicos, los nodos pueden entrar y salir de un grupo en cualquier momento. Un nodo puede ser miembro de varios grupos de forma simultánea.

- No hay limitaciones en el número de nodos que pueden estar un grupo.
- Un nodo puede enviar a un grupo sin pertenecer a él.
- Los grupos pueden ser permanentes o temporales.
- Los grupos permanentes tiene dirección IP fijas asignadas
- Los grupos temporales existen sólo mientras tengan miembros.

El servicio multidifusión (Multicast) de CANTV, permitirá a los suscriptores IPTV recibir canales de televisión (audio + video) tanto de señales abiertas (canales locales tipo VTV, ViVe, Venevisión) como los ofrecidos por otras cableras Sony, E, Discovery, HBO, Cimenax (servicio multidifusión), cuyas fuentes de señal serán provenientes de los codificadores/decodificadores “encoders/decoders” ubicados en el Headend.

Para la configuración del servicio de tráfico de multidifusión del servicio de IPTV de CANTV, serán establecidas VPLS por zona Metro Ethernet que permita entregar una sola copia de los canales multicast que provienen del Headend. La VPLS incluirá todos los switches Metro Ethernet que serán atendidos y los enrutadores de servicio que cuentan con la posibilidad de entregar los canales. Un enrutador de servicio será el maestro de la solución y el segundo enrutador será el respaldo en caso de falla del maestro garantizando alta disponibilidad del servicio, como se puede observar en la figura 9. (CANTV, 2007).

Para la inserción de los canales multicast y transporte de los mismos serán configurados los siguientes protocolos:

- **PIM SM** ó **SSM** para los Enrutadores de servicio, BBIP y Headend.
- **IGMP** para el Enrutador de servicio, Metro Ethernet, IPDSLAM y CPE. (CANTV, 2007).

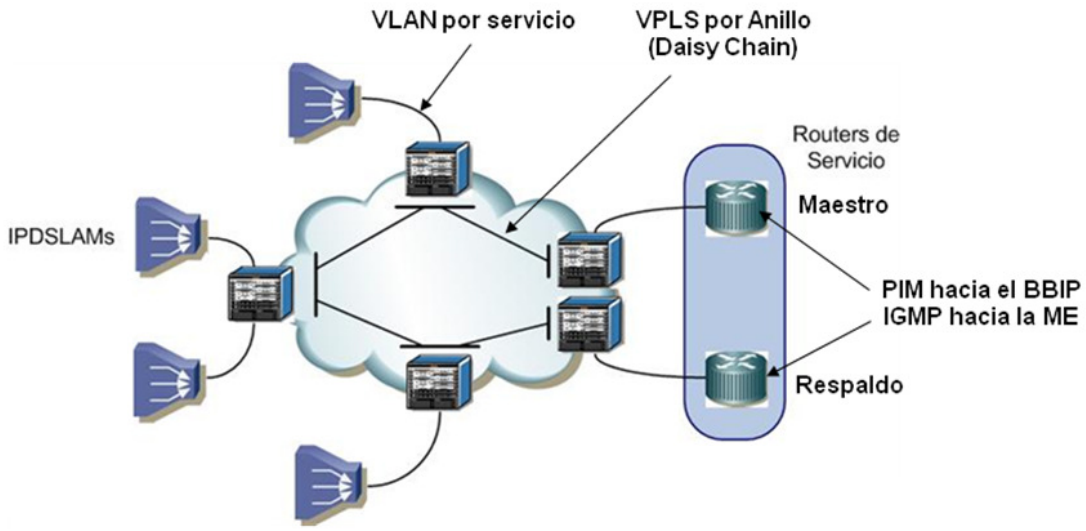


Figura 9. VPLS para el servicio de multidifusión IPTV CANTV. Fuente: CANTV 2007

2.6.4 SERVICIOS UNICAST

La técnica de transmisión unicast realiza el envío de contenidos creando conexiones individuales entre el centro de datos y el decodificador de usuario. Por ejemplo, si cuatro usuarios desean acceder al mismo canal, se deben crear cuatro conexiones punto a punto desde el centro de datos hasta el decodificador de cada usuario a través de la red IP. (Tanenbaum, 2003).

Por tanto, es una transmisión punto a punto con cada destinatario. Si se desea enviar la misma información y hay “n” destinatarios, habrá “n” comunicaciones puntos a punto independientes o “n” copias de la misma información enviadas desde la máquina origen.

Los servicios de unidifusión son creados para la conexión de un solo terminal, como pueden ser los de vídeo bajo demanda, donde cada terminal accede a un flujo específico de vídeo y los relacionados con almacenamiento

selectivo de información por medio de PVR (Grabador de Vídeo Personal), así como también los de Time Shift TV (TSTV).

En el caso de CANTV el servicio unicast, como se muestra en la figura 10, está asociado a todo el tráfico dedicado para cada usuario residencial. Este tráfico comprende el acceso dinámico al direccionamiento IP a través de servidores DHCP, el acceso al middleware y a los servidores de video bajo demanda. (CANTV, 2007).

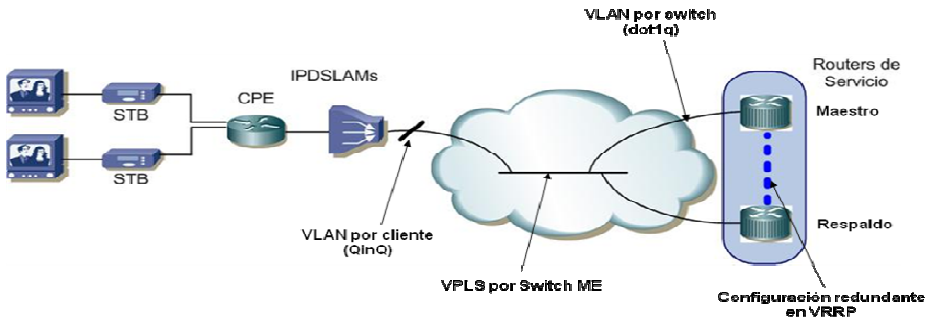


Figura 10. VPLS por switch para el servicio de unidifusión. Fuente: CANTV 2007

La configuración del servicio de unidifusión dentro de la red de CANTV comprende lo siguiente:

- Creación de una VPLS por switch Metro Ethernet para el servicio Unicast.
- Configurar un pool de direcciones IP por cada VPLS.
- Se debe crear una VLAN por cliente en la interfaz de uplink del DSLAM IP.
- Se debe crear un PVC para el servicio de Unidifusión por cada puerto ADSL2+ del usuario que cuente con el servicio.

2.6.5 SERVICIO VIDEO BAJO DEMANDA (VOD).

Mediante el servicio de VOD (vídeo on demand) el sistema de IPTV permite arrendar películas para ser visualizadas por los suscriptores. Estas están almacenadas por el operador y pueden ser reproducidas cuando las solicita el suscriptor generalmente a un costo adicional.

Para contratar las mismas, se navega en una serie de menús que están disponibles en el middleware accesible por los STB. El operador, clasifica aquí, de una manera atractiva las películas que dispone. Cada película es acompañada por información de: año, género, director, actores y demás datos que incluye la metadata de ellas. (Ver figura 11)

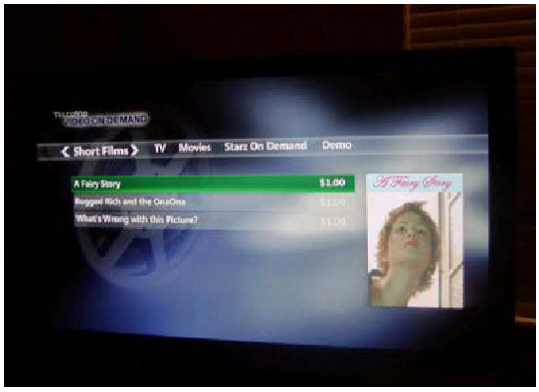


Figura 11. Vídeo Bajo Demanda. Fuente: TURBOTELTIC Cia. Ltda.

2.6.6 OTROS SERVICIOS DISPONIBLES CON IPTV

a) Personal Vídeo Recorder (PVR)

Permite a los suscriptores del servicio de IPTV la grabación de programas en vivo para luego ser reproducidos posteriormente emulando las funcionalidades de un vídeo grabador. Durante la reproducción se dispondrá las funciones de Play, Pause, Stop, REW (reversa), FF (avance rápido).

Dependiendo de la solución de IPTV que se adopte, el almacenamiento de los programas grabados pueden realizarse esencialmente de dos modos. En discos rígidos que pueden disponer STB de gama alta o en discos rígidos que se dispongan en la red para este fin.

b) Time Shift TV (TSTV).

Consiste en pausa de TV en vivo. Es una novedosa funcionalidad que permite “congelar” una imagen de un programa en vivo o repetir (Replay) alguna escena que fue reproducida recientemente.

Para implementar el TSTV se almacena en discos rígidos (en los STB o en una granja de servidores, dependiendo de la modalidad de trabajo que se hubiere elegido) un tiempo estipulado de la programación en vivo que se esté presenciando. Esa “porción de historia” de programa permitirá realizar un replay de lo ocurrido como máximo en ese tiempo almacenado o permitirá que durante la pausa o reproducción de replay se almacenen las escenas que se continúan emitiendo en el canal en vivo.

Cuando se reanuda la reproducción del programa, se continuará viendo el mismo donde se dejó. De aquí en adelante la programación emitida se almacena y se reproduce desplazado en el tiempo lo almacenado un tiempo atrás. Se puede disponer de la facilidad de adelanto para regresar a la reproducción en tiempo real.

c) Pay Per View (PPV).

Mediante el servicio PPV (pague por ver) se brinda a lo suscriptores la facilidad de contratar la posibilidad de ver un programa en particular. Es una característica que generalmente es utilizada para eventos deportivos o conciertos que están siendo emitidos en vivo. La modalidad conjuga

características de transmisión de TV en vivo y exige una contratación del contenido como en los casos de VOD.

2.6.7 MPEG (MOVING PICTURES EXPERT GROUP)

Para Tanenbaum (2003), los estándares MPEG (Grupo de Expertos de Imágenes en movimiento), comprende los algoritmos principales usados para comprimir video y han sido estándares internacionales desde 1993.

Los algoritmos del MPEG comprimen la información en pequeños paquetes que pueden ser transmitidos fácilmente y después ser descomprimidos. Con la compresión que utiliza el MPEG se pierden ciertos datos, pero ésta pérdida es generalmente imperceptible al ojo humano.

Tabla 2. Formatos de compresión multimedia

Formatos de compresión multimedia			
Formatos de compresión de video	**ISO/IEC**	**ITU-T**	**Otros**
	MJPEG • MPEG-1 • MPEG-2 • MPEG-4 ASP • MPEG-4/AVC • Motion JPEG 2000	H.120 • H.261 • H.262 • H.263 • H.264	AMV • AVS • Bink • Dirac • Indeo • Pixlet • RealVideo • RTVideo • SheerVideo • Smacker • Snow • Theora • VC-1 • VP6 • VP7 • WMV
Formatos de compresión de audio	**ISO/IEC MPEG**	**ITU-T**	**Otros**
	MPEG-1 Layer III (MP3) • MPEG-1 Layer II • AAC • HE-AAC	G.711 • G.722 • G.722.1 • G.722.2 • G.723 • G.723.1 • G.726 • G.728 • G.729 • G.729.1 • G.729a	AC3 • AMR • Apple Lossless • ATRAC • FLAC • iLBC • Monkey's Audio • Mu-law • Musepack • Nellymoser • OptimFROG • RealAudio • RTAudio • SHN • Siren • Speex • TAK • Vorbis • WavPack • WMA
Formatos de compresión de imagen	**ISO/IEC/ITU-T**		**Otros**
	JPEG • JPEG 2000 • lossless JPEG • JBIG • JBIG2 • PNG • WBMP		BMP • GIF • ICER • ILBM • PCX • PGF • TGA • TIFF • HD Photo
Formatos contenedor multimedia	**General**		**Sólo Audio**
	3GP • ASF • AVI • Bink • DMF • DPX • FLV • Matroska • MP4 • MXF • NUT • Ogg • Ogg Media • QuickTime • RealMedia • Smacker • RIFF • VOB		AIFF • AU • WAV

Los principales formatos de compresión MPEG son:

- **MPEG-1:** es el estándar inicial de compresión de audio y vídeo, publicado como ISO 11172. Proporciona video con una resolución de

352x240 a 30 frames por segundo (fps). Esto produce una calidad de video levemente inferior a la calidad de los videos convencionales VCR. Incluye el formato de compresión de audio de Capa 3 (MP3). MPEG-1 puede ser transmitido sobre par trenzado a distancias medias, también es utilizado para almacenamiento de películas en CD-ROM.

- **MPEG-2:** estándar para audio y vídeo para difusión de calidad de televisión, publicado como estándar ISO 13818. Ofrece resoluciones de 720x480 y de 1280x720 a 60 fps, con calidad CD de audio. Esto es suficiente para la mayoría de estándares de TV, incluyendo NTSC, e incluso HDTV. MPEG-2 se utiliza para video, servicios de TV por satélite y señales de TV digital por cable. MPEG-2 puede comprimir un vídeo de 2 horas en algunos gigabytes. Aunque descomprimir una secuencia de datos Mpeg-2 no requiere muchos recursos del ordenador, la codificación a formato Mpeg-2 requiere considerablemente más energía para el proceso.
- **MPEG-4:** algoritmo estándar de compresión de gráficos y video basado en la tecnología de Mpeg-1, Mpeg-2 y de Apple QuickTime. Los archivos Mpeg-4 son más pequeños que archivos JPEG o QuickTime, así que se diseñan para transmitir vídeo e imágenes a través de un ancho de banda estrecho y pueden mezclar vídeo con texto, gráficos y capas de animación 2D y 3D.

2.7 SOLUCION IPTV DE CANTV

2.7.1 DESCRIPCION DEL SERVICIO Y SUS ATRIBUTOS

CANTV ofrecerá el servicio de difusión por suscripción desarrollado sobre tecnología ADSL en la actual red de cobre, el cual incluirá una variada oferta de planes de canales básicos (broadcast TV), canales premium, canales a la carta, así como video bajo demanda, grabación personal de video, servicios de música digital, radio local e internacional.

Los atributos básicos y avanzados con los que contaran el servicio serán los siguientes:

- **Básicos:** Channel line-up: de 100 a 140 canales; Guía interactiva; Zapping time no mayor de 2 segundos; inicialmente un máximo de 2 televisores con un Set top-box por televisor; Calidad de la imagen digital; Control parental; Lista de favoritos personalizada
- **Avanzados:** Servicios bajo demanda; Personal Video Recorder (PVR); Canales a la carta; Disponibilidad en múltiples dispositivos (TV, PC, Teléfono); Juegos; e-commerce.

2.7.2 ALINEACION ESTRATEGICA PARA EL DESARROLLO DEL SERVICIO IPTV EN CANTV

La oferta de CANTV está orientada a masificar el servicio de difusión por suscripción en Venezuela, basándose en su amplia cobertura de líneas telefónicas a nivel nacional y una oferta de servicio con variedad de planes y precios orientados a los diferentes niveles socio-económicos existentes en el mercado venezolano, desde las clases sociales más desposeídas hasta aquellas de mayores ingresos, tal como actualmente lo constituye la cartera de clientes de la empresa. (CANTV, 2009).

La visión del proyecto es proveer el servicio de difusión por suscripción a todos y cada uno de los segmentos sociales que conforman la población venezolana, lo cual cambiaría radicalmente la composición de los actuales clientes del servicio en Venezuela, en vista de que hoy día, quienes disfrutan de estos servicios son los hogares que pertenecen a los segmentos de población más pudientes, quedando casi que totalmente excluidos de este servicio, las clases más populares del país.

Esta estrategia se encuentra en concordancia totalmente con cuatro (4) de los ocho (8) lineamientos estratégicos, los cuales son:

- Democratizar el servicio con justicia social.
- Ser líder en calidad del servicio, portafolio de productos y atención al cliente.
- Garantizar la auto sostenibilidad de la empresa.
- Potenciar el poder y la participación popular.
- Crecimiento rentable de ingresos, para contrarrestar una tendencia del segmento de masivos de caída de ingresos.
- Defensa del negocio de voz y de participación de banda ancha.

La incorporación de video a la oferta comercial de CANTV es una movida estratégica, rentable para el dominio del mercado de banda ancha y para el crecimiento y defensa de ingresos de la corporación. La estrategia es que CANTV se posicione como el proveedor preferido para el aprovisionamiento de múltiples servicios para el hogar (voz, datos y video en el corto plazo, juegos y nuevos servicios/contenidos en el mediano/largo plazo).

Perder la batalla del acceso al hogar pone en gran riesgo los negocios de voz y datos, así mismo, adecuar la red para soportar altos anchos de banda (8 Mbps por hogar), permitirá en el futuro desarrollar otros servicios que requieran altos anchos de banda con una inversión marginal.

2.7.3 ARQUITECTURA Y FUNCIONAMIENTO DEL SERVICIO IPTV DE CANTV

El servicio de distribución de video por suscripción consiste en la difusión de canales de televisión, bajo la tecnología IP sobre la red de banda ancha de CANTV. Estará compuesto por cuatro etapas:

Recepción/Procesamiento, Red de Transporte (Red Metro y Backbone IP) y Acceso (DSLAM), Predios del Cliente (CPE y Set Top Box) y Plataforma de Mediación (Middleware), tal y como se muestra en la siguiente figura:

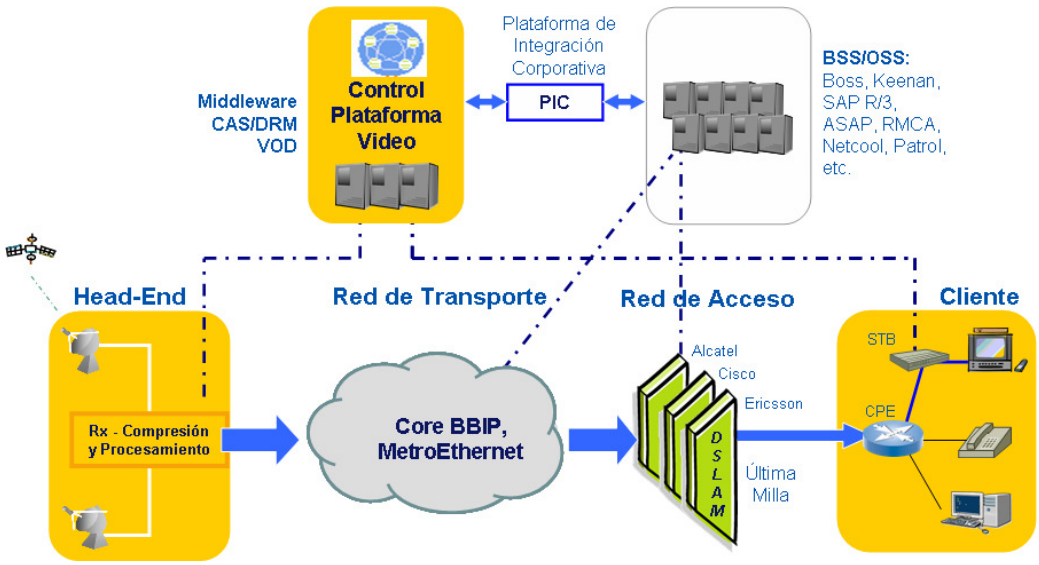


Figura 12. Arquitectura sistema IPTV de CANTV Fuente CANTV 2007

La etapa de recepción y procesamiento comienza con la recepción de las señales de los canales de video desde varias fuentes de origen. La gran mayoría de los canales se recibirán de distintos satélites en banda C y Ku, mientras que el resto de los canales, se obtendrán localmente, bien por señales transmitidas en UHF/VHF o directamente desde la fuente de origen vía fibra óptica. Una vez recibidas, dichas señales son separadas por canal, procesadas para corregir cualquier falla de origen en audio o video, digitalizadas y comprimidas, para posteriormente ser inyectadas a la Red de Transporte como un sólo flujo de datos.

El flujo de datos, conformado por todos los canales de video, se transmitirá de manera multicast sobre la red de transporte, tanto interurbana como urbana, hasta llegar a los nodos de acceso donde se ofrecerá el

servicio de difusión por suscripción. Para garantizar la calidad del servicio de extremo a extremo, se implementarán varias funcionalidades entre las que se encuentran MPLS y QoS.

Los nodos de acceso (DSLAM) serán los encargados de recibir de la red el flujo de video y entregar a los suscriptores los canales de televisión que estos demanden, a través de los equipos terminales de cliente (set top box).

Para prestar el servicio de difusión por suscripción, CANTV se apalancará sobre los nodos de acceso existentes, que son los que usa actualmente para ofrecer el servicio de internet banda ancha.

La capacidad del sistema o solución estará limitada por el número total de puertos ABA que estén instalados y adecuados en los nodos de acceso para ofrecer el servicio de IPTV. Dicha capacidad instalada estará definida por dos premisas fundamentales, la distancia de los clientes al nodo de acceso y el mínimo ancho de banda requerido para garantizar la calidad del servicio.

Toda la solución de video estará implementada sobre una plataforma de mediación (middleware), la cual constituye en términos generales, el corazón de la solución. Esta plataforma y sus diferentes componentes, son la interfaz de comunicación/interpretación entre los diferentes sistemas operativos implementados y las diversas aplicaciones/productos que operan en todo el sistema. La plataforma de mediación integrada con las plataformas y sistemas de CANTV (OSS/BSS), será la responsable por el proceso de facturación del servicio. (CANTV, 2007).

2.7.4 INTEGRACION SERVICIO IPTV EN LA RED CANTV

La implementación de la solución de IPTV adquirida por CANTV, requiere de la integración dentro de las tres capas más importantes de la red, las cuales comprenden: la capa de acceso; la capa de transporte y la capa core (red troncal IP).

En la figura 13 se muestra un diagrama general de la topología de la solución de CANTV:

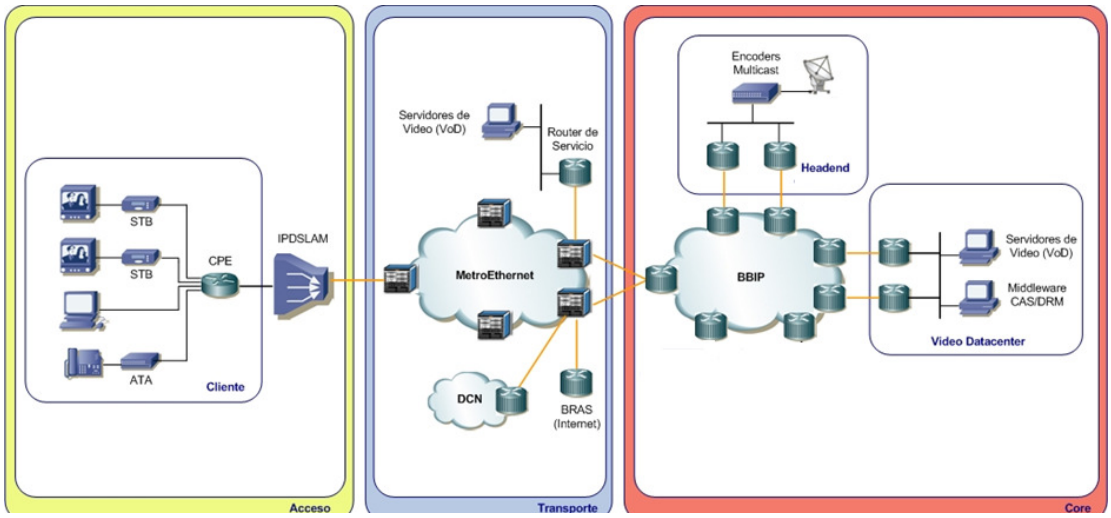


Figura 13. Topología de la solución de CANTV. Fuente: CANTV 2007

a) Capa core (Red Troncal IP)

La Red Troncal IP de CANTV está conformada por nodos de alta capacidad, mientras que el nivel de acceso está conformado por nodos de mediana capacidad que agregan y envían el tráfico a los usuarios finales. Estos dos niveles están conectados por anillos Metro Ethernet para el transporte metropolitano. (CANTV, 2006).

La siguiente figura muestra la topología del Transporte IP (niveles Troncal y Distribución):

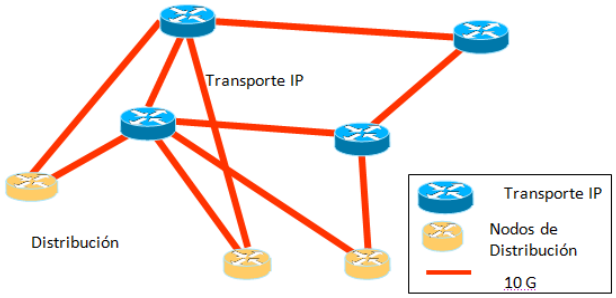


Figura 14. Topología de la Red Troncal y Red de Distribución.
Fuente: CANTV 2006

b) Capa de transporte (Metro Ethernet)

Se usará la red Metro Ethernet para el transporte y distribución de video a nivel metropolitano. Esta red está conformada por 35 anillos urbanos redundantes interconectados por los enrutadores de transporte, los cuales manejan interfaces desde los 1Gbps hasta los 10Gbps. (CANTV, 2006).

La siguiente figura muestra un diagrama de uno de los anillos:

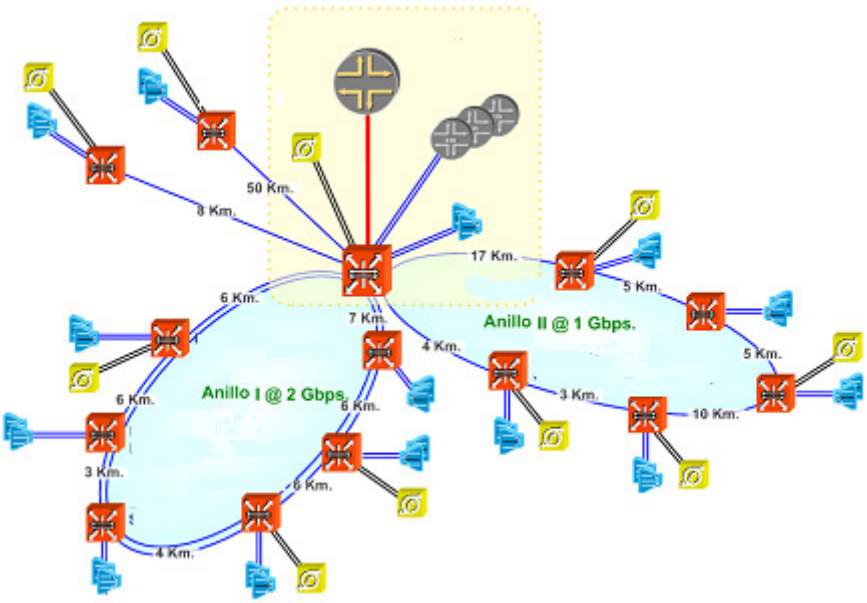


Figura 15. Topología de un Anillo Metro Ethernet Fuente: CANTV 2006

Una vez que el flujo de video llega a los DSLAMs, finaliza la funcionalidad multidifusión y se establece un intercambio uno-a-uno entre el nodo de acceso y el STB del usuario final. Esta etapa de la red de Acceso es sumamente crítica para el éxito del servicio.

c) Capa de acceso y última milla

La planta externa de CANTV tiene un total de 4.844.000 líneas instaladas de las cuales 3.280.000 o 68% están activas. La planta total está protegida por gel (48%) o por presurización (52%). (CANTV, 2006).

Actualmente se está suministrando un servicio de internet de alta velocidad (HSI) en todos los calibres con planes comerciales y ofertas de ancho de banda de hasta 2 Mbps.

CAPITULO III

ESTÁNDARES DE ADMINISTRACIÓN DE RIESGO

3.1 GESTION DE RIESGO

La gestión del riesgo es una responsabilidad de todos, y más si se está presente dentro de funciones o procedimientos susceptibles de cualquier análisis de auditoría sobre el mismo. Una activa gestión del riesgo, soportada en sistemas de información y un continuo monitoreo ayuda a proteger el personal, los proyectos y los activos.

Para GIT Ltda. (2010), “La gestión del riesgo, contribuye a una adecuada Gobernabilidad Corporativa, al proveer a la Junta y Alta Gerencia, de una seguridad razonable de que los objetivos de la organización serán logrados, dentro de un grado tolerable de riesgo residual”

En este sentido, las principales razones que motivan a la Gerencia de Seguridad de la Operación de CANTV a la aplicación de esta tendencia de administración de riesgo operacional, para cumplir con la función de aseguramiento de la calidad para las plataformas operativas Telco y Móvil, se pueden mencionar las siguientes:

- Evitar impactos costosos, garantizando la estabilidad de las operaciones.
- Arraigar la cultura de Gestión del Riesgo para asegurar el logro de los objetivos y metas.
- Hacer realidad uno de los objetivos estratégicos de la empresa, como lo es el aseguramiento de la calidad de servicio de su portafolio de productos.
- Flexibilidad para afrontar cambios en el ambiente operativo,

directrices del estado e implementación de nuevas estrategias.

- Cumplir con las normas y regulaciones del estado.
- Mantener la competitividad.

Según el estándar AS/NZS: 4360, el riesgo se define como: “la posibilidad de que algo ocurra y afecte las metas”.

El Comité de Basilea define el riesgo operacional como “el riesgo de pérdidas resultantes de la falta de adecuación o fallas en los procesos internos, de la actuación del personal o de los sistemas o bien aquellas que sean producto de eventos externos”.

3.2 ESTANDARES MUNDIALES PARA LA ADMINISTRACION DE RIESGOS

Los estándares mundiales bajo los cuales se fundamenta hoy en día la Administración de Riesgos, a fin de efectuar el diseño e implementación de un Sistemas de Gestión Integral del Riesgo, son los indicados en el figura 16.

Figura 16. Estándares Mundiales y la Administración del Riesgo.
Fuente: Elaboración propia

3.2.1 MODELO COSO (COMMITTEE OF SPONSORING ORGANIZATIONS)

COSO, o Comité de Organizaciones Patrocinadoras tiene como misión desarrollar marcos generales y de orientación sobre la gestión del riesgo empresarial, control interno y la disuasión del fraude, a fin de mejorar el desempeño, la gestión y reducir el alcance del fraude en las organizaciones. (Coso.org , 2011).

Este comité se formó en 1985 en los Estados Unidos para patrocinar a la Comisión Nacional de Fraudes Financieros, también conocida como "Comisión Treadway", creada con el objetivo de identificar las causas de la presentación de información financiera en forma fraudulenta o falsificada y emitir recomendaciones que llevaran a garantizar la máxima transparencia en lo que se refiere a la información financiera.

El grupo de trabajo estuvo constituido por representantes de cinco organismos profesionales:

- AAA – Asociación Americana de Contadores.
- AICPA – Instituto Americano de Contadores Públicos Autorizados
- FEI – Instituto de Ejecutivos Financieros
- IIA – Instituto de Auditores Internos
- IMA – Instituto de Contadores Gerenciales

Todas las organizaciones patrocinadoras de la Comisión Treadway mencionadas anteriormente, debatieron durante más de cinco años y finalmente en 1992, se emite el informe COSO, denominado Internal Control-Integrated Framework (IC-IF), conocido también como COSO I, el cual fue adoptado por el sector público y privado en USA, por el Banco Mundial y se extendió rápidamente por toda Latino América.

En septiembre de 2004, se publica el informe denominado Enterprise Risk Management – Integrated Framework, el cual incluye el marco global para la administración integral de riesgos. (Ver figura 17)

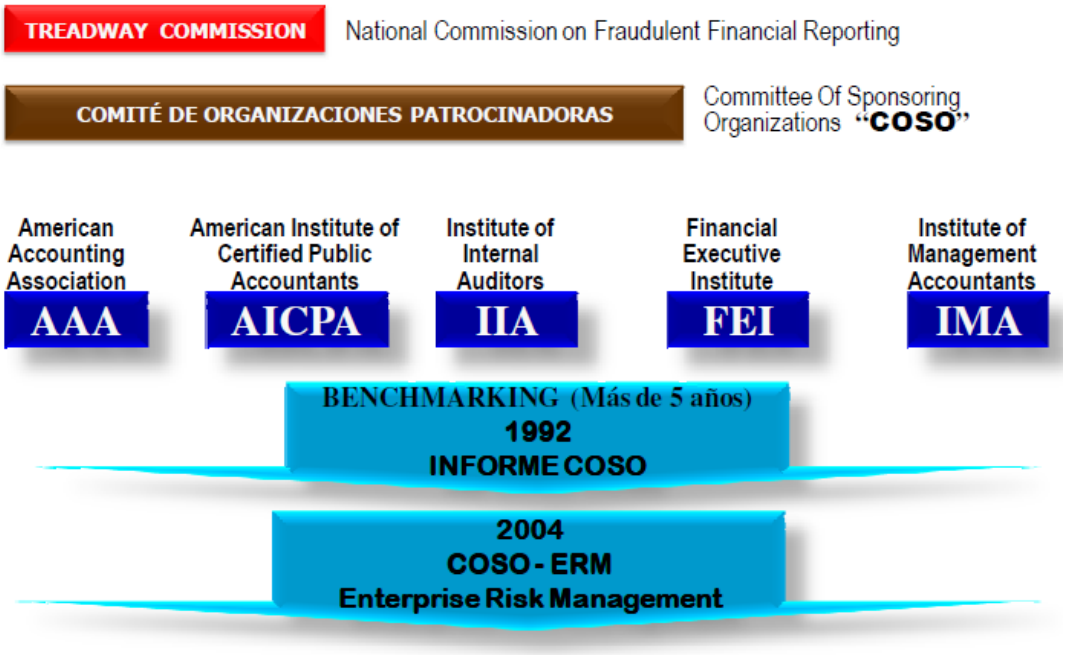


Figura 17. Esquema COSO. Fuente: GIT Ltda.

3.2.2 INFORME COSO

El “Informe COSO” constituyó un gran avance al acordar una definición respecto al concepto de control interno, logrando establecer un marco conceptual común y se constituye en una visión integradora del control interno.

COSO (1992). El control interno es un proceso efectuado por la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos dentro de las siguientes categorías:

- Eficacia y eficiencia de las operaciones.
- Confiabilidad de la información financiera.
- Cumplimiento de las leyes, reglamentos y normas que sean aplicables.

De acuerdo al marco COSO, el control interno consta de cinco componentes relacionados entre sí. Estos derivarán de la manera en que la dirección dirija la empresa y estarán integrados en el proceso de dirección. Los componentes son los mismos para todas las organizaciones (sean públicas o privadas) y dependerá del tamaño de la misma la implantación de cada uno de ellos. Estos se detallan a continuación y se muestran en resumen en la figura 18:

- **Ambiente de control**, el cual marca la pauta del funcionamiento de una organización e influye en la concienciación de sus empleados respecto al control. Es la base de todos los demás componentes del control interno.

- **Evaluación de los riesgos:** consiste en la identificación y el análisis de los riesgos relevantes para la consecución de los objetivos, y sirve de base para determinar cómo han de ser gestionados los riesgos.

- **Actividades de control:** las actividades de control son las políticas y los procedimientos que llevan a cabo las instrucciones de la dirección. Hay actividades de control en toda la organización, a todos los niveles y en todas las funciones; en éstas incluyen aprobaciones, autorizaciones, verificaciones, conciliaciones, y otras.

- **Información y comunicación:** hay que identificar, recopilar y comunicar información pertinente en forma y plazo que permitan cumplir a cada empleado con sus responsabilidades.

- **Supervisión:** los sistemas de control requieren de un proceso que comprueba que se mantiene el adecuado funcionamiento del sistema a lo largo del tiempo; esto se consigue mediante supervisión controlada, evaluaciones periódicas o ambas.

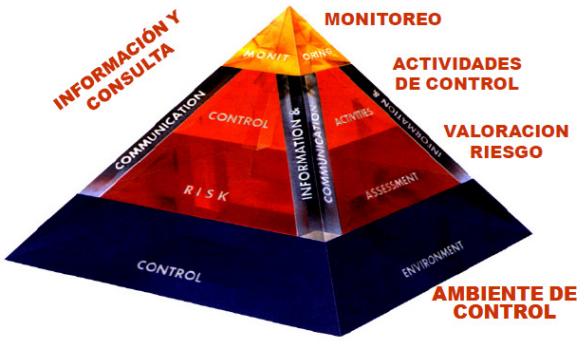


Figura 18. Componentes Informe COSO 1992. Fuente: GIT Ltda.

En lo que respecta a la evaluación de *riesgos*, la dirección de la empresa debe examinar detalladamente los riesgos existentes a todos los niveles de la empresa y tomar las medidas oportunas y poder gestionarlos. De esta manera debe efectuarse la identificación y análisis de los riesgos

relevantes que existen que podrían afectar la consecución de los objetivos. La administración de la empresa debe decidir el nivel de riesgo que considerara aceptable, ya que estos no pueden reducirse a cero.

Identificación de los Riesgos

La identificación de los riesgos debe ser efectuada de la siguiente manera:

- **Nivel de Empresa:** en esta fase se analizan los factores externos e internos que pueden incidir:

  Factores externos:

  - Avances tecnológicos.
  - Necesidades y expectativas de los clientes.
  - La competencia.- provocando cambios en mercadeo y servicios.
  - Nuevas normas y reglamentos.
  - Desastres naturales.
  - Cambios económicos.

  Factores Internos:

  - Averías en los sistemas informáticos.
  - Calidad de los empleados y métodos usados en la empresa para su motivación y formación.
  - Cambios de responsabilidades para los directivos.
  - Naturaleza de las actividades de la entidad.
  - Un comité de auditoría o de administración ineficaz.

La mayoría de los métodos de identificación de riesgos comprenden métodos cualitativos o cuantitativos para establecer el orden de prioridad de las actividades de alto riesgo sobretodo las desarrolladas por auditores externos e internos. Además, los riesgos también pueden ser identificados con las previsiones a corto y a largo plazo, y con la planificación estratégica.

- **Nivel de Actividad:** Los riesgos a este nivel son principalmente enfocados a su evaluación en las unidades o funciones más importantes del negocio como ventas, producción, marketing, etc.

Análisis de los Riesgos

El proceso de análisis incluye:

- Estimar la importancia del riesgo
- Evaluar la probabilidad de que éste se materialice
- Un análisis de cómo ha de gestionarse el riesgo, qué medidas se adoptaran.

La empresa debe tener en cuenta que un riesgo importante y que tiene una alta probabilidad de materializarse requerirá un análisis profundo. Luego de esto se debe estudiar la mejor forma de gestionar estos riesgos, para esto debe hacerse un análisis de los costos en los que se puede incurrir para reducir el riesgo.

La empresa siempre debe tener en cuenta que habrá cierto nivel de riesgo residual, por limitaciones de recursos y otras inherentes al sistema de control interno.

3.2.2.1 COSO II- ERM (ENTERPRISE RISK MANAGEMENT)

El modelo COSO ERM-Framework fue publicado en el año 2004 e introduce nuevos elementos a modelo anterior COSO de 1992/94. Delinea los principios de administración de riesgo, proporcionando dentro de su marco conceptual:

- Una definición de Enterprise Risk Management.
- Los principios y componentes críticos de un efectivo proceso de Enterprise Risk Management.
- Dirección para que las organizaciones lo utilicen en la determinación de cómo mejorar su administración de riesgo.
- Criterio para determinar si su administración de riesgo es efectiva, y si no, que necesita.

Según COSO II-ERM (2004), la gestión de riesgo empresarial (ERM, según sus siglas en inglés), se define como, " un proceso efectuado por el directorio, administración y las personas de la organización, es aplicado desde la definición estratégica hasta las actividades del día a día, diseñado para identificar eventos potenciales que pueden afectar a la organización y administrar los riesgos dentro de su contexto organizacional, a objeto de proveer una seguridad razonable respecto del logro de los objetivos de la organización".

Dentro de lo que es la presentación del ERM se encuentran cinco conceptos claves que sintetizan los aspectos más importantes de este marco de Administración de Riesgos:

- **Gestión de riesgos:** es un proceso, llevado a cabo por el directorio, las gerencias y el resto del personal, destinado a establecer estrategias para toda la entidad, diseñado para identificar eventos potenciales que pudieran afectar a la entidad, y administrar los riesgos

para que estén dentro de los límites de su disposición al riesgo, con el fin de proporcionar una razonable seguridad respecto al logro de los objetivos de la entidad.

- **Eventos y riesgos:** se consideran como hechos importantes, de los cuales no se tiene certeza si ocurrirán, cuando ocurrirán y cuáles serán sus resultados. Cuando estos eventos tienen un impacto negativo, se consideran riesgos, y cuando son positivos, se consideran oportunidades.

- **Apetito al riesgo:** es el nivel de riesgo máximo aceptable. Intuitivamente la cultura de la organización permite saber si es una organización en la cual sus ejecutivos son adversos al riesgo o tomadores de los mismos. Sin embargo, este tema es lo suficientemente importante para que se explicite en una política y se eviten colisiones entre áreas con diverso “apetito” de riesgo.

- **Tolerancia al riesgo:** el nivel de riesgo máximo aceptable debe tener una tolerancia ya que en caso contrario limitaría las decisiones, o se eludiría el nivel máximo en forma arbitraria. La tolerancia al riesgo es el nivel aceptable de desviación en relación con el logro de los objetivos.

- **Portafolio de riesgos:** considera el total de los riesgos individuales de cada unidad de negocio en forma integrada, logrando una visión de riesgo global de la entidad.

Con ERM, se plantea una relación directa entre los objetivos que la entidad desea lograr y los componentes de la gestión de riesgos corporativos, que representan lo que hace falta para lograr aquellos. La

relación se representa con una matriz tridimensional, en forma de cubo, la cual se muestra en la siguiente figura.

Figura 19. Componentes modelo COSO II-ERM 2004. Fuente: GIT Ltda.

Las cuatro categorías de objetivos (estrategia, operaciones, información y conformidad) están representadas por columnas verticales, los ocho componentes lo están por filas horizontales y las unidades de la entidad, por la tercera dimensión del cubo. Los componentes son:

1. **Ambiente Interno**

El ámbito interno al proveer disciplina y estructura, es el fundamento para todos los demás componentes de la ERM.

El ámbito interno influye en la forma como se establecen la estrategia y los objetivos, como se estructuran las actividades de negocios y como se identifican, aprecian y tratan los riesgos. En el diseño y funcionamiento de las actividades de control, los sistemas de información y comunicación y en las actividades de monitoreo.

El ámbito interno comprende entre otros:

- Valores éticos de la entidad.
- Competencia y desarrollo del personal.
- Estilo operativo de la gerencia y la forma como ésta asigna responsabilidad y autoridad.
- Estructura organizativa.
- Políticas y prácticas de recursos humanos.

Como parte del ámbito interno, la gerencia establece una filosofía gerencial del riesgo, establece el nivel de riesgo aceptado, desarrolla una cultura de riesgo e integra ERM con iniciativas relacionadas.

2. Establecimiento de Objetivos

La gerencia establece los objetivos estratégicos, selecciona la estrategia y establece los objetivos relacionados y alineados con la estrategia.

Los objetivos se pueden categorizar en:

- Estratégicos: son aquellos que se relacionan con las metas de alto nivel, y que sustentan y están alineados con la misión de la entidad.
- Referidos a las operaciones: son aquellos que se relacionan con la eficacia y la eficiencia en las operaciones de la entidad.
- Referidos a la elaboración de la información: se relacionan con la eficacia del proceso de elaboración de información.
- Referidos al cumplimiento: son aquellos que se relacionan con el cumplimiento de leyes y regulaciones que afecten a la entidad.

3. Identificación de Eventos

Se deben identificar eventos potenciales que afectan la implementación de la estrategia o el logro de los objetivos, con impacto positivo (oportunidades), negativo (riesgos) o ambos.

Los eventos con un impacto positivo son recanalizados por la Gerencia al establecimiento de la estrategia y de los objetivos.

Los eventos con un impacto negativo representan riesgos, los cuales necesitan ser evaluados y administrados.

Para la identificación de eventos existen diferentes técnicas tales como:

- Inventarios de eventos.
- Análisis de información histórica.
- Análisis de flujos de procesos.
- Indicadores de excepción.
- Entrevistas y cesiones grupales guiadas por facilitadores.

4. Evaluación de Riesgos

Permite a la entidad considerar cómo los eventos potenciales podrían impactar en el logro de los objetivos.

La evaluación de riesgos puede realizarse desde dos perspectivas: probabilidad de ocurrencia e impacto, su metodología comprende una combinación de técnicas cualitativas y cuantitativas.

5. Respuesta al Riesgo

Evaluado el riesgo, la Gerencia identifica y evalúa posibles respuestas al riesgo en relación al nivel máximo aceptable de riesgo de la entidad. Se definen distintas categorías de respuesta al riesgo:

- Evitarlo
- Reducirlo
- Compartirlo
- Aceptarlo

ERM propone que el riesgo sea considerado desde una perspectiva de la entidad en su conjunto o de portafolio de riesgos. Permite desarrollar una visión de portafolio de riesgos tanto a nivel de unidades de negocio como a nivel de entidad, para lo cual es necesario considerar como se relacionan los riesgos individuales.

6. Actividades de Control

Son las políticas y procedimientos necesarios para asegurar que las respuestas al riesgo se lleven a cabo de manera adecuada y oportuna. Estas actividades, se realizan a lo largo de toda la organización, a todos los niveles y en todas las funciones.

Existen distintos tipos de actividades de control: preventivas, detectivas, manuales, computarizadas y controles gerenciales.

7. Información y Comunicación

La información es necesaria en todos los niveles de la organización para identificar, evaluar y dar una respuesta al riesgo. Se debe obtener y

comunicar la información pertinente en tiempo y forma, permitiendo a los miembros de la organización cumplir con sus responsabilidades.

La comunicación se debe realizar en sentido amplio y fluir por la organización en todos los sentidos (ascendente, descendente, paralela). Asimismo debe existir una comunicación adecuada con partes externas a la organización como ser: clientes, proveedores, reguladores y accionistas.

8. Monitoreo

Implica corroborar que el proceso de administración de riesgos mantiene su efectividad a lo largo del tiempo y que todos los componentes del marco ERM funcionan adecuadamente.

El monitoreo puede ser realizado de dos formas o una combinación de ambas:

- *Actividades de monitoreo continuo*, que se llevan a cabo durante el curso normal de las operaciones.
- *Evaluaciones puntuales*, realizadas por personal que no es el responsable directo de la ejecución de las actividades.

Todos los componentes antes mencionados, se resumen en la figura 20:

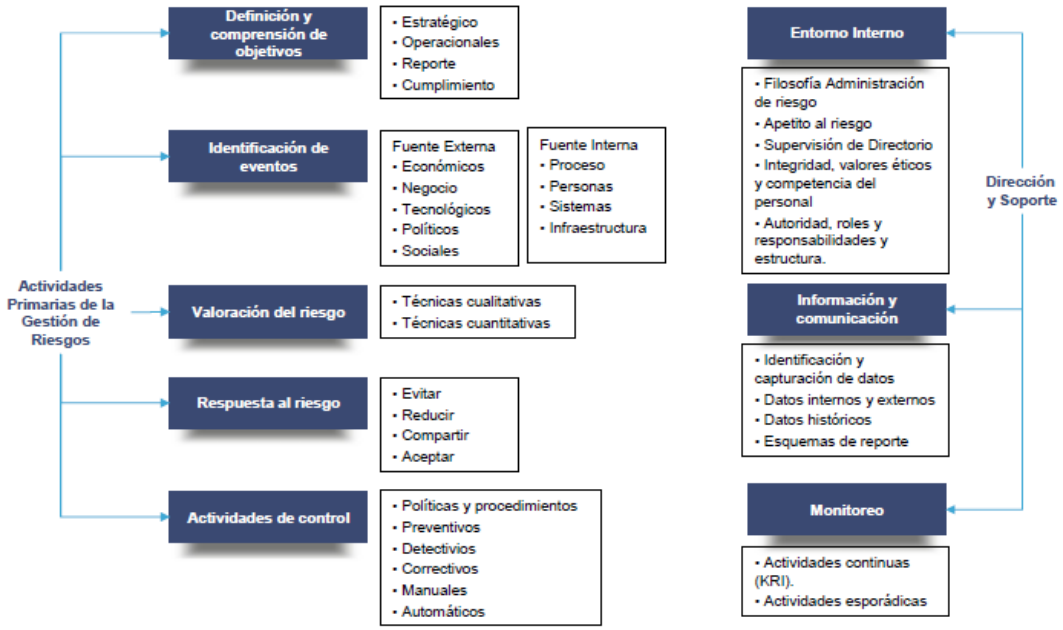


Figura 20. Componentes claves de ERM. Fuente: Rafael Ruano Diez

Una ERM bien diseñada y ejecutada puede proveer a la gerencia y al directorio una seguridad razonable respecto a cada una de las categorías de objetivos de la entidad que están siendo alcanzados: (ver figura 21)

- Objetivos estratégicos.
- Objetivos operativos.
- Elaboración de información confiable.
- Cumpliendo con las leyes y regulaciones aplicables.

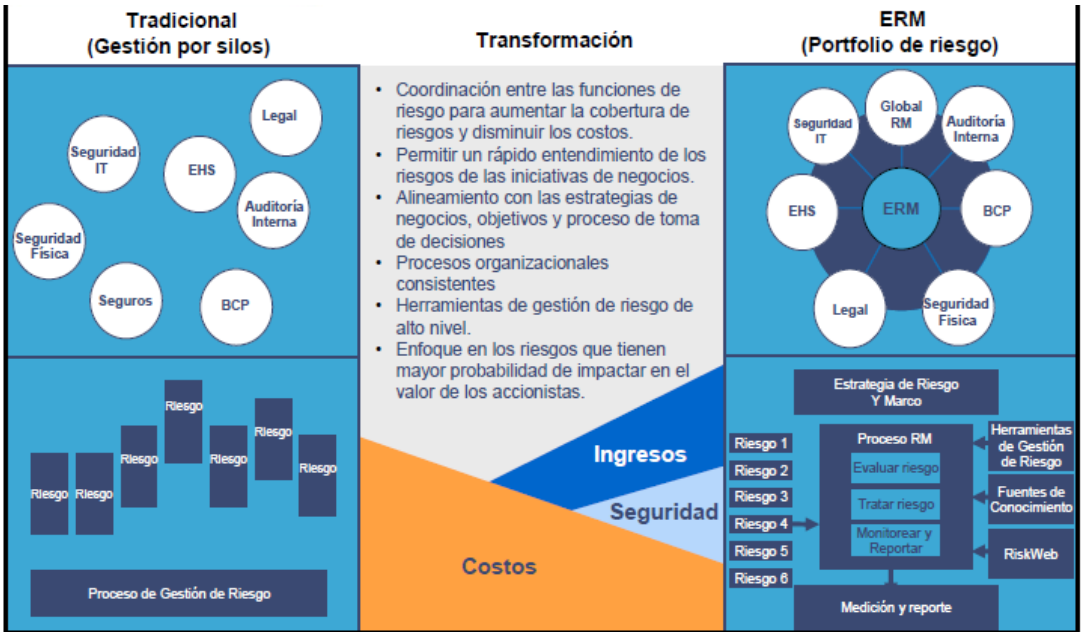


Figura 21. Resultados ERM. Fuente: Rafael Ruano Diez

3.2.3 MODELO COBIT

Modelo para evaluar y/o auditar la función de servicios de información y tecnología relacionada (IT).

Es el resultado de una investigación de más de 4 años y consenso de expertos a nivel mundial, desarrollada por la Information, Systems Audit and Control Association “ISACA”.

El modelo COBIT ha sido aceptado y adoptado por todo tipo de organizaciones y de todo el mundo.

COBIT es un marco para el gobierno de la TI y que permite a gerentes acortar el hueco entre exigencias de control, cuestiones técnicas y riesgos de negocio. COBIT permite el desarrollo de políticas claras y buenas prácticas para el control de TI en las organizaciones. (Isaca.org, 2011).

La orientación a negocios es el tema principal de COBIT. Está diseñado para ser utilizado no solo por proveedores de servicios, usuarios y auditores de TI, sino también y principalmente, como guía integral para la gerencia y para los propietarios de los procesos de negocio.

COBIT define las actividades de TI en un modelo genérico de procesos en cuatro dominios, tal y como se muestra en la figura 22. Estos dominios son Planear y Organizar, Adquirir e Implementar, Entregar y Dar Soporte y Monitorear y Evaluar. Los dominios se equiparan a las áreas tradicionales de TI de planear, construir, ejecutar y monitorear.

Figura 22. Modelo COBIT. Fuente: GIT Ltda.

Para gobernar efectivamente TI, es importante determinar las actividades y los riesgos que requieren ser administrados. Éstos se pueden resumir dentro de COBIT en cuatro dominios:

1. PLANEACION Y ORGANIZACION (PO).

Este dominio cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que TI pueda contribuir de la mejor manera al logro de los objetivos del negocio. Además, la realización de la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, se debe implementar una estructura organizacional y una estructura tecnológica apropiada. Este dominio cubre los siguientes procesos:

1. Definir un Plan estratégico de TI
2. Definir la Arquitectura de Información
3. Determinar la Dirección Tecnológica
4. Definir los procesos, organización y relaciones de TI
5. Administrar la Inversión en TI
6. Comunicar Directrices y expectativas Gerenciales
7. Administrar Recursos Humanos de TI
8. Administrar la Calidad (QA)
9. Evaluar y Administrar los Riesgos de TI
10. Administrar los Proyectos

2. ADQUISICION E IMPLEMENTACIÓN (AI)

Para llevar a cabo la estrategia de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas, así como ser implementadas e integradas en los procesos del negocio. Este dominio también dirige el desarrollo de un plan de mantenimiento que una empresa debería adoptar para prolongar la vida de un sistema TI y sus componentes. Este dominio incluye los siguientes procesos:

1. Identificar soluciones automatizadas

2. Adquirir y mantener software aplicativo
3. Adquirir y mantener la arquitectura tecnológica
4. Facilitar la operación y el uso
5. Adquirir recursos de TI
6. Administrar cambios
7. Instalar y acreditar soluciones y cambios

3. ENTREGA Y SOPORTE (ES)

Este dominio cubre la entrega en sí de los servicios requeridos, lo que incluye la prestación de estos, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operacionales. Los procesos en cuales se basa este dominio son:

1. Definir y administrar niveles de servicio.
2. Administrar servicios de terceros.
3. Administrar el desempeño y capacidad.
4. Garantizar la continuidad del servicio.
5. Garantizar la seguridad de los sistemas.
6. Identificar y asignar costos.
7. Educar y entrenar a los usuarios.
8. Administrar la mesa de servicio y los incidentes.
9. Administrar la configuración.
10. Administrar los problemas.
11. Administrar los datos.
12. Administrar el ambiente físico.
13. Administrar la operación.

4. MONITOREAR Y EVALUAR (ME)

Todos los procesos de TI deben evaluarse de forma regular en el tiempo en cuanto a su calidad y al cumplimiento de los requerimientos de control. Este dominio abarca los siguientes cuatro procesos:

1. Monitorear y evaluar el desempeño de TI.
2. Monitorear y evaluar el control interno.
3. Garantizar el cumplimiento regulatorio.
4. Proporcionar gobierno de TI.

En detalle, el marco de trabajo general COBIT se muestra gráficamente en la figura 23, con el modelo de procesos de COBIT compuesto de cuatro dominios que contienen 34 procesos genéricos, administrando los recursos de TI para proporcionar información al negocio de acuerdo con los requerimientos del negocio y de gobierno.

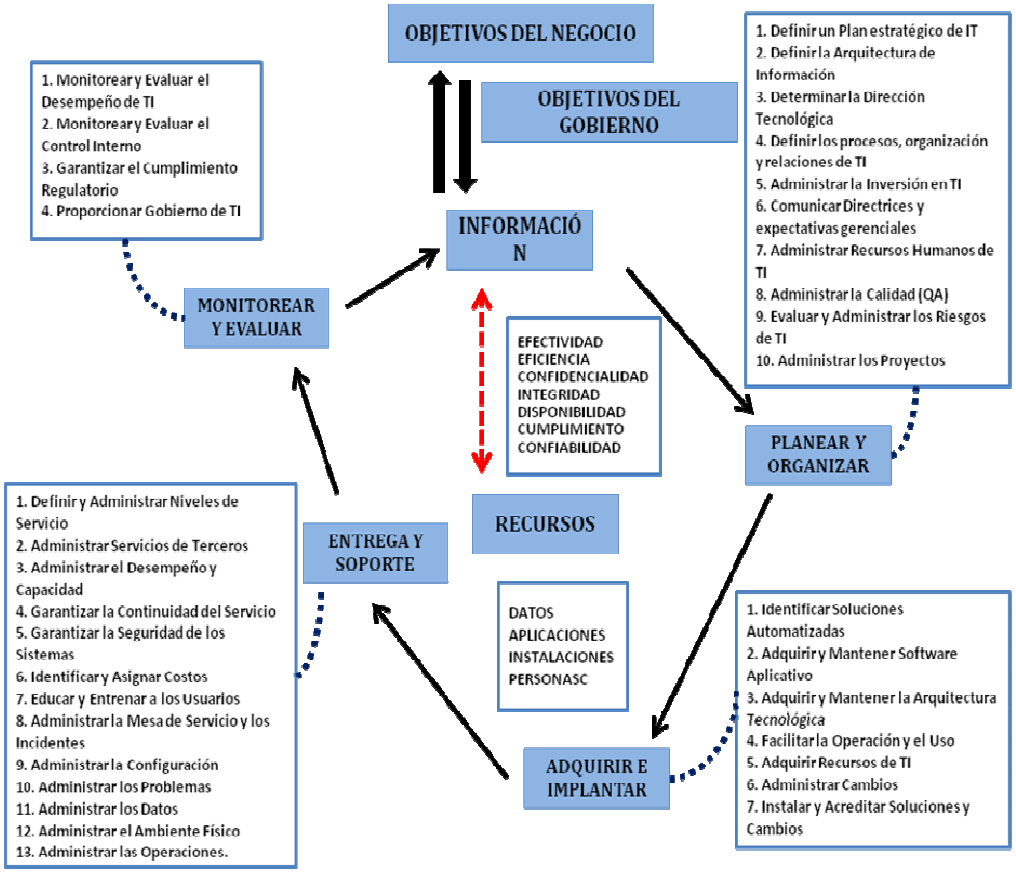


Figura 23. Marco de trabajo general de COBIT. Fuente: Elaboración propia.

Para cada uno de los procesos TI de COBIT, se proporciona un objetivo de control de alto nivel, junto con las metas y métricas clave en forma de cascada (ver figura 24).

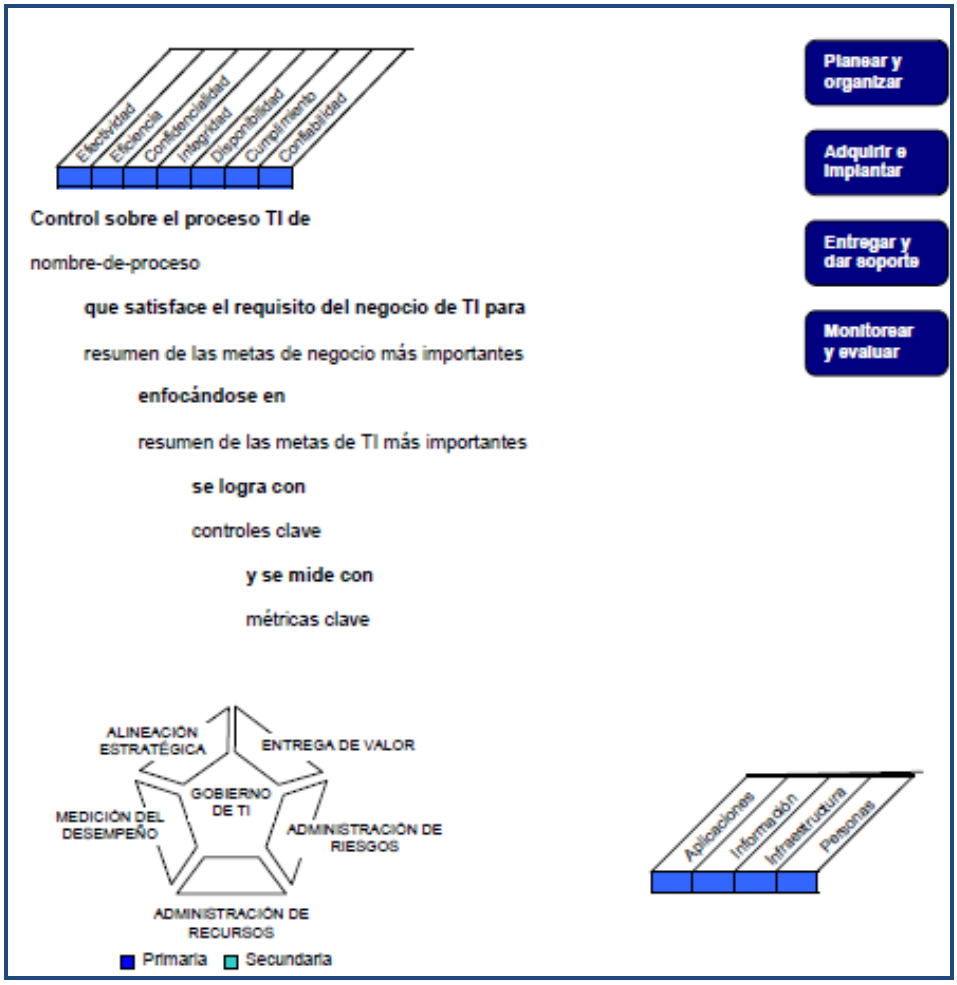


Figura 24. Navegación en COBIT. Fuente: isaca.org

Para el subdominio PO9 Evaluar y administrar los riesgos de TI, el marco de trabajo documenta un nivel común y acordado de riesgos de TI, estrategias de mitigación y riesgos residuales acordados. Cualquier impacto potencial sobre las metas de la organización, causado por algún evento no planeado se debe identificar, analizar y evaluar. Se deben adoptar estrategias de mitigación de riesgos para minimizar los riesgos residuales a un nivel aceptable. El resultado de la evaluación debe ser entendible para los participantes y se debe expresar en términos financieros, para permitir a los participantes alinear los riesgos a un nivel aceptable de tolerancia. (Ver figura 25)

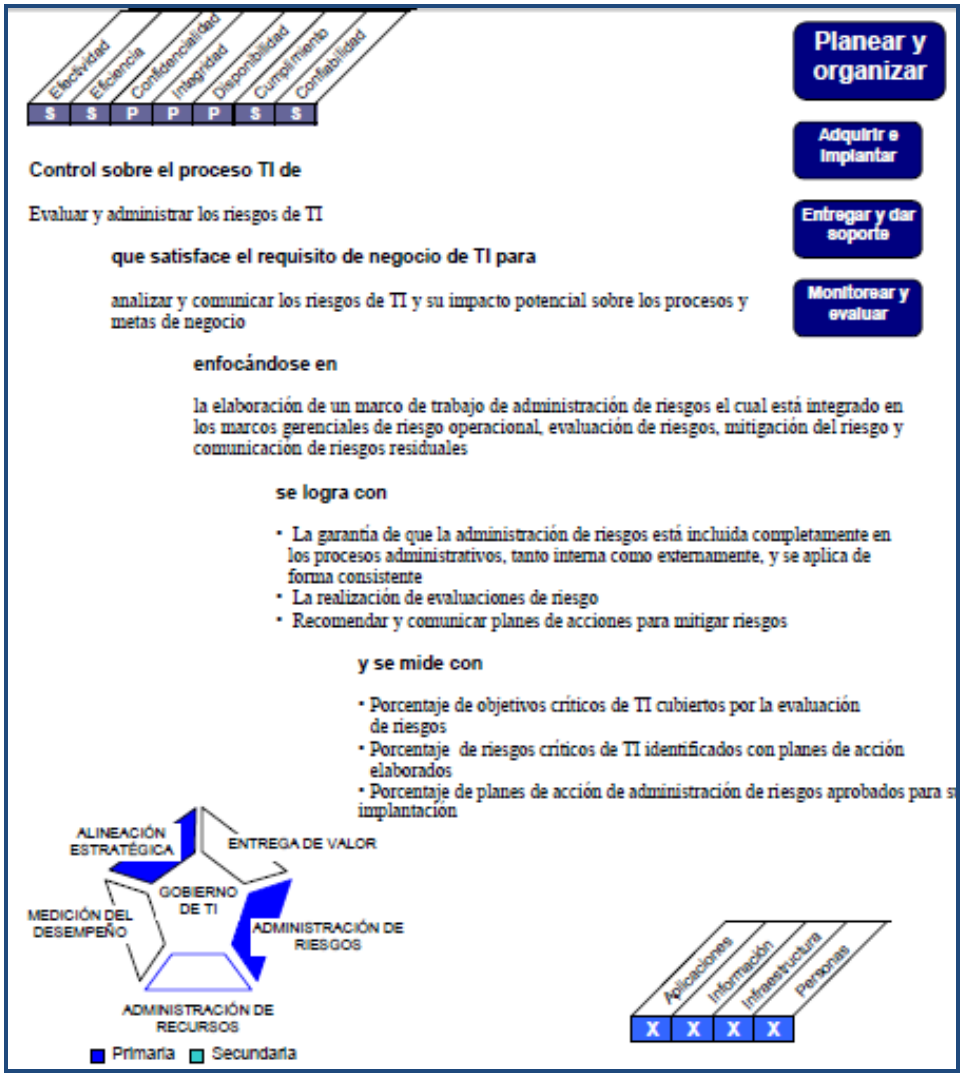


Figura 25. Subdominio PO9 Evaluar y administrar los riesgos de TI.
Fuente: isaca.org

3.2.4 ISO 27000

La ISO (Organización International de Normalización), es el mayor desarrollador mundial y editor de las normas internacionales. La ISO es una red de los institutos de normas nacionales de 162 países, sobre la base de un miembro por país, con una secretaría central en Ginebra (Suiza) que

coordina el sistema. La Organización Internacional de Normalización (ISO), con sede en Ginebra, está compuesta por delegaciones gubernamentales y no gubernamentales subdivididos en una serie de subcomités encargados de desarrollar las guías que contribuirán al mejoramiento ambiental. Su función principal es la de buscar la estandarización de normas de productos y seguridad para las empresas u organizaciones a nivel internacional. (iso.org ,2011).

ISO 27000 provee una base genérica de “código de mejores prácticas” en la administración del riesgo, para implementar y documentar sistemas de Administración de la Seguridad de Tecnología de Información. (GIT Ltda., 2011).

ISO/IEC 27000 es un conjunto de estándares desarrollados por la ISO e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña. (iso.org, 2011).

La ISO ha reservado la serie ISO/IEC 27000 para una gama de normas de gestión de la seguridad de la información (SGSI) de manera similar a lo realizado con las normas de gestión de la calidad, la serie ISO 9000.

La numeración actual de las Normas de la serie ISO/IEC 27000 es la siguiente:

- ISO/IEC 27000: Fundamentos y vocabulario.
- ISO/IEC 27001: Norma que especifica los requisitos para la implantación del Sistema de Gestión de Seguridad de la Información (SGSI). Es la norma más importante de la familia, adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos.
- ISO/IEC 27002: Código de buenas prácticas para la gestión de

Seguridad de la Información.

- ISO/IEC 27003: Directrices para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). Es el soporte de la norma ISO/IEC 27001.
- ISO/IEC 27004: Métricas para la gestión de Seguridad de la Información. Es la que proporciona recomendaciones de quién, cuándo y cómo realizar mediciones de seguridad de la información.
- ISO/IEC 27005: Gestión de riesgos de la Seguridad de la Información. Es la que proporciona recomendaciones y lineamientos de métodos y técnicas de evaluación de riesgos de Seguridad en la Información, en soporte del proceso de gestión de riesgos de la norma ISO/IEC 27001.
- ISO/IEC 27006: Requisitos para la acreditación de las organizaciones que proporcionan la certificación de los sistemas de gestión de la Seguridad de la Información. Esta norma específica requisitos para la certificación de SGSI y es usada en conjunto con la norma 17021-1, la norma genérica de acreditación.

Se utiliza el modelo PDCA (Planificar-Hacer-Verificar-Actuar), para establecer, implementar, monitorear y mejorar el SGSI, tal y como se ilustra en la siguiente imagen:

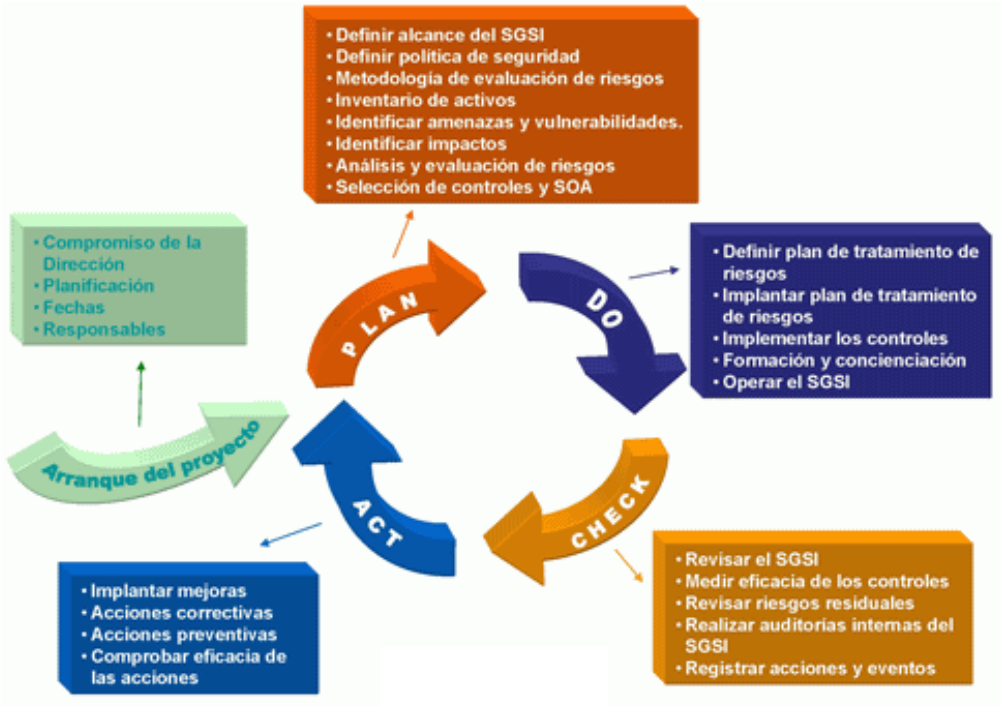


Figura 26. Modelo PDCA ISO 27000. Fuente: ISO27000.es

Dentro del proceso "Planificación" para el análisis de riesgos se tienen las siguientes actividades:

- **Definir el enfoque de evaluación de riesgos:** definir una metodología de evaluación de riesgos apropiada para el SGSI y las necesidades de la organización, desarrollar criterios de aceptación de riesgos y determinar el nivel de riesgo aceptable. Existen muchas metodologías de evaluación de riesgos aceptadas internacionalmente; la organización puede optar por una de ellas, hacer una combinación de varias o crear la suya propia. ISO 27001 no impone ninguna ni da indicaciones de detalle, aunque ISO 27005 sí profundiza en directrices sobre la materia. El riesgo nunca es totalmente eliminable, por lo que es necesario definir una estrategia de aceptación de riesgo.

- **Identificar amenazas y vulnerabilidades:** todas las que afectan a los activos del inventario.

- **Identificar los impactos:** los que podría suponer una pérdida de la confidencialidad, la integridad o la disponibilidad de cada uno de los activos de información.

- **Análisis y evaluación de los riesgos:** evaluar el daño resultante de un fallo de seguridad (es decir, que una amenaza explote una vulnerabilidad) y la probabilidad de ocurrencia del fallo; estimar el nivel de riesgo resultante y determinar si el riesgo es aceptable (en función de los niveles definidos previamente) o requiere tratamiento.

- **Identificar y evaluar opciones para el tratamiento del riesgo:** el riesgo puede ser reducido (mitigado mediante controles), eliminado (p. ej., eliminando el activo), aceptado (de forma consciente) o transferido (p. ej., con un seguro o un contrato de outsourcing).

- **Selección de controles:** seleccionar controles para el tratamiento el riesgo en función de la evaluación anterior. Se debe utilizar para ello los controles del ISO 27001 (teniendo en cuenta que las exclusiones habrán de ser justificadas) y otros controles adicionales si se consideran necesarios.

- **Aprobación por parte de la Dirección del riesgo residual y autorización de implantar el SGSI:** los riesgos de seguridad de la información son riesgos de negocio y sólo la Dirección puede tomar decisiones sobre su aceptación o tratamiento. El riesgo residual es el que queda, aún después de haber aplicado controles (el "riesgo cero" no existe prácticamente en ningún caso).

Dentro del proceso “Hacer” para el análisis de riesgos se tienen las siguientes actividades:

- **Definir plan de tratamiento de riesgos:** que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.
- **Implantar plan de tratamiento de riesgos:** con la meta de alcanzar los objetivos de control identificados.
- **Implementar los controles:** todos los que se seleccionaron en la fase anterior.

Dentro de proceso “Verificar” para el análisis de riesgos se tienen las siguientes actividades:

- **Revisar regularmente la evaluación de riesgos:** los cambios en la organización, tecnología, procesos y objetivos de negocio, amenazas, eficacia de los controles o el entorno tienen una influencia sobre los riesgos evaluados, el riesgo residual y el nivel de riesgo aceptado.

- **Actualizar planes de seguridad:** teniendo en cuenta los resultados de la monitorización y las revisiones.

- **Registrar acciones y eventos que puedan tener impacto en la eficacia o el rendimiento del SGSI:** sirven como evidencia documental de conformidad con los requisitos y uso eficaz del SGSI.

En la figura 27 se ilustra el mapa de análisis de riesgos, aplicando el estándar ISO 27000.

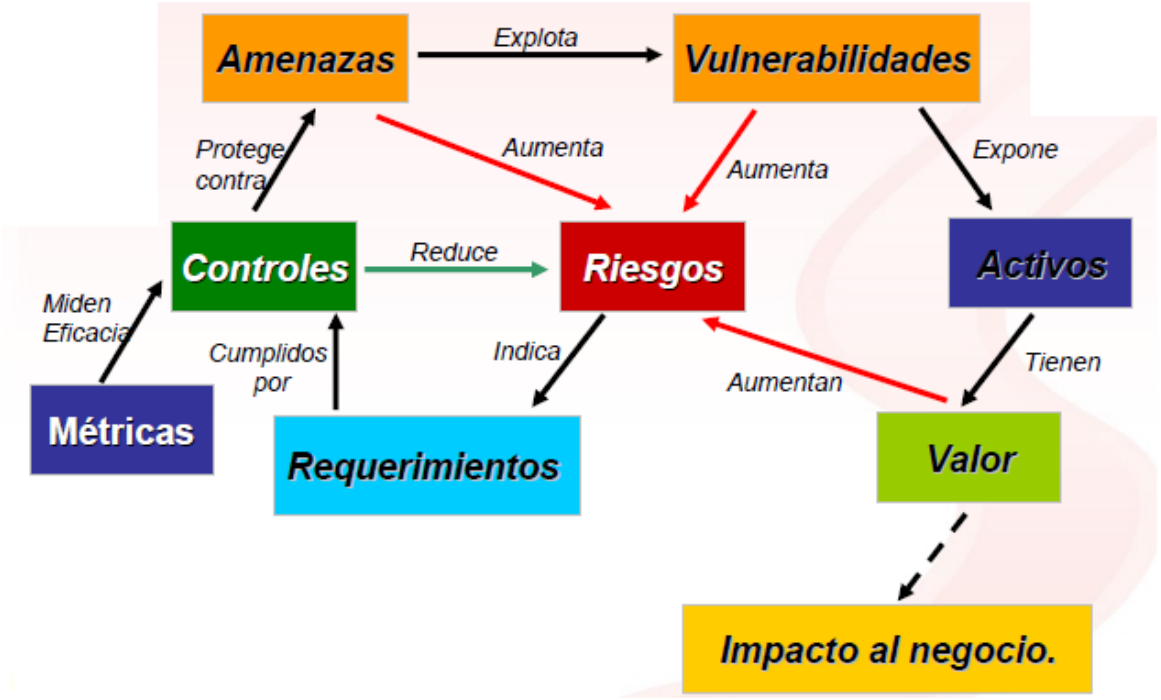


Figura 27. Mapa Análisis de Riesgos ISO 27000.
Fuente: Ing. Reynaldo C. de la Fuente

3.2.5 IIA-THE INSTITUTE OF INTERNAL AUDITORS

El Instituto de Auditores Internos (IIA), es una asociación profesional internacional, establecida en el año de 1941, la cual actualmente cuenta con más de 170.000 miembros. Su sede central se encuentra en Altamonte Springs, Florida, Estados Unidos de Norteamérica. El IIA es reconocido a nivel mundial como el líder de la profesión de la auditoría interna en aspectos tales como la certificación profesional de los auditores internos, así como en educación, investigación y dirección tecnológica en los temas de auditoría interna, control, gestión de riesgos y gobierno. (theiia.org, 2011).

La auditoría interna es una actividad independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de una organización. Ayuda a una organización a cumplir sus objetivos aportando un enfoque sistemático y disciplinario para evaluar y

mejorara la efectividad de los procesos de gestión de riesgos, control y gobierno. (fccpv.org, 2011).

Según el IIA, el riego se define como “la posibilidad de que ocurra un evento que tendrá un impacto en el logro de los objetivos, el cual es medido en términos de impacto y probabilidad”.

La actividad de auditoría interna esta referenciada por la guía 2120 del IIA, a través de la cual se debe evaluar la eficacia y contribuir a la mejora de los procesos de gestión de riesgos. La auditoría interna provee aseguramiento normalmente en tres áreas:

- Procesos de gestión de riesgos, tanto en su diseño y como qué tan bien están trabajando.
- Gestión de aquellos riesgos clasificados como “claves”, incluyendo efectividad de los controles y otras respuestas a éstos.
- Confiabilidad y evaluaciones apropiadas de riesgos y reportes de riesgo y estatus de controles.

La actividad de auditoría interna puede recopilar la información para apoyar esta evaluación durante múltiples compromisos. Los resultados de estos compromisos, cuando se ven en conjunto, proporcionan una comprensión de los procesos de la organización de gestión del riesgo y su eficacia.

Los procesos de gestión de riesgos son monitoreados a través de las actividades de gestión en curso, evaluaciones separadas, o ambas cosas. En este sentido existen las siguientes divisiones de la guía 2120 para la gestión de riesgo, en las cuales se aplican los siguientes:

- **2120. A1**. La actividad de auditoría interna debe evaluar la exposición a riesgos relacionados con la gobernanza de la organización, operaciones y sistemas de información con respecto a la:
    - La fiabilidad y la integridad de la información financiera y operativa.
    - Eficacia y eficiencia de las operaciones y programas.
    - Salvaguarda de los activos.
    - Cumplimiento de las leyes, reglamentos, políticas, procedimientos y contratos.

- **2120. A2.** La actividad de auditoría interna debe evaluar el potencial para la ocurrencia de fraude y cómo la organización gestiona el riesgo de fraude.

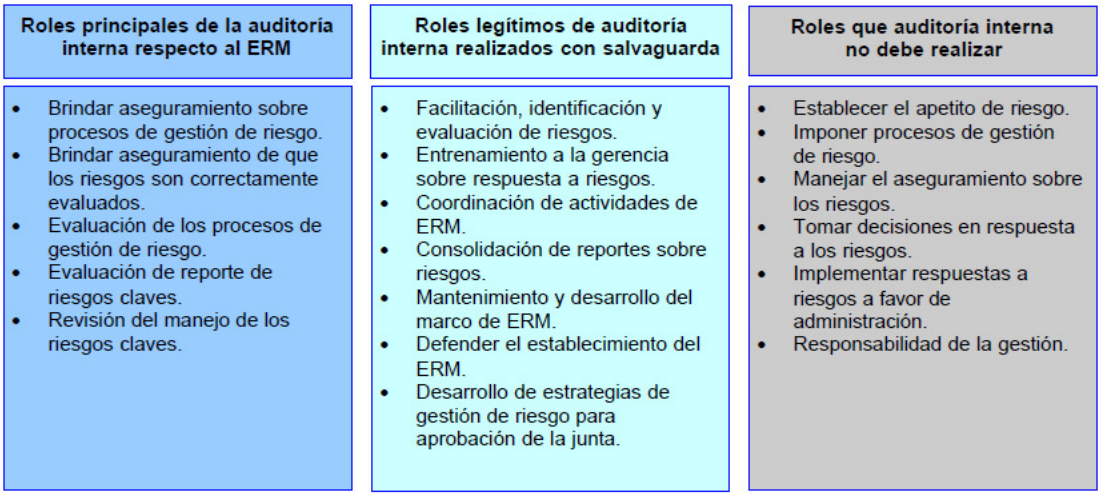
- **2120. C1.** Durante los trabajos de consultoría, los auditores internos deben considerar el riesgo compatible con los objetivos del trabajo y estar alertas a la existencia de otros riesgos significativos.

- **2120. C2**. Los auditores internos deben incorporar el conocimiento de los riesgos de la consulta de los compromisos adquirido en su evaluación de los procesos de la organización de gestión de riesgos.

- **2120. C3.** Al ayudar a la administración en el establecimiento o mejora de los procesos de gestión de riesgos, los auditores internos deben abstenerse de asumir ninguna responsabilidad por la gestión realmente la gestión de riesgos.

La auditoría interna es una actividad independiente, objetiva de aseguramiento y consulta. Su rol principal con relación al ERM (Enterprise Risk Management) definido por el COSO, es proveer aseguramiento objetivo

a la junta sobre la efectividad de la gestión de riesgo. En la figura 28, se presenta el rango de las actividades de ERM e indica cuales roles una función de auditoría interna profesional debe hacer e, igualmente importante que no debe realizar.



Roles principales de la auditoría interna respecto al ERM	Roles legítimos de auditoría interna realizados con salvaguarda	Roles que auditoría interna no debe realizar
• Brindar aseguramiento sobre procesos de gestión de riesgo. • Brindar aseguramiento de que los riesgos son correctamente evaluados. • Evaluación de los procesos de gestión de riesgo. • Evaluación de reporte de riesgos claves. • Revisión del manejo de los riesgos claves.	• Facilitación, identificación y evaluación de riesgos. • Entrenamiento a la gerencia sobre respuesta a riesgos. • Coordinación de actividades de ERM. • Consolidación de reportes sobre riesgos. • Mantenimiento y desarrollo del marco de ERM. • Defender el establecimiento del ERM. • Desarrollo de estrategias de gestión de riesgo para aprobación de la junta.	• Establecer el apetito de riesgo. • Imponer procesos de gestión de riesgo. • Manejar el aseguramiento sobre los riesgos. • Tomar decisiones en respuesta a los riesgos. • Implementar respuestas a riesgos a favor de administración. • Responsabilidad de la gestión.

Figura 28. Rol de Auditoría Interna en el ERM. Fuente: http://www.theiia.org

Las actividades de la izquierda de la figura 28, son todas las relacionadas al aseguramiento. Ellas forman parte del objetivo amplio de dar aseguramiento sobre la gestión de riesgo. Una función de auditoría interna cumpliendo con las normas para el ejercicio profesional de la auditoría interna puede y debe realizar por los menos algunas de estas actividades.

Cuando incrementa la madurez de riesgo en la organización y la gestión de riesgo se encaja más en las operaciones del negocio, el rol de auditoría interna de defensor de ERM se puede reducir. Similarmente, si la organización emplea los servicios de un especialista o posee una función de gestión de riesgo, auditoría interna podría agregar mayor valor a través de concentrarse en su rol de aseguramiento, en vez de realizar mayores actividades de consultoría.

El centro de la figura 28, presenta el rol de consultoría que la auditoría interna puede realizar en relación con el ERM. En general, mientras más a la derecha del cuadro se aventure el auditor, mayores deben de ser los salvaguardadas que son requeridos para asegurarse que la objetividad e independencia son consideradas.

En el caso de ERM, la auditoría interna puede proveer servicios de consultoría mientras no tenga rol, actualmente, en la gestión de riesgos esa es una responsabilidad de la gerencia. Cada vez que auditoría interna actúe ayudando al equipo gerencial en el establecimiento y mejora de los procesos de gestión de riesgo, su plan de trabajo debe incluir una estrategia clara y un tiempo asignado para transferir la responsabilidad de estas actividades a los miembros del equipo gerencial.

La auditoría interna puede ampliar su participación en el ERM, como se muestra en la figura 28, aplicando ciertas condiciones. Estas condiciones son:

- Debe estar claro que la gerencia mantiene la responsabilidad de la gestión de riesgo.
- La naturaleza de la responsabilidad de auditoría interna debe ser documentada en los estatutos de auditoría y aprobado por el Comité de Auditoría.
- Auditoría interna no debe gestionar ningún riesgo a favor de la gerencia.
- Auditoría interna debe proveer consejo, motivar y soportar las decisiones realizada por la dirección, en vez de tomar decisiones de riesgo por ellos mismos.
- Auditoría interna tampoco puede brindar aseguramiento objetivo en ninguna parte del marco de ERM de la cual es responsable.

3.2.6 BASILEA:

El Comité de Supervisión Bancaria de Basilea constituye un foro para la cooperación regular en materia de supervisión bancaria. Su objetivo es mejorar la calidad de la supervisión bancaria en todo el mundo. Se trata de hacerlo mediante el intercambio de información sobre los problemas nacionales de supervisión, enfoques y técnicas, con el fin de promover un entendimiento común. En ocasiones, la comisión recurre a este entendimiento común de elaborar directrices y normas de supervisión en las zonas donde se consideran deseables. En este sentido, el comité es el más conocido por sus altos estándares internacionales sobre la suficiencia de capital, los principios básicos para una supervisión bancaria efectiva, y el concordato en la supervisión bancaria transfronteriza. (bis.org, 2011).

El Comité de Supervisión Bancaria de Basilea (el Comité) reconoce que el método concreto para la gestión de riesgos operativos que elija cada banco dependerá de una serie de factores, como son su tamaño y sofisticación así como la naturaleza y complejidad de sus actividades. Sin embargo, a pesar de estas diferencias, son muchos y variados los elementos fundamentales para una gestión adecuada de estos riesgos, sea cual sea el tamaño y ámbito de actuación del banco; a saber, estrategias claramente definidas y seguimiento de las mismas por parte del consejo de administración y de la alta gerencia, una sólida cultura de gestión del riesgo operativo y de control interno (como pueden ser unas líneas inequívocas de responsabilidad y la segregación de funciones), herramientas eficaces para la transmisión interna de información y planes de contingencia. El comité estima por lo tanto que los principios aquí recogidos ofrecen a todos los bancos las pautas para desarrollar unas buenas prácticas. (Comité de Supervisión Bancaria de Basilea, 2003).

El comité estructura el informe “Buenas prácticas para la gestión y supervisión del riesgo operativo” descrito en el anexo 1, en torno a una serie de principios, en los cuales se agrupan:

- Desarrollo de un marco adecuado para la gestión del riesgo.
- Gestión del riesgo: identificación, evaluación, seguimiento y cobertura/control.
- La función de los supervisores.
- La función de la divulgación de información.

El Comité de Basilea, define las siguientes categorías de eventos de pérdida para la identificación de riesgos, los cuales se encuentran detallados en el anexo 2:

- Fraude interno
- Fraude externo
- Relaciones laborales y seguridad en el puesto de trabajo
- Ejecución, entrega y gestión de procesos
- Daños a activos materiales
- Incidencias en el negocio y fallos en los sistemas
- Fraude Interno

3.2.7 AS/NZS: 4360

El Estándar de Australia y Nueva Zelanda AS/NZS 4360, es genérico y aplicable en cualquier tipo de organización sin importar el sector, naturaleza o tamaño; esta norma es consistente o apoya otros modelos y normas mundiales o locales relativas a la gestión del riesgo y el control, tales como el modelo COSO, COBIT, entre otros.

El estándar AS/NZS 4360, para Administración del Riesgo provee una guía general para el establecimiento y la implantación de procesos de

administración del riesgo, que dentro de su contexto involucra: identificación, análisis, evaluación, tratamiento, comunicación y monitoreo sobre los riesgos. (standards.co.nz (2011).

La administración del riesgo, es un término aplicado a un método lógico y sistemático que establece el contexto, identificación, análisis, evaluación, tratamiento, monitoreo y comunicación sobre los riesgos asociados con una determinada actividad, función o proceso, con el fin de capacitar a las organizaciones para minimizar sus pérdidas y maximizar sus oportunidades. Administración del riesgo está orientada a identificar y aprovechar las oportunidades y/o reducir las pérdidas.

En la figura 29, se ilustra lo mencionado anteriormente en cuanto a los elementos que conforman la administración de riesgos aplicando el estándar AS/NZS 4360.

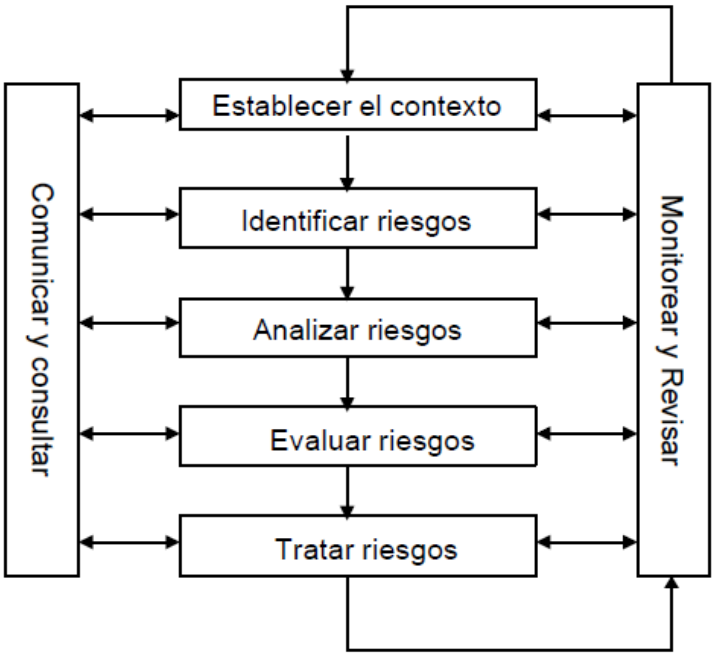


Figura 29. Elementos Administración de Riesgos AS/NZS: 4360.
Fuente: www.standards.co.nz

Este estándar puede ser aplicado a la totalidad de escenarios en el ciclo de vida de una actividad, funciones, proyectos, productos u oportunidades. El mayor beneficio es generalmente obtenido por los procesos de administración del riesgo desde su inicio. Frecuentemente un número de diferentes estudios están fuera de curso sobre diferentes escenarios de un proyecto.

Los elementos principales que conforman el proceso de administración del riesgo, que se muestran en la figura 29, son los siguientes:

3.2.7.1 Establecer el Contexto

Establecer el contexto estratégico, organizacional y de la administración del riesgo, dentro del cual el resto de procesos tienen lugar. Deben establecerse criterios contra los cuales el riesgo debe ser evaluado y definir la estructura del análisis.

Define las relaciones entre la organización y su medio ambiente, identificando las fortalezas, debilidades, oportunidades y amenazas de la organización. Este contexto incluye los aspectos financieros, operativos, competitivos, político (percepción imagen ante el público), sociedad, clientes, cultural y aspectos legales de las funciones de la organización.

Identificar los stakeholders internos y externos, es decir, las personas y las organizaciones quienes pueden ser afectadas, son afectadas por, o percibe que ellos mismos pueden ser afectados por una decisión o actividad y considerar sus objetivos. En la figura 30, se muestra un resumen de los stakeholders internos y externos que pueden ser considerados.

Figura 30. Stakeholders internos y externos. Fuente: GIT Ltda.

En resumen, se debe determinar el alcance y los límites en los cuales se aplicará el proceso para la administración del riesgo, lo cual incluye:

a) Definir el proyecto o actividad y establecer sus metas y objetivos.
b) Definir el alcance del proyecto, el tiempo asociado y su ubicación.
c) Identificar los estudios necesarios y su alcance, objetivos y recursos requeridos. Las fuentes genéricas del riesgo y las áreas de impacto puede servir de guía para esto.
d) Definir la extensión y comprensión de las actividades de administración del riesgo a ser ejecutadas.

3.2.7.2 Identificación del riesgo

Identificar qué, cómo y porqué se pueden originar los hechos como base para posterior análisis. El propósito es generar una lista que contenga todos los eventos que puedan afectar la actividad o proyecto objeto de estudio.

Aproximaciones usadas para identificar riesgos incluyen: listas de chequeo, juicios basados en la experiencia y registros, flujo gramas, tormenta de ideas, análisis de sistemas, análisis del escenario y técnicas de ingeniería de sistemas.

El acercamiento utilizado dependerá de la naturaleza de la actividad bajo revisión y de los tipos de riesgo.

3.2.7.3 Análisis de los riesgos

El objetivo del análisis es separar los riesgos menores aceptables de los más representativos, y proveer información para asesorar la evaluación y tratamiento de los mismos. El análisis involucra la consideración de las fuentes del riesgo, sus consecuencias y la probabilidad de que estas consecuencias puedan ocurrir. Factores que afectan las consecuencias y la probabilidad de ocurrencia deben ser identificados.

Consecuencia y probabilidad son combinadas para determinar el nivel del riesgo. La consecuencia y la probabilidad pueden ser determinadas mediante análisis estadísticos y cálculos. Alternativamente, cuando no hay datos históricos disponibles, pueden realizarse estimativos subjetivos que reflejen opiniones individuales o de grupo sobre el convencimiento de que un posible hecho o pérdida pueda ocurrir.

Para evitar bases subjetivas lo mejor es basarse en fuentes de información y técnicas disponibles para el análisis de la consecuencia y probabilidad. Como fuentes de información pueden incluirse las siguientes:

a) Registros históricos.
b) Experiencias significativas.
c) Práctica de la industria y experiencia.

d) Literatura publicada relevante.
e) Pruebas de mercadeo e investigación de mercados.
f) Experimentos y prototipos.
g) Modelos de economía, ingeniería y otros.
h) Opiniones de especialistas y expertos.

Técnicas incluidas

i) Entrevistas estructuradas con expertos en el área de interés.
ii) Conformar equipos multidisciplinarios de expertos.
iii) Evaluaciones individuales usando cuestionarios.
iv) Usar el computador y otros modelamientos.
v) Usar árboles de fallas y árboles de eventos.

El análisis del riesgo debe emprender diferentes grados de refinamiento, dependiendo de la información del riesgo y la disponibilidad de datos. El análisis puede ser cualitativo, semi-cuantitativo, cuantitativo o una combinación de estos, dependiendo de las circunstancias. En detalle, los tipos de análisis son los siguientes:

a. **Análisis cualitativo:** utiliza formas descriptivas para presentar la magnitud de consecuencias potenciales y la posibilidad de que estas se presenten. Estas escalas pueden ser adaptadas o ajustadas a las circunstancias, y diferentes descripciones se pueden usar para diferentes riesgos.

b. **Análisis semi-cuantitativo:** En este análisis a las escalas cualitativas, como las descritas anteriormente, le son asignados valores. El número asignado a cada descripción no tienen que tener una relación exacta frente a la magnitud actual de la

consecuencia o probabilidad. Los números pueden ser combinados en cualquier rango de fórmulas. El ordenamiento admite que existan posibles cambios dependiendo del sistema de evaluación utilizado y la forma de asignar el orden a los mismos. El objetivo es producir una mejor priorización de la que se obtiene del análisis cualitativo pero no tan preciso como un análisis cuantitativo.

c. **Análisis Cuantitativo:** El análisis cuantitativo utiliza valores numéricos (más que escalas descriptivas que se utilizan en análisis cualitativos y semi-cuantitativos) para expresar las consecuencias y probabilidad utilizando datos de diversos orígenes.

Las consecuencias pueden ser estimadas por modelamiento de las pérdidas de un evento o grupo de eventos, o por extrapolación de estudios experimentales o datos históricos.

3.2.7.4 Evaluación del Riesgos

Comparar el nivel estimado del riesgo contra un criterio preestablecido. Esto permite clasificar los riesgos así como también las prioridades para su administración. Si el nivel establecido del riesgo es bajo, entonces el riesgo se puede considerar dentro de una categoría aceptable y tratarlo puede ser no necesario.

El resultado de la evaluación del riesgo es la lista de priorización de los riesgos para futuras acciones. Las decisiones deberán establecerse tomando en cuenta el amplio contexto del riesgo e incluyendo

consideraciones de la tolerabilidad del riesgo soportado por las partes, más que los beneficios que la organización obtiene de ellos.

Si el riesgo resultante es considerado bajo o aceptable, este debe ser aceptado con un mínimo tratamiento futuro. Este tipo de riesgos deben ser monitoreados y periódicamente revisados para asegurar que ellos se mantienen en niveles aceptables.

3.2.7.5 Tratamiento del riesgo

Se debe aceptar y monitorear los riesgos de baja prioridad, y para los que no cumplan esta condición, se debe desarrollar e implantar un plan específico de administración el cual involucra consideraciones sobre la inversión requerida. La figura 31 ilustra el proceso para el tratamiento del riesgo.

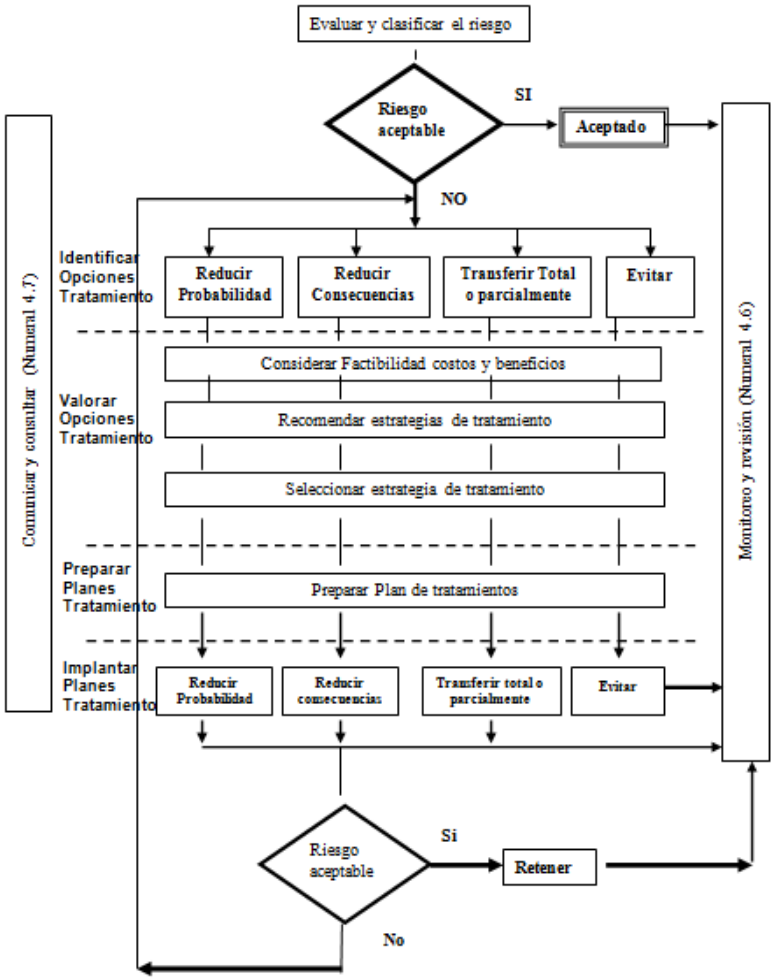


Figura 31. Proceso de tratamiento del riesgo AS/NZS: 4360. Fuente: www.standards.co.nz

Las opciones deben ser valoradas teniendo en cuenta que tanto logran la reducción del riesgo, y el alcance de cualquier beneficio adicional o creación de oportunidades. Seleccionar la opción más apropiada involucra balancear el costo de implantación de cada opción contra el benefició derivado de la misma. En general, el costo de administrar un riesgo debe ser medido conjuntamente con el beneficio a obtener.

Cuando se puede obtener una reducción significativa del riesgo con un relativo bajo costo, tal opción debe ser implantada. Las opciones que más

se alejen de la anterior pueden resultar no económicas y se hace necesario hacer el ejercicio de determinar si tales opciones se justifican. Esto es ilustrado en la figura 32.

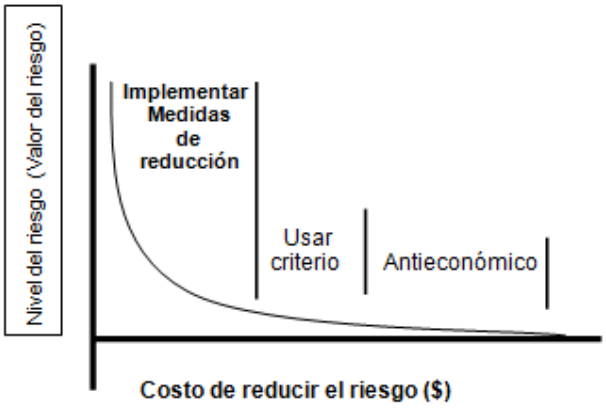


Figura 32. Costo de las medidas de reducción del riesgo.
Fuente: www.standards.co.nz

Cuando el costo acumulado para implementar todos los tratamientos del riesgo, excede el presupuesto disponible, el plan deberá identificar claramente el orden de prioridades en el que los tratamientos deben ser implementados, el cual puede establecerse mediante el uso de varias técnicas, incluida la clasificación de riesgos (ranking) y análisis de costo beneficio. Los tratamientos de los riesgos que no pueden ser implementados dentro de los límites del presupuesto disponible, deben esperar la disponibilidad de recursos financieros futuros o, si por alguna razón uno o todos los tratamientos pendientes se consideran urgentes, deben iniciarse acciones para asegurar el financiamiento adicional.

3.2.7.6 Monitoreo y revisión

Es necesario monitorear los riesgos, la efectividad del plan de tratamiento del riesgo, estrategias y el sistema gerencial establecido para controlar la implementación. Las revisiones continuas son esenciales para

asegurar que el plan de tratamiento permanezca consistente con la realidad.

3.2.7.7 Comunicación y consulta.

La comunicación y consulta es una consideración importante en cada paso del proceso de administración del riesgo. Es importante desarrollar, en los inicios del proceso, un plan de comunicación tanto con los stakeholders internos como externos. El plan debe considerar aspectos relativos al riesgo en sí mismo como al proceso de administrarlo.

Una comunicación interna y externa efectiva, es importante para asegurar que los responsables por implementar la administración del riesgo y aquellos interesados o afectados, han entendido las bases con las cuáles las decisiones se han tomado y el por qué de las acciones particulares requeridas (transparencia).

3.2.8 ISO 31000

La ISO 31000:2009- Gestión del riesgo. Principios y directrices, emitida por la Organización Internacional de Normalización (ISO), proporciona instrucciones sobre cómo establecer y mantener un marco de gestión de riesgos de carácter oficial que puede ser adoptada por cualquier organización. Aunque esta norma proporciona directrices genéricas, no es su intención promover la uniformidad de la gestión de riesgo a través de las compañías, ya que, se entiende que el diseño y ejecución de un modelo de gestión de riesgos y los marcos de referencia deben tener en cuenta las diversas necesidades de una organización específica, sus objetivos estratégicos particulares, el contexto, estructura, volumen de operaciones, procesos, funciones, proyectos, productos, servicios o activos específicos y las prácticas empleadas.

En principio, este estándar ofrece una nueva definición para la práctica de riesgo operacional en el mundo de las organizaciones como: El efecto de la incertidumbre sobre los objetivos. La importancia de dicha definición estriba en que ahora no puede ser vista la gerencia de riesgos como un tema de una unidad especializada de la organización; sino de toda la organización.

La ISO 31000:2009 ha incorporado conceptos adicionales al estándar Australiano Neozelandés AS/NZS 4360:2004 y entre sus principios más importantes se encuentran los siguientes:

- Define el riesgo como un efecto de incertidumbre en el logro de los objetivos.
- Los principios que recomienda a seguir por las organizaciones son más explícitos que su antecesor AS/NZS 4360:2004.
- Aconseja integrar en forma explícita el mejoramiento continuo de la estructura de administración de riesgo.
- Incorpora la necesidad de contar con la integración de elementos principalmente como: gobierno, estrategia y planificación, políticas, valores y la cultura de la organización.

Figura 33. Procesos de gestión de riesgos de la ISO 31000. Fuente: GIT Ltda.

En la figura 33, se muestran las fases que componen este modelo, las cuales se describen a continuación:

- **Establecimiento del Contexto:** establecer los contextos estratégico, organizacional y de gestión en los cuales tendrá lugar el proceso de gestión de riesgos. Deben establecerse los criterios contra los cuales se evaluarán los riesgos y definirse la estructura de análisis, los roles y responsabilidades.

- **Identificación de Riesgos y Oportunidades**: identificar los riesgos que podrían impedir, degradar o demorar el cumplimiento de los objetivos estratégicos y operativos de la organización, así como las oportunidades que puedan contribuir al logro de los referidos objetivos.

- **Análisis de Riesgos:** el análisis debería considerar el rango de consecuencias potenciales y cuán probable es que los riesgos puedan ocurrir. Consecuencia y probabilidad se combinan para producir un nivel estimado de riesgo según la definición de la organización. Adicionalmente se debe identificar y analizar los controles mitigantes existentes.

- **Evaluación de Riesgos**: comparar los niveles de riesgo encontrados contra los criterios de riesgo preestablecidos (si es que han sido establecidos por la dirección) considerando el balance entre beneficios potenciales y resultados adversos. Ordenar y priorizar mediante un ranking los riesgos analizados.

- **Tratamiento de Riesgos:** de acuerdo al ranking de riesgos y al nivel de riesgo preestablecido por la organización (si es que ha sido establecido por la dirección), definir su tratamiento y/o monitoreo, desarrollando e implementando estrategias y planes de acción específicos, que mantengan el riesgo dentro de los niveles aceptados por la organización.

- **Monitoreo y Revisión**: definir y utilizar mecanismos para monitorear y revisar el desempeño del proceso de gestión de riesgos y dar cuenta de la evolución del nivel del riesgo en procesos críticos para la administración.

- **Comunicación y Consulta:** definir y utilizar mecanismos para comunicar y consultar con los interesados internos y externos, según resulte apropiado en cada etapa del proceso de gestión de riesgos. Dichos mecanismos deben permitir a las autoridades tomar decisiones en forma oportuna respecto de

los riesgos con mayores desviaciones en relación a los niveles aceptado.

A diferencia de otras ISO, la ISO 31000:2009, no exige certificación, pero pretende que la norma sea utilizada para armonizar los procesos de gestión de riesgos con las normas existentes y futuras. Además, proporciona un enfoque común en favor de otras normativas que tratan sobre riesgos específicos y/o sectores, y no las sustituyen. En cuanto a los beneficios, éstos se relacionan principalmente a:

- incrementar la probabilidad de alcanzar los objetivos de la organización.
- lograr prácticas de administración de riesgo compatibles entre organizaciones y naciones.
- cumplir con requerimientos legales, regulatorios y normas internacionales.
- mejorar la confianza y credibilidad de los stakeholders.
- establecer una base confiable para la toma de decisiones y la planificación.
- realizar una asignación y uso de recursos efectiva para la implementación de los planes de acción para la mitigación de los riesgos.
- mejorar la prevención de pérdidas y disminuir la probabilidad de ocurrencia de incidentes a nivel de la administración.

El estándar ISO 31000 acoge prácticamente todo el AS/NZ4360; adicionalmente, incorpora once (11) principios clave, en los cuales, se recomienda, por la novedad que imprime a un estándar de riesgos, revisar con detalle cinco (5) de ellos, enunciados a continuación:

- Principio I: La Gerencia de Riesgos crea y protege valor.
- Principio II: La Gerencia de Riesgos es parte integral de los procesos de la organización.
- Principio III: La Gerencia de Riesgos es parte de la toma de decisiones.
- Principio V: La Gerencia de Riesgos es sistemática, estructurada y oportuna.
- Principio XI: La Gerencia de Riesgos facilita el mejoramiento continuo de la organización.

En la figura siguiente, se muestra la visión general de ISO 31000, con los onces (11) principios antes mencionados.

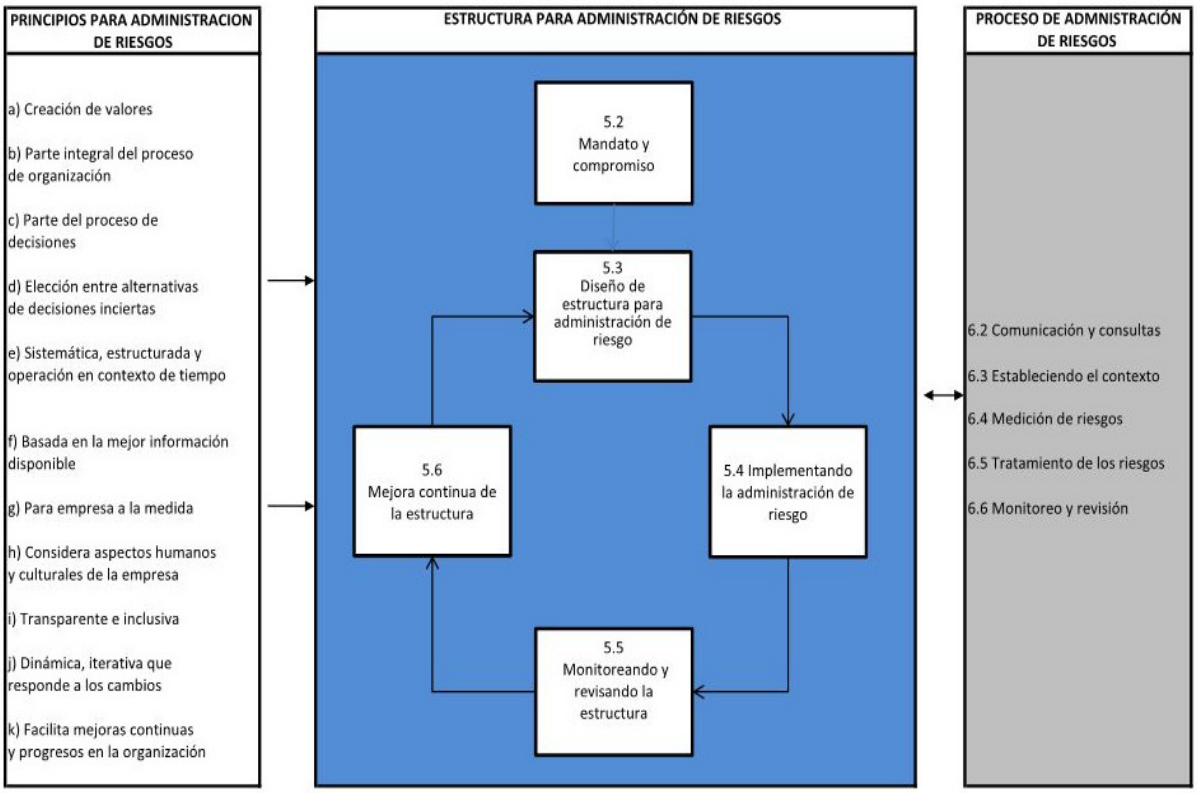


Figura 34. Visión general de ISO 31000. Fuente: ISO 31000.

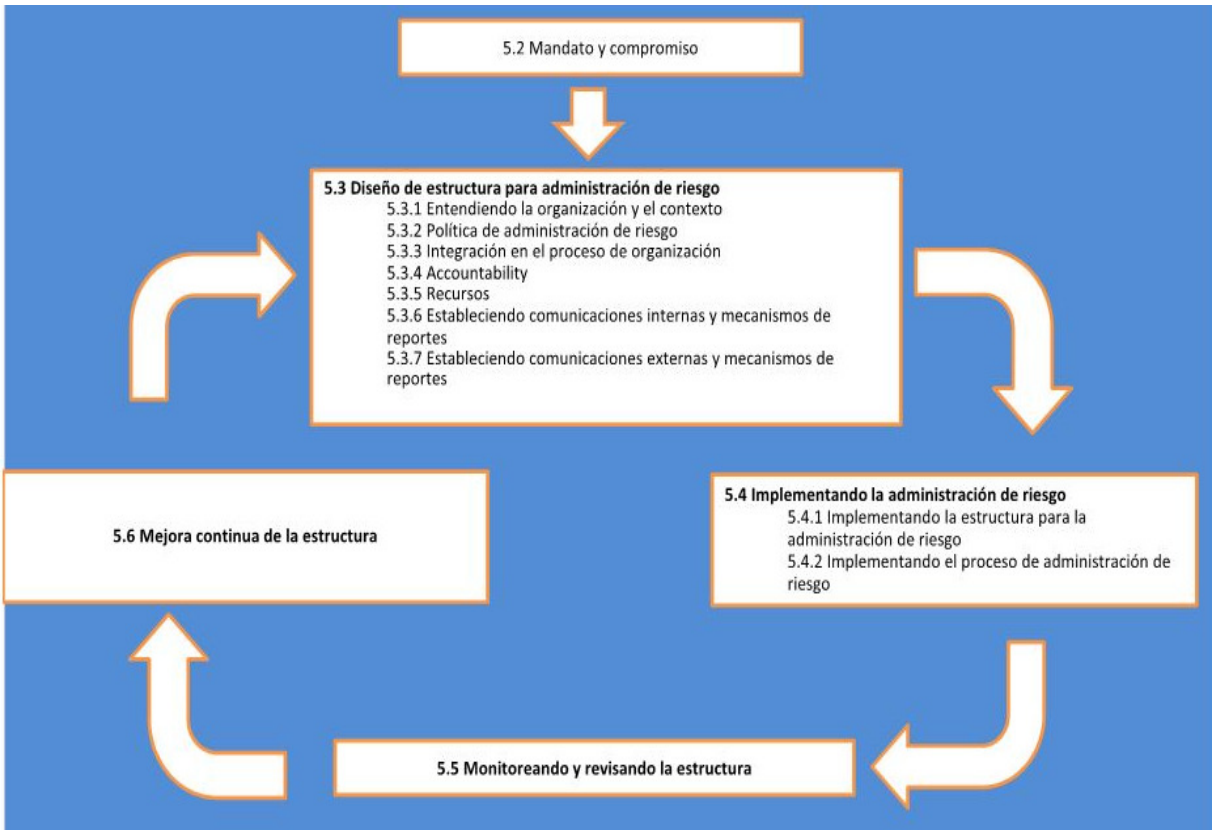


Figura 35. Estructura para la administración de riesgos ISO 31000. Fuente: ISO 31000- Traducción libre al español del Sr. Carlos Valdivieso

Lo descrito en la figura anterior, brinda a la gerencia de riesgos el piso firme para desarrollar el modelo de gestión de riesgo operacional más amplio y abarcar todos los objetivos que se soporten en la estrategia del negocio, respondiendo así al cuestionamiento constante, si debe considerarse la gestión de riesgo operacional, como un asunto estratégico.

En resumen, el estándar ISO 31000 adopta lo mejor del mundo gerencial y de riesgos; además fortalece el trabajo de los especialistas que han luchado por hacerse ver en las organizaciones como factores críticos de éxito en las estrategias de negocios, los cuales, cuando logran hacer funcionar dicha gestión, los objetivos de las organizaciones son alcanzados.

CAPÍTULO IV

METODOLOGÍA DE ANÁLISIS DE RIESGO OPERACIONAL

El diseño metodológico empleado en el desarrollo de este trabajo, fue basado en las fases definidas por el estándar ISO 31000:2009 y el AS/NZS: 4360 descritas en el capítulo anterior, las cuales se describen a continuación:

4.1 FASE 1: ESTABLECIMIENTO DEL CONTEXTO

Para establecer los contextos estratégico, organizacional y de gestión en los cuales tendrá lugar el proceso de gestión de riesgos a realizar en este trabajo, fueron determinados los siguientes:

1. Definir el proyecto o actividad.

El proyecto objeto de estudio para el análisis de riesgo operacional es: Implementación del servicio IPTV en CANTV.

2. Identificar objetivos y recursos requeridos.

Masificar el servicio de TV por suscripción en Venezuela, a través de una oferta diferenciada y superior a la de las cableras a nivel nacional. Los elementos diferenciadores de la propuesta se basan en: i) Calidad superior de video (calidad DVD), ii) Video por demanda" (VOD), iii) Oferta de canales a la carta, iv) Guía interactiva y v) Servicios avanzados adicionales.

La solución para ofrecer TV por suscripción, presenta como elementos

funcionales los siguientes:

- **Subsistema cabecera (Headend):** implica las etapas de recepción, procesamiento, compresión y monitoreo.
- **Red de transporte y acceso con sus componentes:** está compuesta por: red urbana e interurbana, nodos de acceso, última milla y predios del cliente.
- **Red Urbana e Interurbana:** consta de anillos interurbanos y urbanos.
- **Nodos de Acceso:** proveen servicio de acceso de banda ancha al igual que proveerán servicio de TV por suscripción.
- **Ultima milla**: mediante la cual el usuario se conecta a la red.

La tecnología de acceso utilizada en los nodos de acceso exige ciertas condiciones para garantizar la velocidad final. Se prevé la velocidad de 8Mbps para la transmisión simultánea de dos canales de video.

3. Definir el alcance del proyecto, el tiempo asociado y su ubicación.

Se busca desarrollar una oferta triple play (TV, Voz y Datos), alcanzando una participación en el mercado de Televisión por Suscripción del 14% en 5 años en Venezuela, al tiempo que se defiende el negocio tradicional de voz y se apunta al logro de una participación en el mercado del 78% en banda ancha residencial.

4. ¿Cual actividad inicia el proceso, proyecto o actividad?

Documento de definición del proyecto generado por la unidad de negocio de Mercadeo Corporativo y Planificación Corporativa.

5. ¿Cuál actividad finaliza el proceso, proyecto o actividad?

Implementación y pase a producción del servicio IPTV en CANTV.

6. ¿Cuáles son las principales amenazas y oportunidades que presenta el proyecto?

Amenazas que presenta el proyecto:

- Para prestar el servicio de difusión por suscripción CANTV se apalancará sobre los nodos de acceso ya existentes, que son los que usa actualmente para ofrecer el servicio de Internet Banda Ancha.

- La capacidad del sistema o solución estará limitada por el número total de puertos ABA que estén instalados y adecuados en los nodos de acceso para ofrecer servicios de difusión de video por suscripción. Dicha capacidad máxima instalada estará definida por dos premisas fundamentales, la distancia de los clientes al nodo de acceso y el mínimo ancho de banda requerido para garantizar la calidad del servicio.

- La zona de cobertura abarca todas las regiones del país donde CANTV posee instalaciones e infraestructura de acceso.

- La entrada tardía de CANTV al mercado y el fortalecimiento de

competidores que ofrecen una oferta empaquetada de servicios de voz, data y video.

Oportunidades que presenta el proyecto:

- La incorporación de video a la oferta comercial de CANTV es una movida estratégica y rentable para el dominio del mercado de banda ancha y el crecimiento y defensa de ingresos de la corporación. La estrategia es que CANTV se posicione como el proveedor preferido para el aprovisionamiento de múltiples servicios para el hogar (voz, datos y video en el corto plazo, juegos y nuevos servicios/contenidos en el mediano/largo plazo).

- La oferta de CANTV está orientada a masificar el servicio de difusión por suscripción en Venezuela, basándose en su amplia cobertura de líneas telefónicas a nivel nacional y una oferta de servicio con variedad de planes y precios orientados a los diferentes niveles socio-económicos existentes en el mercado venezolano, desde las clases sociales más desposeídas hasta aquellas de mayores ingresos, tal como actualmente lo constituye la cartera de clientes de CANTV.

7. ¿Quiénes son las partes interesadas? (Stakeholders)

En esta actividad son definidas las personas y las organizaciones quienes pueden ser afectadas o beneficiadas por la implementación del

servicio IPTV en CANTV. En este sentido se presenta en la tabla 3 los stakeholders internos y externos identificados.

Tabla 3. Partes interesadas-Stakeholders

Proyecto:Implementación Sevicio IPTV en CANTV
Responsable: Gerencia General Servicios Audiovisuales

Partes Involucradas
Internas
Gerencia General de Proyectos Mayores
Gerencia General Tecnologia y Operaciones
Gerencia General Seguridad Integral
Gerencia General Gestión Humana
Gerencia General Centro de Servicios
Gerencia General de Finanzas
Gerencia General Consultoria Juridica
Gerencia General de Mecados Masivos
Gerencia General Mercadeo Corporativo
Gerencia General Servicios Audiovosuales
Externas
Proveedores: ZTE, CISCO, PROTOKOL,ALCATEL
CONATEL
Gobierno Ejecutivo
Clientes residenciales de CANTV

8. Definir los criterios del riesgo:

En este proceso se deben identificar las "áreas de impacto" y las "fuentes de riesgos" que se pueden presentar y la forma en que se van a medir.

1. Área de Impacto:

Es todo recurso, bien u oportunidad al cual la organización le ha (o debe) asignar un valor y su afectación podría comprometer el cumplimiento de sus objetivos y metas. Para el análisis de la implantación del servicio IPTV en CANTV fueron definidas las siguientes: Activos y recursos básicos; Desempeño; Oportunidad e intangibles. Todas estas se encuentran

detalladas en la tabla 4.

Tabla 4. Áreas de Impacto

AREAS DE IMPACTO (¿Qué?)				
Activos y recursos básicos ($)	***Ingresos y Derechos ($)***	***Costos de las Actividades ($)***	***Desempeño***	***Intangibles***
Activos / Pasivos / Capital / Recursos de TI (información) / Personas	Ventas / Patentes / Intereses / Regalías / Comisiones	Directos / Indirectos / Reposición / Indemnización / Sanciones	Productividad Calidad	Imagen / Credibilidad / Conocimiento
-Pérdida de Activos -Pérdida de Información -Pérdida de Capital -Pérdida de vidas humanas	-Dejar de percibir ingresos por -Incremento de intereses por -Pérdida de comisiones por	-Incremento en costo de las operaciones de -Incremento en costo por reposición -Incremento en costos por pago de indemnizaciones	-Pérdida de productividad del área -Incremento de la operatividad del área	-Pérdida de imagen y credibilidad pública -Pérdida de reputación

2. Fuentes de Riegos:

Es todo individuo, grupo humano, entidad, elemento físico, o fenómeno del entorno, de los cuales se pueden derivar eventos que podrían afectar las Áreas de Impacto de la organización. En este sentido, fueron definidas las siguientes cuatro categorías tomando como referencia la lista de eventos definidos por el Comité de Basilea:

- Personal.
- Procesos.
- Sistemas.
- Fuentes externas

Todas estas se ilustran en la tabla 5.

Tabla 5. Fuentes de Riesgos

FUENTES DE RIESGO (¿Por qué y Cómo?)		
Categoría 1	**Categoría 2 (¿Por Qué?)**	**Eventos de Riesgo (¿Cómo?)**
Relativos a las Personas	Ausencia o pérdida de personal clave	Ausencia de personal entrenado y adecuado
		Pérdida de personal clave / indispensable
Relativos al proceso	Documentación riesgosa	Documentos no apropiadamente elaborados
	Relativos al Cumplimiento	No-adherencia al cumplimiento de procedimientos internos
		No-adherencia a cumplimiento de procedimientos externos
	Proyectos / Administración de cambios riesgosos	Propuestas inadecuadas de proyectos / planes
		Procesos de nuevos productos deficientes
		Proyectos excedidos (Tiempo / presupuesto)
	Riesgos relativos a ventas	Inapropiada selección productos
		Complejidad de los Productos
Relativos a los Sistemas	Inversiones riesgosas en tecnología	Arquitectura Inapropiada
		Estrategias de plataformas riesgosas
		Definición Inapropiada de requerimientos del negocio
		Incompatibilidad con sistemas existentes
		Obsolescencia del hardware
		Obsolescencia del software
	Desarrollo e Implementación de sistemas	Costo / tiempo reproceso
		Errores en la Programación (internos / externos)
		Fallas en la integración con sistemas existentes
		Fallas en la migración desde sistemas existentes
		Fallas en los sistemas para cumplir requerimientos del negocio
	Capacidad de los Sistemas	Ausencia de una planeación de capacidad adecuada
		Software inadecuado
	Fallas de los Sistemas	Fallas de la interconexión (Redes)
		Riesgos en el intercambio de datos
		Fallas en las interfaces
		Fallas de Hardware
		Fallas de Software
		Fallas internas en las comunicaciones
		Fallas externas en las comunicaciones
	Violaciones a la seguridad de los Sistemas	Violaciones externas a la seguridad
		Violaciones internas a la seguridad
		Fraude por programación
		Virus de computación
De fuentes externas	Riesgos Regulatorios	Cambios en las reglas de regulación en la industria / país
	Riesgos Políticos / Gubernamentales	Otros cambios en la ley

Luego de definir las áreas de impacto y fuentes de riesgos que pueden ser consideradas en la implementación del servicio IPTV en CANTV, la técnica a utilizar para la identificación de riesgos en la siguiente fase consistirá en la conjugación de una matriz de fuentes y áreas de impacto, similar a la descrita en la figura 36.

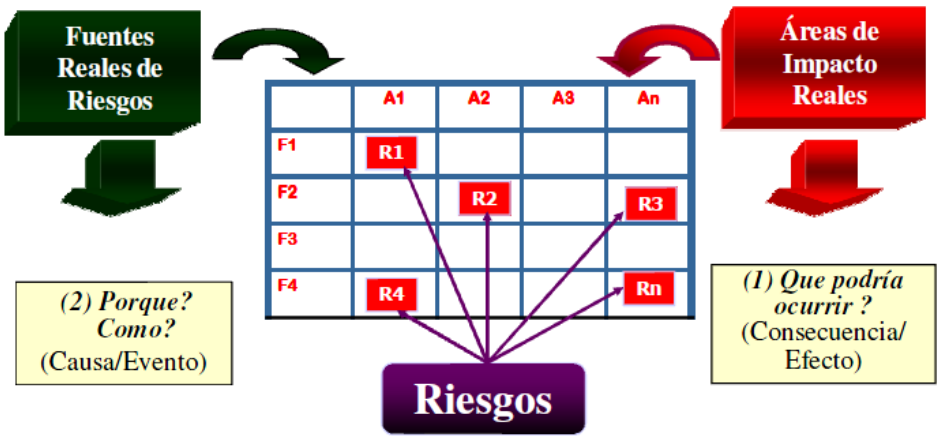


Figura 36. Técnica para Identificar los Riesgos: Matriz de Fuentes y Áreas Impacto. Fuente: GIT Soluciones Integrales

9. ¿Cómo se va a definir la probabilidad y consecuencia?

1. Consecuencia:

Es el resultado de un evento (Causa) expresado cualitativa o cuantitativamente, sea este una pérdida, perjuicio, desventaja o ganancia. Para la medición de esta serán considerados cinco niveles y tres áreas de impacto, tal y como se muestran en la siguiente tabla 6.

Tabla 6. Factores para medición de consecuencias

Valor	Descriptor	Impacto en Objetivos	Comunidad / Reputación / Medios	Legales
5	Catastrófico	Impacto crítico en los Objetivos Corporativos Críticos	Efecto publicitario sostenido a nivel país y en el ámbito internacional, pérdida de clientes en gran escala	Acusaciones y multas significativas organismo regulador. Litigios muy serios.
4	Mayor	Alto impacto en los Objetivos Corporativos	Efecto publicitario sostenido a nivel de ciudades y limitado en el ámbito nacional, serias pérdidas de clientes	Requerimiento formal o investigación organismo regulador. Litigios mayores.
3	Moderado	Mediano impacto en los Objetivos Corporativos	Efecto publicitario en la poblaciones limitadas, gran incremento en reclamos de clientes, alguna pérdida de clientes	Requerimiento informal del organismo regulador. Litigios menores.
2	Menor	Menor impacto en los Objetivos Corporativos	Efecto publicitario local o en la industria limitado, incremento en reclamos de clientes, posibles retiros de clientes	Requerimiento informal del organismo regulador. Conciliaciones menores.
1	Insignificante	Impacto insignificante en los Objetivos Corporativos	Sin efecto publicitario, incremento en reclamos de clientes	Asuntos legales menores.

2. Probabilidad:

En la terminología de la gestión del riesgo, la palabra "probabilidad" se utiliza para hacer referencia a la oportunidad de que algo suceda, esté o no definido, medido o determinado objetiva o subjetivamente, cualitativa o cuantitativamente, y descrito utilizando términos generales o matemáticos (como la probabilidad numérica (probability) o la frecuencia en un periodo de tiempo determinado).

Para la medición de esta, serán considerados cinco niveles comprendidos entre 1 y 5, cada uno de los cuales representa un descriptor

asociado al valor numérico de la probabilidad matemática correspondiente, tal y como se muestran en la tabla 7.

Tabla 7. Definición de la probabilidad.

Valor	Descriptor	Probabilidad Matemática
5	Casi Cierta	Mayor al 4.5
4	Muy Probable	Entre el 3.5 y 4.5
3	Posible	Entre 2.3 y 3.4
2	Improbable	Entre 1.1 y 2.2
1	Rara	Menor o igual a 1

Para determinar el valor de la probabilidad matemática fue utilizada una técnica de sistema de puntuación riesgo o scoring de riesgo, aplicada comúnmente para análisis financiero, la cual consiste en la definición de factores de riesgo, los cuales son ponderados con pesos definidos por el dueño del proceso, y se determina el peor escenario de impacto al presentarse los factores de riesgo identificados.

La suma del puntaje de los factores ponderados representa la probabilidad de que el riesgo, si se materializara, resulte “con la mayor criticidad”, en donde el responsable del proceso es quien define lo que significa de mayor criticidad. Los factores de riesgo son todas aquellas características o condiciones, cuya presencia ó comportamiento incide en una mayor o menor consecuencia de materialización de una o varias causas asociadas a un riesgo o conjunto de riesgos. Luego de esto el responsable o grupo de responsables pondera cada uno de los factores antes definidos con la incidencia en el escenario actual del factor evaluado.

Una vez obtenido ambas valoraciones es aplicada la formula 1, para determinar el porcentaje de probabilidad de que el evento suceda y su valoración de acuerdo a las definiciones mostradas en la tabla 7.

% Probabilidad = puntaje total causa/total de puntaje posible

(Rango de 0 – 1 / %)

Fórmula 1. Calculo del porcentaje de probabilidad.

9.2.1 Factores para valoración del riesgo

Los factores definidos para la evaluación del riesgo, se agruparon en las siguientes categorías:

1. Ambiente de control (Externo / Interno)

- Valores ciudadanos
- Nivel de seguridad del entorno
- Estabilidad social, política, económica, legislativa
- Calidad de la comunicación Externa / Interna
- Grado Supervisión Alta Gerencia (Gobernabilidad Corporativa)
- Grado Monitoreo independiente (Auditoría Externa / Interna)
- Conciencia de control de la gerencia
- Presión en el cumplimiento de objetivos y metas excesivas
- Idoneidad del personal
- Moral y Valores éticos del personal
- Rotación del personal
- Ambiente de control general de la TI

2. **Ambiente de negocios (Externo / Interno)**

- Rápido crecimiento
- Nuevos productos
- Mercados desconocidos
- Productos o actividades ajenas al “Core” del negocio.

3. **Características del proceso / Actividad/ Transacciones**

- Complejidad
- Grado de manualidad o de automatización
- Grado de cambios
- Calidad documentación
- Negociabilidad objetos financieros (Efectivo, Títulos valores, Activos fijos, etc.)
- Concentración (Funciones / Decisiones / Operaciones / Transacciones, etc.)

4. **Ambiente Físico e instalaciones**

- Localización susceptible a inundaciones, Químicos,
- Susceptibilidad a variaciones de voltaje
- Susceptibilidad a variaciones de temperatura
- Susceptibilidad a variaciones de humedad, polvo, tierra.
- Susceptibilidad a radiaciones electromagnéticas.

5. **Comunicaciones**

- Pobre unión del cableado
- Líneas Dial-up (Conmutadas).

6. **Software**

- Interfaces de usuario complicadas o poco amigables
- Divulgación de las debilidades de control del software
- Calidad documentación

En la figura 37, se muestra un ejemplo de valoración de riesgo absoluto utilizando la técnica de scoring. En este escenario se indican (5) factores de riesgo, cada uno ponderado con valores entre cero (1) y diez (10) dependiendo de su incidencia. De esta manera el peor escenario evaluado con los factores de riesgo definidos, arroja un puntaje igual a 270, lo cual representa el 100% de probabilidad de ocurrencia.

Factores	Rango evaluación	P	Ponderación	Descripción Factor	Puntaje
Complejidad	Sencillo	1	1		
	Algo complejo	5			
	Muy complejo	10			10
	No aplica	0			
Grado Automatización	Automatizado	1	10		
	Combinado	5			
	Manual	10			100
	No aplica	0			
Calidad Comunicación	Excelente	1	1		
	Maderada	5			
	Pobre	10			10
	No aplica	0			
Calidad documentación	Muy completa	1	5		
	Aceptable	5			
	Deficiente	10			50
	No aplica	0			
Idoneidad del personal	Excelente	1	10		
	Aceptable	5			
	Deficiente	10			100
	No aplica	0			
Puntaje Total Factores que aplican al escenario/Causa del Riesgo					270
% Probabilidad (Puntaje Total de la causa / Total de puntaje posible) 270/270					100%

Figura 37.Tecnica del scoring para calculo del % Probabilidad. Fuente: GIT Soluciones Integrales

10. ¿Cómo se va a determinar el nivel de riesgo?

La magnitud de un **riesgo** es expresada en términos de la combinación de las consecuencias y su probabilidad, lo cual arroja como resultado la severidad o nivel de riesgo resultante.

Consecuencia x Probabilidad= Severidad

En este sentido serán definidos cuatro valores de severidad, que serán representado en una matriz grafica, tal y como se muestra en la siguiente figura:

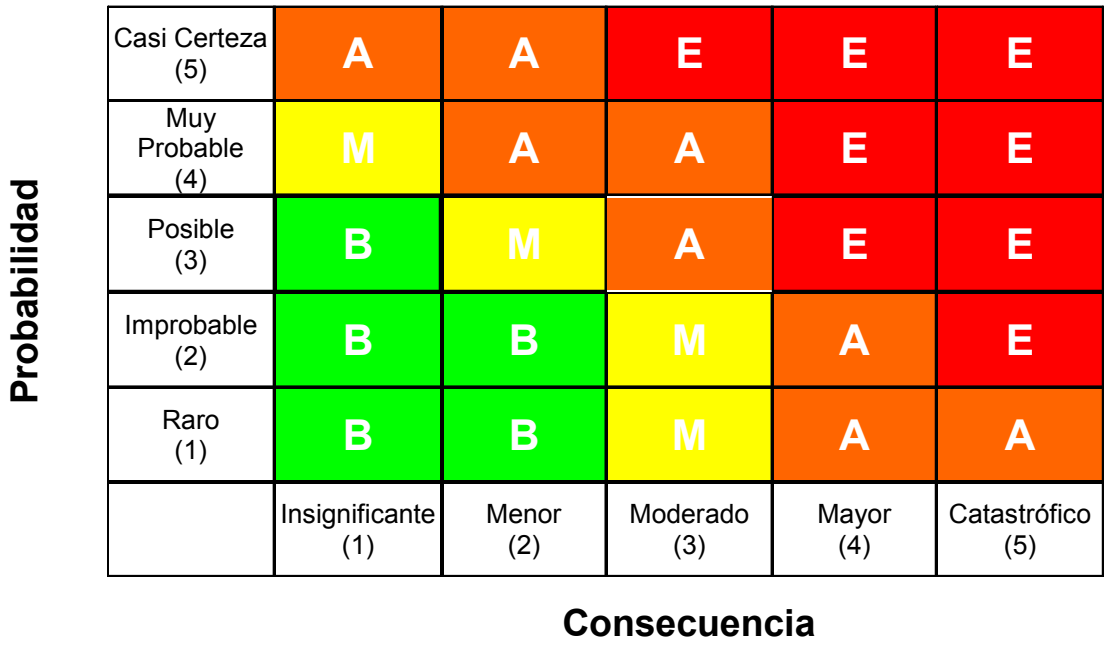


Figura 38. Matriz de evaluación de severidad de riesgo operacional.
Fuente: Fuente: Elaboración Propia

La tabla de valoración asociada a la severidad asociada a la matriz grafica, se muestra a continuación:

Tabla 8. Valoración de severidad del riesgo.

Es importante mencionar que el valor de riesgo a determinar en este trabajo corresponde al riesgo absoluto o inherente, que es identificado dentro del proyecto.

11. ¿En cuál nivel el riesgo se torna aceptable o tolerable?

Dentro de la Gerencia de Seguridad de la Operación, será considerado como un riesgo aceptable aquel cuyo valor se encuentre dentro de la categoría de severidad bajo al momento de determinar el valor de riesgo absoluto.

Así mismo, para aquellos riesgos que se sitúen después de la evaluación con severidad extrema, alta y moderada deben ser reducidos, definiendo sus tratamientos a través del desarrollo e implementación de planes de acción específicos para su mitigación, considerando la prioridad del nivel de severidad encontrado.

4.2 FASE 2: IDENTIFICACIÓN DE RIESGOS

Dentro de esta fase, se realizó la identificación de los riesgos que podrían impedir, degradar o demorar el cumplimiento de los objetivos

asociados a la implementación del servicio IPTV en CANTV, desde el punto de vista operacional.

La identificación de los riesgos operacionales se ejecutó mediante la conjugación de una matriz de fuentes de riesgo y áreas de impacto, descritas en la tabla 4 y 5, tal y como se ilustra en la figura 39.

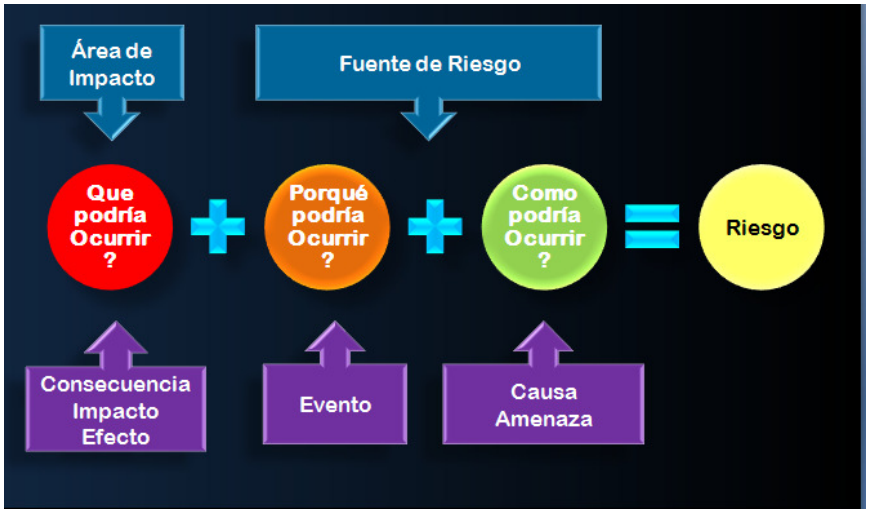


Figura 39. Definición de los Riesgos. Fuente: GIT Soluciones Integrales

Luego de realizar el análisis de riesgo operacional asociado a la implementación del servicio IPTV en CANTV, fueron identificados **16 eventos** que de materializarse pudiesen causar una desviación en la implementación del servicio.

Es importante mencionar que el ámbito de estudio de las desviaciones abarcó el análisis de las plataformas de redes de CANTV que transportarán el servicio de IPTV, así como aquellas desviaciones que puedan impactar la degradación y/o negación del servicio y por ende la calidad hacia el usuario final.

En la siguiente tabla se ilustran los riesgos operaciones identificados para la implementación del servicio IPTV en CANTV, así como las áreas responsables para el tratamiento de los mismos:

Tabla 9. Identificación de riesgos para la implementación del servicio IPTV en CANTV

RIESGO			
Referencia	**Datos del Riesgo**		
Código Referencia del Riesgo	**Nombre Corto Riesgo (Porque y Como resumido)**	**Descripción del Riesgo (Que puede suceder, Porque puede suceder, Como puede suceder, Cuando puede suceder).**	**Áreas Responsables**
R1	Implementación de las adecuaciones lógicas en la red Metro Ethernet, que presenten errores en la configuración de las plantillas sobre los SW Alcatel 7450	Pérdida de servicios actuales en la red Metro Ethernet por la implementación de las adecuaciones lógicas para el soporte del servicio IPTV, que presenten errores en la configuración de las plantillas sobre los switch Alcatel 7450 para configurar protocolo multicast IGMP y desarrollar los servicios para tráfico Unicast y Multicast	1. GGPM/ 1. Gerencia de Programas de Infraestructura de TI – IPTV
R2	Implementación de las adecuaciones en la red troncal IP, que presenten errores en la plantillas sobre los router Cisco 12000	Pérdida de servicios actuales en la red troncal IP por la implementación de las adecuaciones lógicas para el soporte del servicio IPTV, que originen errores en la programación de las platillas para activar protocolos multicast PIM SSM en los equipos Cisco 12000	1. GGPM/ 1. Gerencia de Programas de Infraestructura de TI – IPTV
R3	Implementación de las adecuaciones en la red de acceso, que presenten errores en la plantillas sobre los DSLAM IP Alcatel 7302	Pérdida de servicios actuales en la red de acceso por la implementación de las configuraciones lógicas para el soporte del servicio IPTV, que originen errores en la programación de las plantillas para activar las licencias multicast en los DSLAM IP Alcatel 7302	1. GGPM/ 1. Gerencia de Programas de Infraestructura de TI – IPTV
R4	Aprovisionamiento del servicio IPTV en los equipos DSLAM IP, que originen fallas en el desempeño de los equipos ALCATEL 7302 en el otorgamiento del servicio de internet.	Afectación del servicio de Internet debido al aprovisionamiento del servicio IPTV sobre los equipos DSLAM IP, que ocasionen fallas en el desempeño de los equipos ALCATEL 7302 , para la convergencia de ambos servicios en el mismo equipo.	1. GGPM/ 1. Gerencia de Programas de Infraestructura de TI – IPTV

RIESGO			
Referencia	**Datos Riesgo**		
Código Referencia del Riesgo	**Nombre Corto Riesgo (Porque y Como resumido)**	**Descripción del Riesgo (Que puede suceder, Porque puede suceder, Como puede suceder, Cuando puede suceder).**	**Aéreas Responsables**
R5	Fallas en los equipos DSLAM IP, por no contar con redundancia de equipos, interfaces y energía de estos elementos.	Afectación de la imagen corporativa con el servicio IPTV, por fallas concurrentes en los equipos DSLAM IP, por no contar con redundancia de equipos, interfaces y energía de estos elementos.	1. GGPM/ 1. Gerencia de Programas de Infraestructura de TI – IPTV
R6	Fallas en los elementos de la cabecera de video, por ausencia de un plan redundancia física y lógica de cada uno de los elementos que conforman el subsistema Headend de la plataforma IPTV.	Corte del servicio IPTV por fallas en los elementos de la cabecera de video (Headend) y elementos de conexión hacia la red de distribución del servicio, por ausencia de un plan de redundancia física y lógica de cada uno de los elementos que conforman el subsistema Headend de la plataforma IPTV.	1. GGPM/ Gerencia de Arquitectura de Redes 2. GGPM/ Gerencia de Programas de Infraestructura de TI – IPTV 3. GGSA/ Gerencia de Servicios Audiovisuales
R7	Fallas en los elementos del mediador, por ausencia de un plan redundancia física y lógica de cada uno de los elementos que conforman el subsistema mediador de la plataforma IPTV.	Corte del servicio IPTV por fallas en los elementos del mediador (middleware) y elementos de conexión hacia la red de distribución del servicio, por ausencia de un plan de redundancia física y lógica de cada uno de los elementos que conforman el subsistema mediador de la plataforma IPTV.	1. GGPM/ Gerencia de Arquitectura de Redes 2. GGPM/ Gerencia de Programas de Infraestructura de TI – IPTV 3. GGSA/ Gerencia de Servicios Audiovisuales
R8	Fallas en los elementos que dan soporte al servicio de video bajo demanda, al no contar con un plan de redundancia de los servidores de video bajo demanda.	Corte del servicio IPTV por fallas en los elementos que dan soporte al servicio de video bajo demanda y elementos de conexión hacia la red de distribución del servicio, por no contar con un plan de redundancia 1:1/1:N de los servidores de video bajo demanda.	1. GGPM/ Gerencia de Arquitectura de Redes 2. GGPM/ Gerencia de Programas de Infraestructura de TI – IPTV 3. GGSA/ Gerencia de Servicios Audiovisuales
R9	Inversión riesgosa en la plataforma IPTV, al no contar con la arquitectura apropiada de red de acceso para otorgar el servicio al usuario final.	Afectación de la imagen corporativa de CANTV por inversiones riesgosa en la plataforma IPTV, al no contar con la arquitectura apropiada de red de acceso para otorgar el servicio al usuario final.	1. GGPM/ Gerencia de Programas de Infraestructura de TI – IPTV 2. GGSA/ Gerencia Operaciones de Servicios Audiovisuales

RIESGO			
Referencia	**Datos Riesgo**		
Código Referencia del Riesgo	**Nombre Corto Riesgo (Porque y Como resumido)**	**Descripción del Riesgo (Que puede suceder, Porque puede suceder, Como puede suceder, Cuando puede suceder).**	**Áreas Responsables**
R10	Definición inapropiada de mecanismos para proveer denegación de servicio a las peticiones de VoD, al presentarse congestiones de red y servicio.	Alteración en el desempeño de la red de CANTV, por definición inapropiada de mecanismos para proveer denegación de servicio a las peticiones de VoD, al presentarse congestiones de red y servicio (congestión de la red de transporte, congestión en IPDSLAM, capacidad máxima de los servidores VOD alcanzados, etc.)	1. GGPM/ 1. Gerencia de Programas de Infraestructura de TI – IPTV 2. GGSA/ Gerencia Operaciones de Servicios Audiovisuales
R11	Incremento en la capacidad de asignación de direcciones IP a los STB y Módems, por ausencia de una planeación de capacidad adecuada de los servidores actuales de DHCP.	Disminuir la disponibilidad de los servidores DHCP por el incremento en la capacidad de asignación de direcciones IP a los STB para el servicio y a los Módems para la gestión, por ausencia de una planeación de capacidad adecuada en la integración de los servicios dentro de los servidores actuales de DHCP.	1. GGPM/ 1. Gerencia de Programas de Infraestructura de TI – IPTV
R12	Violaciones a la seguridad de los sistemas de autenticación de usuarios del servicio IPTV, al no contar con mecanismos que restrinjan el acceso de otros STB.	Dejar de percibir ingresos por violaciones a la seguridad de los sistemas de autenticación de usuarios del servicio IPTV, al no contar con mecanismos de seguridad que restrinjan el acceso de otros STB por parte del cliente.	1. GGPM/ 1. Gerencia de Programas de Infraestructura de TI – IPTV 2. GGSA/ Gerencia Operaciones de Servicios Audiovisuales 3.GGSI/Gerencia de Seguridad de la Información
R13	Fallas en la red de CANTV que superen el tiempo promedio de cambio de canal mayor a 2 segundos,	Pérdida de imagen del producto, por fallas en la red de CANTV que superen el tiempo promedio de cambio de canal mayor a 2 segundos, ocasionando impacto en la calidad de experiencia del cliente.	1. GGPM/ 1. Gerencia de Programas de Infraestructura de TI – IPTV
R14	Pago de sanciones, por incumplimiento de las reglas de regulación para la medición de las métricas de calidad del servicio para IPTV definidas por CONATEL	Incremento en los costos por pago de sanciones, debido al incumplimiento de las reglas de regulación para la medición de las métricas de calidad del servicio para IPTV definidas por CONATEL	1. GGPM/ 1. Gerencia de Programas de Infraestructura de TI – IPTV 2. GGPM/ Gerencia de Asuntos Regulatorios 3. GGTO/Gerencia de Operaciones Centralizadas 4. GGSI/Gerencia de Seguridad de la Operación

RIESGO			
Referencia	**Datos Riesgo**		
Código Referencia del Riesgo	**Nombre Corto Riesgo (Porque y Como resumido)**	**Descripción del Riesgo (Que puede suceder, Porque puede suceder, Como puede suceder, Cuando puede suceder).**	**Áreas Responsables**
R15	Implementación de un sistema de gestión con deficiencias para cumplir con los requerimientos de operación y mantenimiento de la Plataforma IPTV siguiendo las políticas corporativas.	Afectación del servicio IPTV, por la implementación de un sistema de gestión con deficiencias para cumplir con los requerimientos de operación y mantenimiento de la Plataforma IPTV siguiendo las políticas corporativas.	1. GGPM/ 1. Gerencia de Programas de Infraestructura de TI – IPTV 3. GGTO/Gerencia de Operaciones Centralizadas
R16	Operación del servicio IPTV, con deficiencia en los procesos de operación y mantenimiento para este nuevo producto.	Incremento de la actividades en las áreas operativas por la operación del servicio IPTV, al tener deficiencia en los procesos de operación y mantenimiento para este nuevo producto.	1. GGSA 2. GGTO

La matriz utilizada de área de impacto vs. fuentes de riesgo para la identificación de los 16 riesgos listados en la tabla anterior se muestra en el anexo 3.

4.3 FASE 3: ANÁLISIS DE RIESGOS

Para el análisis se consideró el rango de consecuencias potenciales y la probabilidad de que los riesgos pudieran ocurrir, de acuerdo en lo descrito en la tabla 7, para la estimación de la consecuencia y en la tabla 8, para la definición de la probabilidad. Todo este análisis se realizó en conjunto con las áreas responsables identificadas en la fase 2, mediante la ejecución de mesas de trabajo en las cuales se aplicaron las técnicas como la experiencia, juicio de expertos y listas de chequeo.

Para el análisis de consecuencia se obtuvieron los resultados descritos en la tabla 10.

Tabla 10. Análisis de consecuencia para la implementación del servicio IPTV en CANTV

RIESGO			
Referencia	**Datos Riesgo**		
Código Referencia del Riesgo	**Consecuencia**		
	Valor	**Descriptor**	**Tipo**
R1	4	**Mayor**	Impacto en Objetivos
R2	4	**Mayor**	Impacto en Objetivos
R3	4	**Mayor**	Impacto en Objetivos
R4	4	**Mayor**	Comunidad / Reputación / Medios
R5	3	**Moderado**	Comunidad / Reputación / Medios
R6	4	**Mayor**	Impacto en Objetivos
R7	4	**Mayor**	Impacto en Objetivos
R8	4	**Mayor**	Impacto en Objetivos
R9	3	**Moderado**	Comunidad / Reputación / Medios
R10	3	**Moderado**	Impacto en Objetivos
R11	3	**Moderado**	Impacto en Objetivos
R12	4	**Mayor**	Impacto en Objetivos
R13	3	**Moderado**	Comunidad / Reputación / Medios
R14	4	**Mayor**	Legales
R15	3	**Moderado**	Impacto en Objetivos
R16	4	**Mayor**	Impacto en Objetivos

Para el análisis de probabilidad se utilizó la técnica del scoring para cada uno de los 16 riesgos identificados, a los cuales les fueron definidos independientemente los factores de riesgo, y analizados de acuerdo a lo descrito en la fase 1 en conjunto con las áreas responsables de cada evento.

En las tablas 11 y 12, se muestra un ejemplo de valoración de riesgo absoluto, para el análisis efectuado del riesgo uno (1) identificado para la implementación del servicio IPTV en CANTV, para el cual se definieron cinco (5) factores de riesgo, cada uno ponderado con valores entre uno (1) y cinco (5) dependiendo de su incidencia.

Tabla 11. Valoración Riesgo Absoluto: SCORING en el peor escenario.

Riesgo 1: Implementación de las adecuaciones lógicas en la red Metro Ethernet, que presenten errores en la configuración de las plantillas sobre los SW Alcatel 7450
Causa inmediata: errores en la configuración de las plantillas sobre los SW Alcatel 7450

Análisis de Factores-Peor escenario

Factores de Riesgo	Rango de evaluación	P	Ponderación	Puntaje
Capacitación del personal responsable de la configuración	Alta Capacitación	1	5	25
	Mediana Capacitación	3		
	Poca Capacitación	5		
Complejidad de las configuraciones	Muy Complejo	5	3	15
	Complejidad moderada	3		
	Simple	1		
Complejidad de las interfaces/consolas de usuario	Muy Complejo	5	1	5
	Complejidad moderada	3		
	Simple	1		
Nivel de conocimiento de los procesos para ejecución de control de cambio en la red	Son Conocidos	1	5	25
	Poco Conocidos	3		
	Desconocidos	5		
Presión en el cumplimiento de los objetivos	Alta	5	1	5
	Mediana	3		
	Baja	1		
Puntaje total posible de los factores que aplican al escenario/Causa del riesgo= 5*5 + 3*5 + 1*5 + 5*5 + 1*5				**75**

Tabla 12. Valoración Riesgo Absoluto: SCORING en la situación actual.

Riesgo 1: Implementación de las adecuaciones lógicas en la red Metro Ethernet, que presenten errores en la configuración de las plantillas sobre los SW Alcatel 7450
Causa mediata: errores en la configuración de las plantillas sobre los SW Alcatel 7450

Valoración de la Probabilidad

Factores de Riesgo	Rango de evaluación	P	Ponderación	Puntaje
Capacitación del personal responsable de la configuración	Alta Capacitación		5	15
	Mediana Capacitación	3		
	Poca Capacitación			
Complejidad de las configuraciones	Muy Complejo	5	3	15
	Complejidad moderada			
	Simple			
Complejidad de las interfaces/consolas de usuario	Muy Complejo		1	3
	Complejidad moderada	3		
	Simple			
Nivel de conocimiento de los procesos para ejecución de control de cambio en la red	Son Conocidos	1	5	5
	Poco Conocidos			
	Desconocidos			
Presión en el cumplimiento de los objetivos	Alta	5	1	5
	Mediana			
	Baja			
Puntaje total factores que aplican al escenario/Causa del riesgo				**43**
% Probabilidad (puntaje total causa/total de puntaje posible)=(43/75)*100%				**57,3%**

De esta manera el 57,3% de probabilidad representa un valor de 2,86 de acuerdo a lo expresado en la tabla 7, lo que representa que este evento de acuerdo a las condiciones actuales es “posible” que suceda:

POSIBLE
3

Todos los análisis de probabilidades realizados para cada uno de los 16 eventos identificados se encuentran descritos en el anexo 4.

En la tabla siguiente se muestran los valores de probabilidad resultantes de las tablas de valoración de los factores de riesgo:

Tabla 13. Análisis de probabilidad para la implementación del servicio IPTV en CANTV

RIESGO		
Referencia		
Código Referencia del Riesgo	**Probabilidad**	
	Valor	**Descriptor**
R1	3	**Posible**
R2	2	**Improbable**
R3	2	**Improbable**
R4	3	**Posible**
R5	3	**Posible**
R6	2	**Improbable**
R7	2	**Improbable**
R8	2	**Improbable**
R9	3	**Posible**
R10	3	**Posible**
R11	3	**Posible**
R12	3	**Posible**
R13	3	**Posible**
R14	2	**Improbable**
R15	1	**Rara**
R16	3	**Posible**

Para determinar la magnitud de cada riesgo, los valores de consecuencia y probabilidad fueron combinados para producir el nivel de severidad, utilizando la matriz descrita en la figura 38.

Los resultados de la severidad se muestran en la siguiente tabla:

Tabla 14. Análisis de severidad de los riesgos identificados para la implementación del servicio IPTV en CANTV

Riesgos	Consecuencia	Probabilidad	Severidad
R1	4	3	E
R2	4	2	A
R3	4	2	A
R4	4	3	E
R5	3	3	A
R6	4	2	A
R7	4	2	A
R8	4	2	A
R9	3	3	A
R10	3	3	A
R11	3	3	A
R12	4	3	E
R13	3	3	A
R14	4	2	A
R15	3	1	M
R16	4	3	E

4.4 FASE 4: EVALUACIÓN DE RIESGOS

En esta fase de evaluación se realizó la comparación de los niveles de riesgo encontrados contra los criterios preestablecidos por la Gerencia de Seguridad de la Operación descritos en la fase 1, para establecer si los

mismos son aceptables, reducidos o evitados. Así mismo fueron ordenados y priorizados para su tratamiento de acuerdo a los resultados de severidad determinados por el análisis efectuado en la fase 3.

En la tabla 15 se puede observar que los 16 riesgos analizados, se encuentran distribuidos por severidad de la siguiente manera:

- Cuatro (4) riesgos con severidad extrema.
- Once (11) riesgos con severidad alta
- Un (1) riesgo con severidad moderada.

En este sentido, en la fase 5 " Tratamiento de Riesgos", serán definidos los planes de acción para la mitigación todos los riegos operacionales identificados y analizados para la implementación del servicio IPTV en CANTV.

Tabla 15. Escala de riesgos según severidad analizada para la implementación del servicio IPTV en CANTV.

Riesgos	Descripción	Consecuencia	Probabilidad	Severidad
R1	Implementación de las adecuaciones lógicas en la red MetroEthernet, que presenten errores en la configuración de las plantillas sobre los SW Alcatel 7450	4	3	E
R16	Operación del servicio IPTV, con deficiencia en los procesos de operación y mantenimiento para este nuevo producto.	4	3	E
R4	Aprovisionamiento del servicio IPTV en los equipos DSLAM IP, que originen fallas en el desempeño de los equipos ALCATEL 7302 en el otorgamiento del servicio de datos (Internet)	4	3	E
R12	Violaciones a la seguridad de los sistemas de autenticación de usuarios del servicio IPTV, al no contar con mecanismos que restrinjan el acceso de otros STB.	4	3	E

Riesgos	Descripción	Consecuencia	Probabilidad	Severidad
R2	Implementación de las adecuaciones en la red troncal IP, que presenten errores en la plantillas sobre los Router Cisco 12000	4	2	A
R3	Implementación de las adecuaciones en la red de acceso, que presenten errores en la plantillas sobre los DSLAM IP Alcatel 7302	4	2	A
R7	Fallas en los elementos del mediador, por ausencia de un plan redundancia física y lógica de cada uno de los elementos que conforman el subsistema mediador de la plataforma IPTV.	4	2	A
R6	Fallas en los elementos de la cabecera de video, por ausencia de un plan redundancia física y lógica de cada uno de los elementos que conforman el subsistema Headend de la plataforma IPTV.	4	2	A
R9	Inversión riesgosa en la plataforma IPTV, al no contar con la arquitectura apropiada de red de acceso para otorgar el servicio al usuario final.	3	3	A
R11	Incremento en la capacidad de asignación de direcciones IP a los STB y Módems, por ausencia de una planeación de capacidad adecuada de los servidores actuales de DHCP.	3	3	A
R14	Pago de sanciones, por incumplimiento de las reglas de regulación para la medición de las métricas de calidad del servicio para IPTV definidas por CONATEL	4	2	A
R5	Fallas en los equipos DSLAM IP, por no contar con redundancia de equipos, interfaces y energía de estos elementos.	3	3	A
R10	Definición inapropiada de mecanismos para proveer denegación de servicio a las peticiones de VoD, al presentarse congestiones de red y servicio.	3	3	A
R13	Fallas en la red de CANTV que superen el tiempo promedio de cambio de canal mayor a 2 segundos,	3	3	A
R8	Fallas en los elementos que dan soporte al servicio de video bajo demanda, al no contar con un plan de redundancia de los servidores de video bajo demanda.	4	2	A
R15	Implementación de un sistema de gestión con deficiencias para cumplir con los requerimientos de operación y mantenimiento de la Plataforma IPTV siguiendo las políticas corporativas..	3	1	M

4.5 FASE 5: TRATAMIENTO DE RIESGOS

De acuerdo a la escala de riesgos mostrada en la tabla 15 y el nivel de riesgo preestablecido por la organización para su tratamiento, fueron evaluados con cada una de las áreas responsables las estrategias y planes de acción específicos, para reducir cada uno de los riesgos a los niveles aceptados por la organización.

Lo expresado anteriormente se puede observar en la siguiente tabla:

Tabla 16. Definición de los Planes de Acción para el tratamiento de los riesgos evaluados para la implementación del servicio IPTV en CANTV.

R	DESCRIPCIÓN DEL RIESGO	S	PLANES DE ACCIÓN
R1	Implementación de las adecuaciones lógicas en la red MetroEthernet, que presenten errores en la configuración de las plantillas sobre los SW Alcatel 7450	E	• Definir e implementar controles de seguridad que permitan evaluar la ejecución y certificación de funcionamiento de las adecuaciones sobre la red ME. • Presentar cronograma de ejecución de las adecuaciones de la red Metro Ethernet para el soporte de los servicios IPTV.
R16	Operación del servicio IPTV, con deficiencia en los procesos de operación y mantenimiento para este nuevo producto.	E	• Desarrollar un modelo de proceso de operación y mantenimiento, que detalle las funciones, responsabilidades y procedimiento para el control del servicio IPTV dentro de las distintas áreas operativas impactadas con la entrada a producción de este servicio. • Revisar los procedimientos actuales para la operación y mantenimientos de los servicios actuales de voz y datos, para su adaptación dentro del modelo de procesos a desarrollar.
R4	Aprovisionamiento del servicio IPTV en los equipos DSLAM IP, que originen fallas en el desempeño de los equipos ALCATEL 7302 en el otorgamiento del servicio de datos (Internet)	E	• Definir e implementar controles de seguridad que permitan evaluar la ejecución y certificación de funcionamiento. • Definir e implementar controles de seguridad para mitigar la degradación del servicio de datos (ABA)

R	DESCRIPCIÓN DEL RIESGO	S	PLANES DE ACCIÓN
R12	Violaciones a la seguridad de los sistemas de autenticación de usuarios del servicio IPTV, al no contar con mecanismos que restrinjan el acceso de otros STB.	E	• Validar los niveles de seguridad definidos por el proveedor ZTE, que garanticen la negación del servicio a usuarios no autentificados dentro del sistema. • Definir e implementar políticas que garanticen la negación del servicio a usuarios no autentificados dentro del sistema.
R2	Implementación de las adecuaciones en la red troncal IP, que presenten errores en la plantillas sobre los Router Cisco 12000	A	•Definir e implementar controles de seguridad que permitan evaluar la ejecución y certificación de funcionamiento de las adecuaciones sobre la Red Troncal IP (BBIP) • Presentar cronograma de ejecución de las adecuaciones de la Red Troncal IP para el soporte de los servicios IPTV.
R3	Implementación de las adecuaciones en la red de acceso, que presenten errores en la plantillas sobre los DSLAM IP Alcatel 7302	A	•Definir e implementar controles de seguridad que permitan evaluar la ejecución y certificación de funcionamiento. •Cronograma de ejecución para la activación de las licencias multicast en los nodos de la res de acceso.
R7	Fallas en los elementos del mediador, por ausencia de un plan redundancia física y lógica de cada uno de los elementos que conforman el subsistema mediador de la plataforma IPTV.	A	• Definir un plan de redundancia de los servicios de TV de CANTV, a través de un análisis de las plataformas disponible que permitan establecer los elementos técnicos y de arquitectura de red necesarios del subsistema mediador.
R6	Fallas en los elementos de la cabecera de video, por ausencia de un plan redundancia física y lógica de cada uno de los elementos que conforman el subsistema Headend de la plataforma IPTV.	A	• Definir un plan de redundancia de los servicios de TV de CANTV, a través de un análisis de las plataformas disponible que permitan establecer los elementos técnicos y de arquitectura de red necesarios del Headend.
R9	Inversión riesgosa en la plataforma IPTV, al no contar con la arquitectura apropiada de red de acceso para otorgar el servicio al usuario final.	A	• Definir clientes que cumplen con las condiciones técnicas para la prestación del servicio de video. •Evaluar y definir requerimientos para la implementación del Proyecto 4TEL II, de acuerdo a los elementos de red de acceso (DSLAM IP) que se tiene planificado prestaran el servicio de TV. • Realizar pruebas sobre la ultima milla, para la medición de la calidad del cobre para llegar hasta los predios del cliente. • Definir un documento de "Especificación de Casos de Uso - IPTV".

R	DESCRIPCIÓN DEL RIESGO	S	PLANES DE ACCIÓN
R11	Incremento en la capacidad de asignación de direcciones IP a los STB y Módems, por ausencia de una planeación de capacidad adecuada de los servidores actuales de DHCP.	A	• Controles establecidos para mitigación de degradación de otros servicios. • Evaluar con la Gcia. Arquitectura Redes, el dimensionamiento disponible para la entrada en producción del servicio IPTV para el primer año de operación.
R14	Pago de sanciones, por incumplimiento de las reglas de regulación para la medición de las métricas de calidad del servicio para IPTV definidas por CONATEL	A	• Implementar una solución para el monitoreo de la QoS que garantice la medición de los siguientes parámetros: perdida de paquetes, retraso (delay), Jitter, porcentaje de disponibilidad, entre otros. •Validar que la solución integradora garantice los valores de las métricas de QoS y QoE, definidos por CONATEL. •Supervisión de parámetros de operación del BBIP, Metro Ethernet, IPTV(Headend, Middleware y CPE), que permita certificación de operación dentro de umbrales de calidad establecidos.
R5	Fallas en los equipos DSLAM IP, por no contar con redundancia de equipos, interfaces y energía de estos elementos.	A	• Definir e implementar controles de seguridad que permitan evaluar la ejecución y certificación de funcionamiento. • Implementación de una herramienta de monitoreo para evaluación de la disponibilidad DSLAM IP
R10	Definición inapropiada de mecanismos para proveer denegación de servicio a las peticiones de VoD, al presentarse congestiones de red y servicio.	A	• Definir con el proveedor parámetros de mecanismos de negación de sesiones de VoD soportados por la plataforma. • Implementación y pruebas de certificación que garantices la negación de peticiones de VoD sobre la plataformas cuando se requiera. (congestión de la red de transporte, congestión en DSLAM IP, capacidad máxima de los servidores VOD alcanzados, etc.)
R13	Fallas en la red de CANTV que superen el tiempo promedio de cambio de canal mayor a 2 segundos,	A	• Evaluar si la solución de Calidad de Experiencia ofrecida por el proveedor ZTE, cuanta con este sistema de monitoreo. • Implementar sistema monitoreo que permita garantizar que los niveles de zapping time no excedan los 2 segundos.
R8	Fallas en los elementos que dan soporte al servicio de video bajo demanda, al no contar con un plan de redundancia de los servidores de video bajo demanda.	A	•Definir plan de redundancia física y/o lógica del servicio de video bajo demanda, a partir del segundo año de operación. •Definir con el proveedor los flujos de información, para los distintos casos de usos de la plataforma: Plataforma operativa, Nodo Central Falla, Nodo Edge Falla, Nodo Central y Edge Falla. •Definir e implementar listado de reglas para la configuración de la redundancia soportada por la plataforma. •Incluir dentro del modelo operativo (procesos), la definición y configuración de las políticas de redundancia a partir del 2do año de operación.

R	DESCRIPCIÓN DEL RIESGO	S	PLANES DE ACCIÓN
R15	Implementación de un sistema de gestión con deficiencias para cumplir con los requerimientos de operación y mantenimiento de la Plataforma IPTV siguiendo las políticas corporativas..	**M**	• Definir las áreas y sus funciones que requieran el uso de la gestión de la solución IPTV, a fin de que la solución de gestión soporte tanto la cantidad máxima de usuarios, como la cantidad de usuarios concurrentes • Certificar visualización en forma gráfica de las alarmas/eventos utilizando una codificación de 'íconos' de colores, sobre los mapas de red y de topología, manejo de consola de alarmas. • Soporte de envío de alarmas/eventos a sistemas OSS (p.ej. SNMP) • Manejo de políticas corporativas para el control de acceso al sistema de gestión. • Manejo de perfiles específicos por usuarios

4.6 FASE 6: MONITOREO Y REVISIÓN

En esta última fase, se contemplaron dos mecanismos que permitieran monitorear y revisar el desempeño del proceso de gestión de riesgo, logrando una comunicación efectiva entre los involucrados y asegurando la oportuna y apropiada generación, recolección, control y distribución de la información.

A continuación se presentan las dos herramientas que se desarrollaron:

4.6.1 Estatus Quincenal

Este mecanismo permite confirmar las prioridades quincenalmente, a través del seguimiento de las actividades aplicadas para el cumplimiento de los planes de acción definidos con los responsables de las unidades operativas. De esta manera se reducen las posibilidades de perder el control del proceso, ya que se cuenta con información confiable, a tiempo, y son identificadas las desviaciones oportunamente, para implementar la acción correctiva requerida.

Las estrategias aplicadas consisten de:

- Envío de correo eléctrico a las unidades responsables, para verificar las actividades y ejecución de los planes de acción.
- Documentación los avances dentro de la herramienta ERA, a fin de mantener el histórico de las comunicaciones y documentación del proceso.

4.6.2 Reporte Mensual

El documento generado informa mensualmente a los involucrados claves y la alta gerencia sobre el desempeño del proceso de gestión de riesgos y presenta recomendaciones sobre tendencias y prioridades.

El informe mensual se compone de dos documentos, el primero de ellos muestra la gráfica de riesgo actualizada y el detalle de severidad de cada uno de estos; de la misma manera se reporta un avance gerencial en el cual se presenta: porcentaje de avance físico, logros alcanzados, desviaciones y próximos pasos. (Ver anexo 5)

CAPÍTULO V

MAPA OPERACIONAL DE RIESGOS

La propuesta y enfoque de este trabajo se presenta en este Capítulo, con la elaboración del mapa operacional de riesgos para la implementación del servicio IPTV en CANTV, utilizando la herramienta ERA adquirida por la Gerencia de Seguridad de la Operación para la gestión automatizada del riesgo operacional.

5.1 HERRAMIENTA ERA- ENTERPRISE RISK ASSESSOR

ERA (Enterprise Risk Assessor) es una solución para gestión de riesgos a nivel corporativo, la cual combina la integridad de los estándares ISO 31000 y AS/NZS: 4360 con los conocimientos de expertos a nivel mundial, permitiendo estructurar modelos de riesgo con base en el modelo COSO, ISO 17799 y otros.

El desarrollador de esta herramienta es Methodware, una empresa líder mundial en la producción de software de Gestión del riesgo y Auditoria, los cuales soportan los estándares internacionales, para apoyar la implementación estructurada, efectiva y eficiente de proyectos.

ERA brinda los siguientes beneficios a una organización:

- La habilidad de automatizar todos los aspectos del enfoque de riesgo en una herramienta dinámica, con una estructura de riesgo personalizada y un repositorio central compartido que puede ser accedido por Auditores Internos, Gerentes de Riesgo, Gerentes de Negocio, el Directorio y todos los otros interesados.

- Consolidación, rastreo y monitoreo de la información de riesgo y auditoría en el tiempo.
- Registro de incidentes de pérdida y pérdidas potenciales alineados con los riesgos, con la habilidad de rastrear indicadores claves de desempeño de los riesgos.

Figura 40. Estándares integrados ERA. Fuente: GIT Soluciones Integrales

ERA provee una representación clara de la información de riesgos a cualquier nivel de la organización mediante el uso de mapas y de información gráfica clave, incluyendo:

- Mapas que muestran datos comparativos de riesgos.
- Matrices de riesgos para evaluación grafica del riesgo.
- Tablas Pivot para analizar información detallada por criterios variables.
- Consolidar y mostrar datos de riesgos por unidad individual de negocio o a través de toda la empresa.
- Reportar en formatos estándar (MS Word/Excel) sobre todos los riesgos e información de auditoría.

El proceso para de desarrollo del mapa operacional de riesgos en la herramienta ERA se basa en los siguientes tres pasos:

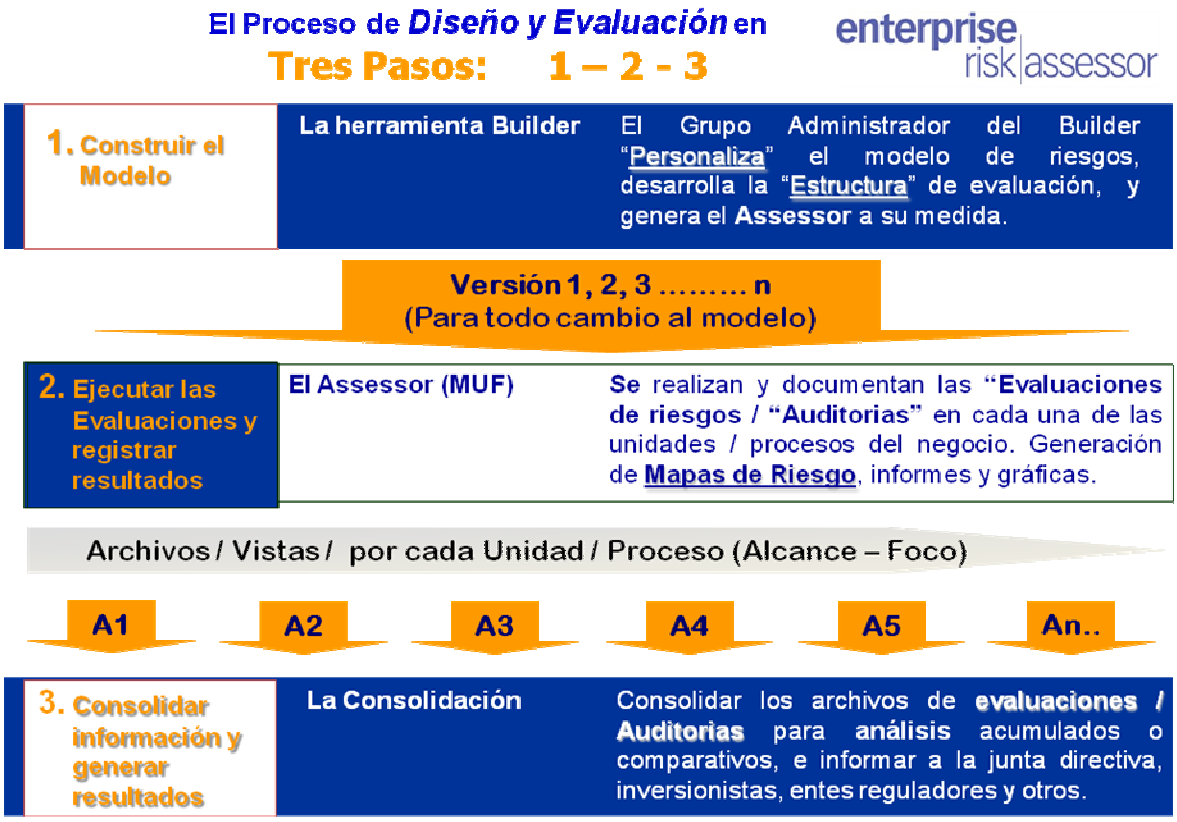


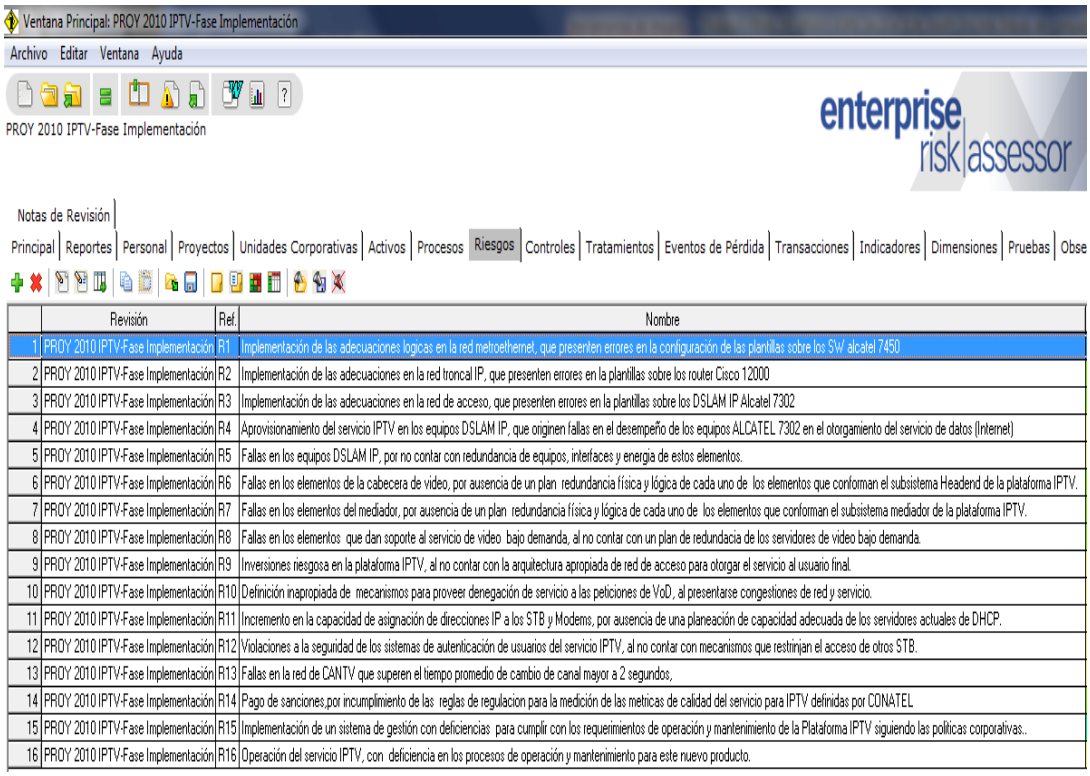
Figura 41. Proceso de Diseño y Evaluación en ERA. Fuente: GIT Soluciones Integrales.

5.2 DISEÑO MAPA OPERACIONAL DE RIESGOS PARA LA IMPLEMENTACIÓN DEL SERVICIO IPTV EN CANTV.

La elaboración del mapa operacional de riesgos para la implementación del servicio IPTV en CANTV, se realizó utilizando la herramienta ERA adquirida por la Gerencia de Seguridad de la Operación, tomando como fuentes de datos los resultados obtenidos en cada una de las

seis fases descritas por el estándar ISO 31000 para la administración de riesgos. Cada parte de esta información se cargó dentro del software adquirido por la unidad antes mencionada, siguiendo el orden que se describe a continuación:

1. **Documentación de riesgos:** con los resultados obtenidos de la identificación de los riesgos asociados a la implementación del servicio IPTV en CANTV, descritos en la tabla 9 del capítulo IV, se procedió a cargar los 16 eventos analizados, obteniendo como resultado final la siguiente vista:



	Revisión	Ref.	Nombre
1	PROY 2010 IPTV-Fase Implementación	R1	Implementación de las adecuaciones logicas en la red metroethernet, que presenten errores en la configuración de las plantillas sobre los SW alcatel 7450
2	PROY 2010 IPTV-Fase Implementación	R2	Implementación de las adecuaciones en la red troncal IP, que presenten errores en la plantillas sobre los router Cisco 12000
3	PROY 2010 IPTV-Fase Implementación	R3	Implementación de las adecuaciones en la red de acceso, que presenten errores en la plantillas sobre los DSLAM IP Alcatel 7302
4	PROY 2010 IPTV-Fase Implementación	R4	Aprovisionamiento del servicio IPTV en los equipos DSLAM IP, que originen fallas en el desempeño de los equipos ALCATEL 7302 en el otorgamiento del servicio de datos (Internet)
5	PROY 2010 IPTV-Fase Implementación	R5	Fallas en los equipos DSLAM IP, por no contar con redundancia de equipos, interfaces y energía de estos elementos.
6	PROY 2010 IPTV-Fase Implementación	R6	Fallas en los elementos de la cabecera de video, por ausencia de un plan redundancia física y lógica de cada uno de los elementos que conforman el subsistema Headend de la plataforma IPTV.
7	PROY 2010 IPTV-Fase Implementación	R7	Fallas en los elementos del mediador, por ausencia de un plan redundancia física y lógica de cada uno de los elementos que conforman el subsistema mediador de la plataforma IPTV.
8	PROY 2010 IPTV-Fase Implementación	R8	Fallas en los elementos que dan soporte al servicio de video bajo demanda, al no contar con un plan de redundacia de los servidores de video bajo demanda.
9	PROY 2010 IPTV-Fase Implementación	R9	Inversiones riesgosa en la plataforma IPTV, al no contar con la arquitectura apropiada de red de acceso para otorgar el servicio al usuario final.
10	PROY 2010 IPTV-Fase Implementación	R10	Definición inapropiada de mecanismos para proveer denegación de servicio a las peticiones de VoD, al presentarse congestiones de red y servicio.
11	PROY 2010 IPTV-Fase Implementación	R11	Incremento en la capacidad de asignación de direcciones IP a los STB y Modems, por ausencia de una planeación de capacidad adecuada de los servidores actuales de DHCP.
12	PROY 2010 IPTV-Fase Implementación	R12	Violaciones a la seguridad de los sistemas de autenticación de usuarios del servicio IPTV, al no contar con mecanismos que restrinjan el acceso de otros STB.
13	PROY 2010 IPTV-Fase Implementación	R13	Fallas en la red de CANTV que superen el tiempo promedio de cambio de canal mayor a 2 segundos,
14	PROY 2010 IPTV-Fase Implementación	R14	Pago de sanciones,por incumplimiento de las reglas de regulacion para la medición de las metricas de calidad del servicio para IPTV definidas por CONATEL
15	PROY 2010 IPTV-Fase Implementación	R15	Implementación de un sistema de gestión con deficiencias para cumplir con los requerimientos de operación y mantenimiento de la Plataforma IPTV siguiendo las politicas corporativas..
16	PROY 2010 IPTV-Fase Implementación	R16	Operación del servicio IPTV, con deficiencia en los procesos de operación y mantenimiento para este nuevo producto.

Figura 42. Identificación de Riesgos en la herramienta ERA. Fuente: Elaboración propia.

2. **Análisis de riesgos:** con los resultados mostrados en la Tabla 10 para el análisis de consecuencias y en el anexo 4 para el análisis de probabilidades de los 16 riesgos identificados, se procedió a realizar la carga de información en la herramienta ERA, en la cual de acuerdo a las reglas definidas en el modelo, se pueden obtener los tres tipos de valoración de la severidad para el riesgo absoluto, a través de la combinación de los valores de probabilidad y consecuencias definidas para cada riesgo. En otras palabras, es posible identificar si el riesgo definido se encuentra en la escala de: Extremo, Alto, Moderado o Bajo.

En la figura 43 la pantalla de valoración del riesgo 1, en la cual el valor de probabilidad se representa como “posible” y el de consecuencia o impacto se califica como “mayor”, obteniendo un nivel de riesgo o severidad “Extrema”, que de acuerdo a las premisas definidas en el capitulo anterior requerirá de la definición de un plan de acción para iniciar la acción de mitigación del mismo, hasta que su nivel de severidad disminuya para poder ser aceptado por la unidad.

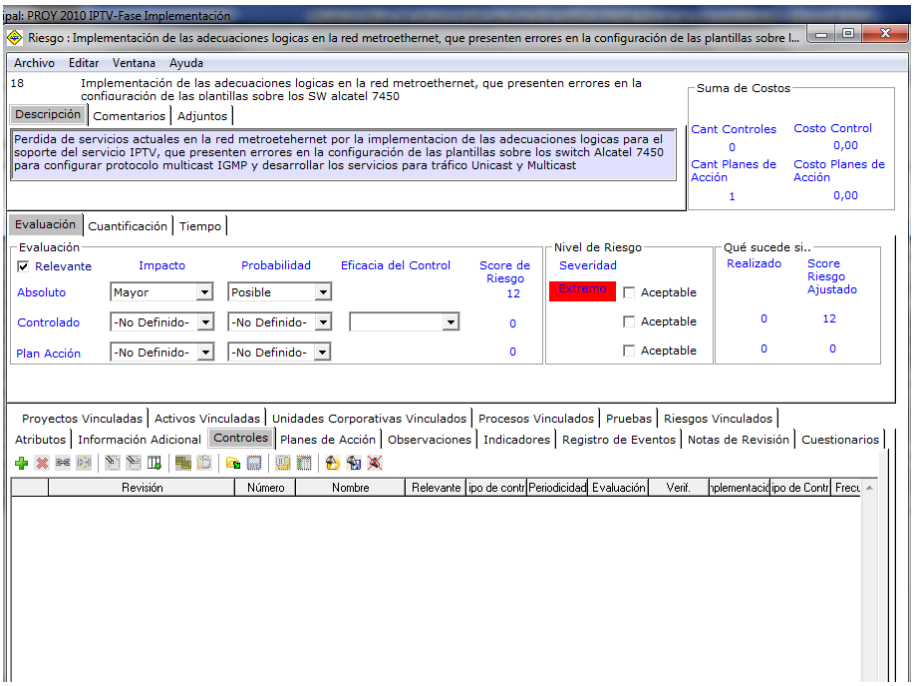
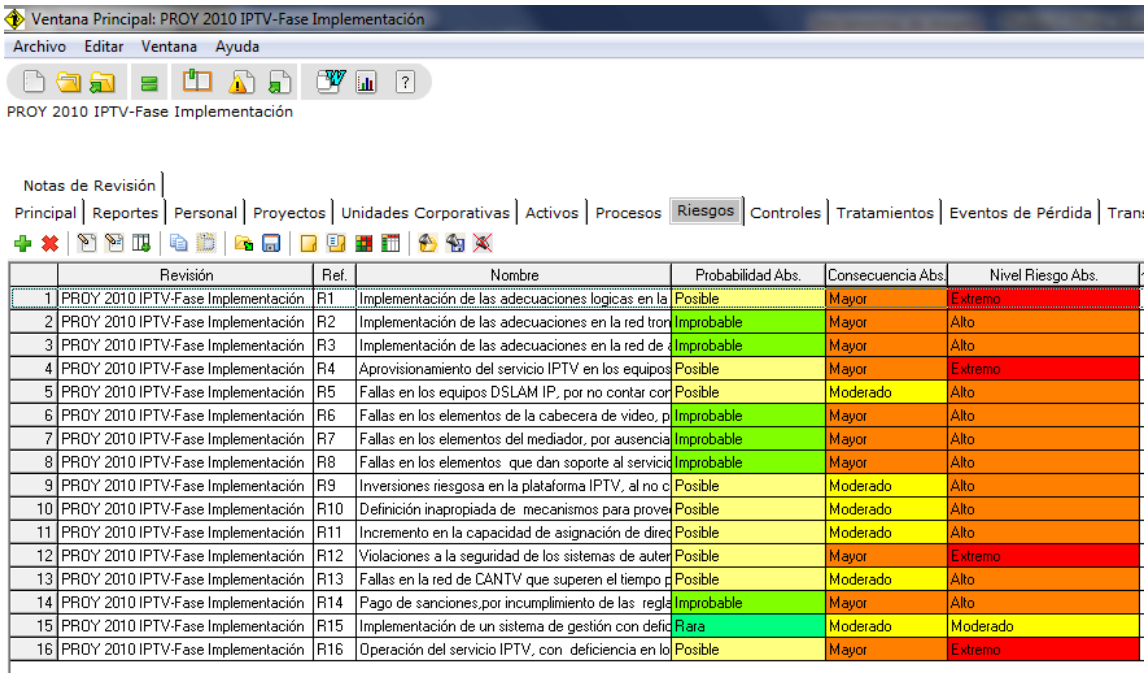


Figura 43. Valoración de riesgos en la Herramienta ERA. Fuente: Elaboración propia.

El procedimiento indicado en el párrafo anterior se efectuó para cada uno de los 16 eventos identificados, y el resultado consolidado de la evaluación se presenta de la siguiente manera:



	Revisión	Ref.	Nombre	Probabilidad Abs.	Consecuencia Abs.	Nivel Riesgo Abs.
1	PROY 2010 IPTV-Fase Implementación	R1	Implementación de las adecuaciones logicas en la	Posible	Mayor	Extremo
2	PROY 2010 IPTV-Fase Implementación	R2	Implementación de las adecuaciones en la red tron	Improbable	Mayor	Alto
3	PROY 2010 IPTV-Fase Implementación	R3	Implementación de las adecuaciones en la red de a	Improbable	Mayor	Alto
4	PROY 2010 IPTV-Fase Implementación	R4	Aprovisionamiento del servicio IPTV en los equipos	Posible	Mayor	Extremo
5	PROY 2010 IPTV-Fase Implementación	R5	Fallas en los equipos DSLAM IP, por no contar con	Posible	Moderado	Alto
6	PROY 2010 IPTV-Fase Implementación	R6	Fallas en los elementos de la cabecera de video, p	Improbable	Mayor	Alto
7	PROY 2010 IPTV-Fase Implementación	R7	Fallas en los elementos del mediador, por ausencia	Improbable	Mayor	Alto
8	PROY 2010 IPTV-Fase Implementación	R8	Fallas en los elementos que dan soporte al servicio	Improbable	Mayor	Alto
9	PROY 2010 IPTV-Fase Implementación	R9	Inversiones riesgosa en la plataforma IPTV, al no c	Posible	Moderado	Alto
10	PROY 2010 IPTV-Fase Implementación	R10	Definición inapropiada de mecanismos para prove	Posible	Moderado	Alto
11	PROY 2010 IPTV-Fase Implementación	R11	Incremento en la capacidad de asignación de direc	Posible	Moderado	Alto
12	PROY 2010 IPTV-Fase Implementación	R12	Violaciones a la seguridad de los sistemas de auter	Posible	Mayor	Extremo
13	PROY 2010 IPTV-Fase Implementación	R13	Fallas en la red de CANTV que superen el tiempo p	Posible	Moderado	Alto
14	PROY 2010 IPTV-Fase Implementación	R14	Pago de sanciones,por incumplimiento de las regla	Improbable	Mayor	Alto
15	PROY 2010 IPTV-Fase Implementación	R15	Implementación de un sistema de gestión con defic	Rara	Moderado	Moderado
16	PROY 2010 IPTV-Fase Implementación	R16	Operación del servicio IPTV, con deficiencia en lo	Posible	Mayor	Extremo

Figura 44. Nivel de severidad de riesgos en la Herramienta ERA.
Fuente: Elaboración propia.

De acuerdo a resultados obtenidos con la evaluación de probabilidad y consecuencia, se puede observar en la figura 44, los niveles de severidad de riesgos obtenidos con la simulación de la herramienta ERA, los cuales presentaron resultados similares a los obtenidos en el análisis del capítulo IV: cuatro (4) riesgos con severidad “Extrema”, once (11) riesgos con severidad “Alta” y un (1) riesgo con severidad moderada.

3. **Identificación de responsables:** una vez completado el paso anterior, se procedió a realizar la carga de las gerencias responsables de cada uno de los riesgos identificados. Para ello se utilizó la opción “Unidades corporativas vinculadas”, a la cual se accede haciendo clic en cada uno de los riesgos identificados para cargar los nombres de las unidades identificadas en el capitulo anterior. El resultado obtenido

se puede apreciar por unidades corporativas asignadas de la siguiente manera:

a. Riesgos asignados a la Gerencia General de Servicios Audiovisuales (GGSA)

Figura 45. Riesgos vinculados a la GGSA en la Herramienta ERA. Fuente: Elaboración propia.

b. Riesgos asignados a la Gerencia General de Proyectos Mayores (GGPM)

Figura 46. Riesgos vinculados a la GGPM en la Herramienta ERA. Fuente: Elaboración propia.

c. Riesgos asignados a la Gerencia General de Tecnología y Operaciones (GGTO)

Figura 47. Riesgos vinculados a la GGTO en la Herramienta ERA. Fuente: Elaboración propia.

d. Riesgos asignados a la Gerencia General de Planificación y Asuntos Corporativos (GGPAC)

Figura 48. Riesgos vinculados a la GGPAC en la Herramienta ERA. Fuente: Elaboración propia.

e. Riesgos asignados a la Gerencia General de Seguridad Integral

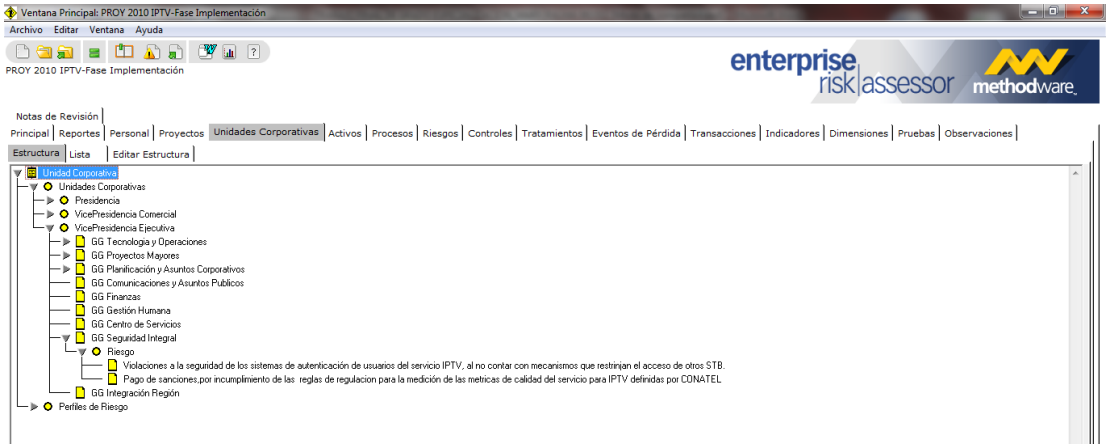


Figura 49. Riesgos vinculados a la GGSI en la Herramienta ERA. Fuente: Elaboración propia.

4. **Documentación de los Planes de Acción:** para cada uno de los 16 riesgos identificados y tomando como base los resultados en la tabla 15, para los cuales el nivel de severidad oscila entre “Extremo” y “Moderado”, se desarrollaron los planes de acción requeridos para mitigar cada uno de estos hasta un valor de severidad “Bajo”, el cual corresponde a el criterio de aceptación definido por la organización.

   La carga de esta información dentro de la herramienta ERA, se realizó a través de la opción “Planes de Acción” habilitada dentro de cada ventana de riesgo, tal y como se ilustra en la figura 50. En la pantalla que despliega el sistema, es posible habilitar campos importantes para el seguimiento como lo son: prioridad, estado, fecha de registrado, fecha de objetivo, fecha de completado, etc.

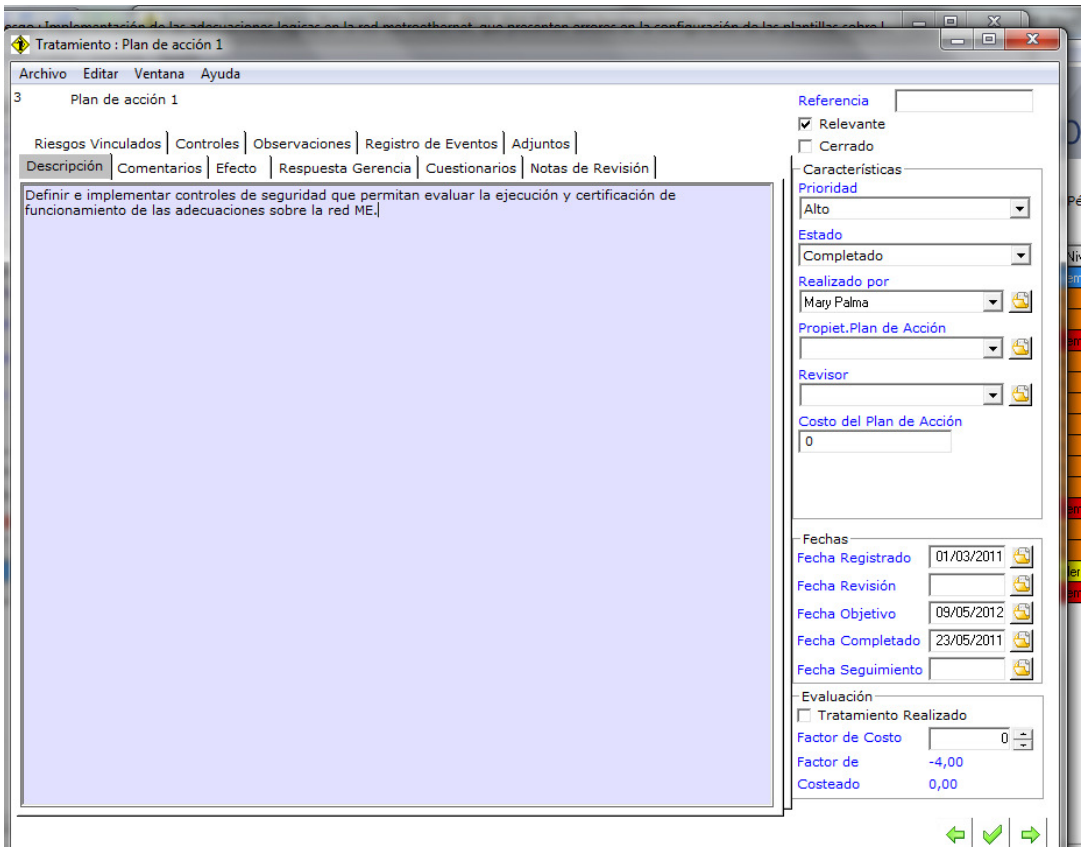


Figura 50. Plan de acción 1 documentado en la Herramienta ERA.
Fuente: Elaboración propia.

Para los 16 riesgos evaluados, fueron descritos un total de 37 planes acción en acuerdo con cada una de las áreas responsables (Ver anexo 6). Actualmente la mayoría de los planes definidos se encuentran en proceso de ejecución por parte de las unidades responsables con la finalidad de mitigar los impactos evaluados y garantizar la salida comercial del producto IPTV con la menor cantidad de brechas operativas que pudieran impactar la calidad del servicio y la imagen corporativa de la empresa.

5. **Seguimiento y control:** De acuerdo a la metodología definida en la fase 6 para el monitoreo y revisión de riesgos para la implementación del servicio IPTV en CANTV, es factible medir los resultados

quincenales generados por las unidades responsables, con lo cuales se procede a la actualización de los avances en la ejecución de los planes de acción y con ello el nivel de severidad de los riesgos, de tal manera de garantizar la mitigación de los riesgos según lo planificado.

Así mismo, a través de la Herramienta ERA es factible generar automáticamente informes de seguimiento que permitan mostrar a la línea directiva el seguimiento y control del plan. Los reportes y formularios disponibles en ERA, se muestran en la siguiente imagen:

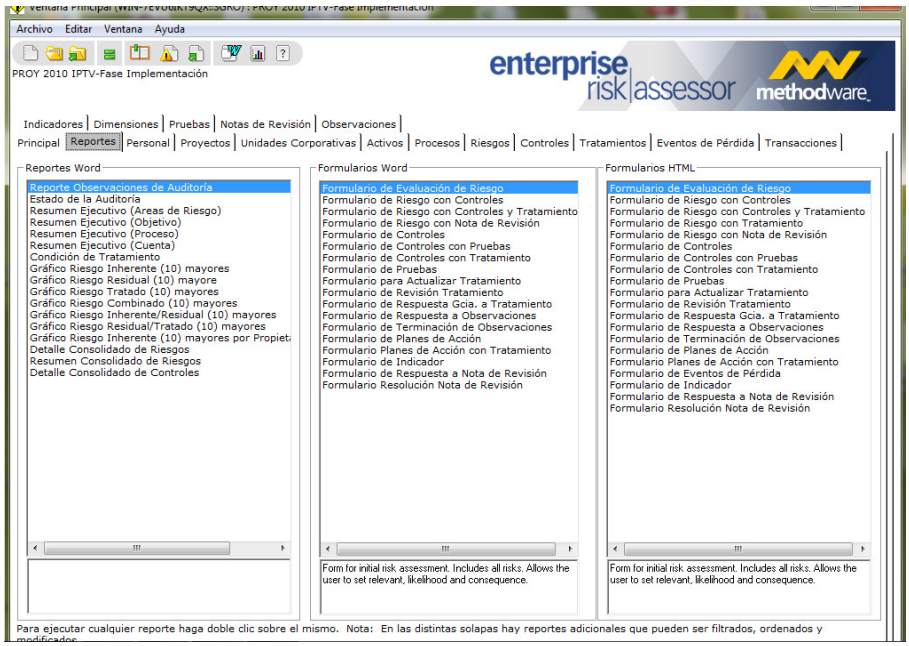


Figura 51. Formularios de Reportes de la Herramienta ERA. Fuente: Herramienta ERA

CONCLUSIONES

1. Lo importante en la adopción de un modelo de gestión de riesgos es que este sea fácilmente comprensible en la organización, que sea el directorio quien tome decisiones basadas en riesgos, que la implementación del modelo sea liderada por la alta gerencia y finalmente que la responsabilidad de los riesgos sea encabezada por unidades de negocio y sus áreas funcionales, para lograr un manejo inteligente en materia de riesgos.

2. Es muy importante resaltar que IPTV es un servicio en el que CANTV tienen el escenario más propicio, puesto que estarían ofreciendo un servicio adicional a los usuarios a través de la misma infraestructura de red, lo que implica poca inversión en función de las ganancias. Sobre todo por la capacidad de captar a los clientes de telefonía y ABA agregando la TV.

3. El requerimiento de calidad de servicio, es uno de los factores de ingeniería más desafiantes en el momento de implementar el servicio IPTV sobre la red de acceso ADSL, que en el caso de CANTV es tema mitigado gracias al control aplicado en cuanto a la implementación de una plataforma independiente que permita realizar las mediciones del desempeño de la red en el otorgamiento del servicios hacia los usuarios finales.

4. Con el despliegue efectivo de IPTV, CANTV ofrecerá el servicio de “triple play” (telefonía, Internet y televisión) que es un servicio de última tecnología y además se optimiza recursos debido a que a través de una misma infraestructura se proporciona este tipo de servicio y el usuario dispone de una cantidad enorme de aplicaciones, que le permitirán obtener una mejor calidad de vida y un aprovechamiento de los avances tecnológicos en un porcentaje muy elevado.

5. IPTV es un servicio completamente nuevo dentro del portafolio de productos de CANTV, que se apalancará de la experiencia adquirida en los otros servicios que pueden considerarse similares en ciertos aspectos (ABA). Serán aplicados los modelos de negocios y servicios similares a los de las redes de televisión por abonados, incluyendo valores agregados como el VoD, TSTV, PVR y guía de programación de interactiva (EPG).

6. La necesidad de gestionar riesgos, aplica a todas las organizaciones y a todas sus funciones y actividades, y se debería reconocer como de importancia fundamental por todos los directivos y el personal.

RECOMENDACIONES

1. Se recomienda a la Gerencia de Seguridad de la Operación el uso continuo de la Herramienta ERA, ya que esta solución tecnológica juega un rol clave en el proceso de automatización de las tareas de la unidad y contribuyen a reducir los tiempos de respuestas de los análisis requeridos.

2. Aplicar y mantener el seguimiento de ejecución de los planes de acción definidos para mitigar las brechas de la implementación del servicio IPTV, a fin de garantizar, que para la fecha de salida comercial del producto, se encuentren aceptados en su totalidad el nivel de severidad de los riesgos

3. Como segunda fase, diseñar, asesorar e implementar los planes de minimización de riesgos potenciales y vulnerabilidades de servicio y antifraude durante la operación del servicio IPTV, que permitan mantener la calidad hacia a las comunidades y maximizar los ingresos de la empresa.

4. Implementar mecanismos de disuasión y divulgación de Seguridad de Operación a CANTV y sus empresas filiales, comunidades y a otras operadoras, para crear cultura de riesgo.

5. Formular y ejecutar los planes de mitigación de Seguridad de Operación, involucrando a las áreas responsables de riesgo para cerrar brechas e identificar oportunidades de mejora, que permitan contribuir con el cumplimiento de las metas de ingresos de la Gerencia.

6. Definir los mapas para establecer los procesos en la administración de riesgo operacional, de plataformas, productos, servicios, procesos nuevos y/o existentes, que sean de gran impacto para la empresa.

BIBLIOGRAFÍA

Referencias bibliograficas:

1. ATIS (2008*). IPTV Interoperability Forum.*
2. CANTV (2006). *Arquitecturas de redes y Plataformas de servicios de Cantv.*
3. CANTV (2007). *Arquitectura de Referencia Servicio de Difusión por Suscripción IPTV.*
4. CANTV (2009). *Descripcion del proyecto PDP-IPTV.*
5. GHASSEM ,KOLEYNI (2008). *ITU-T Focus Group on Internet Protocol Television (FG IPTV).*
1. MASAHITO, KAWAMORI (2008). *Recent Trends in Standardization of IPTV Technologies*
2. OCALLAGHAN, DANIEL (2008). *ATIS IPTV Standards Development via*

   ATIS IPTV Interoperability Forum (IIF).
3. Tanenbaum, Andrew (2003). *Redes de computadora cuarta edición*. Mexico: Limusa.
4. UCV (2008). *Instructivo y normalización para la elaboración de trabajos especiales de grado.*

5. UPEL (2006). *Manual de Trabajos de Grado de Especialización y Maestría y Tesis Doctorales.* Venezuela: FEDUPEL.

Referencias Electronicas:

1. Bank For International Stettlements (2011). Comite Basilea. Consultada 17 de Julio de 2011, http://www.bis.org/bcbs/about.htm?ql=1
2. Enterprise Risk Assessor ERA Version 6 (2010).Consultada el 04 de octubre del 2010, en enterprise risk assessor methoware.
3. GIT Soluciones Integrales (2010). Solucion integral para la implementación de un sistema de administracion del riesgo operacional. Consultado el 12 Octubre del 2010, http://www.gitltda.com/noticias/ERA-WEB.pdf
4. International Organization for Standardization(2010).Estándar ISO 31000. Consultada el 12 de octubre del 2010, http://www.iso.org/iso/catalogue_detail.htm?csnumber=43170.
5. Difusion multicast (2010). Consultada el 05 de noviembre 2010, http://halley.ls.fi.upm.es/~jyaguez/pdfs/librounimultidifu.pdf

6. ETSI TISPAN (2010). TISPAN. Defining the Next Generation Network. Consultada el 02 de diciembre de 2010, http://www.etsi.org/tispan/tispan.htm

7. TURBOTELTIC Cia. Ltda (2010). IPTV. Consultada el 05 de noviembre de 2010, http://www.grupoturbo.com/IPTV.html

ANEXO 1

BUENAS PRÁCTICAS PARA LA GESTIÓN Y SUPERVISIÓN DEL RIESGO OPERATIVO

ANEXO 2

COMITÉ DE BASILEA – CATEGORÍAS EVENTOS DE PÉRDIDA

ANEXO 3

MATRIZ DE ÁREA DE IMPACTO VS. FUENTES DE RIESGO

ANEXO 4

ANÁLISIS DE PROBABILIDADES- TÉCNICA DEL SCORING

ANEXO 5

REPORTE MENSUAL

ANEXO 6

DOCUMENTACIÓN DE LOS PLANES DE ACCIÓN