UNIVERSIDAD CATÓLICA ANDRÉS BELLO
VICERRECTORADO ACADÉMICO
ESTUDIOS DE POSTGRADO
AREA DE CIENCIAS ADMINISTRATIVAS Y DE GESTIÓN
POSTGRADO EN GERENCIA DE PROYECTOS

TRABAJO ESPECIAL DE GRADO

PROPUESTA DE UN PLAN PARA LA MEDICIÓN DEL RENDIMIENTO EN LA PLATAFORMA DE MONITOREO DE SEGURIDAD TECNOLÓGICA DE CANTV

presentado por:

Hernández Barrios Pedro Rafael

para optar al título de

Especialista en Gerencia de Proyectos

Asesor:

Guillén Guédez Ana Julia

Caracas, Septiembre de 2013

UNIVERSIDAD CATÓLICA ANDRÉS BELLO
VICERRECTORADO ACADÉMICO
ESTUDIOS DE POSTGRADO
AREA DE CIENCIAS ADMINISTRATIVAS Y DE GESTIÓN
POSTGRADO EN GERENCIA DE PROYECTOS

TRABAJO ESPECIAL DE GRADO

PROPUESTA DE UN PLAN PARA LA MEDICIÓN DEL RENDIMIENTO EN LA PLATAFORMA DE MONITOREO DE SEGURIDAD TECNOLÓGICA DE CANTV

presentado por:

Hernández Barrios Pedro Rafael

para optar al título de

Especialista en Gerencia de Proyectos

Asesor:

Guillén Guédez Ana Julia

Caracas, Septiembre de 2013

APROBACIÓN DEL ASESOR

Por la presente hago constar que he leído el borrador final del Trabajo Especial de Grado, presentado por el ciudadano, Hernández Barrios Pedro Rafael, titular de la C.I. V –16.578.636, para optar al grado de Especialista en Gerencia de Proyectos, cuyo título es "**PROPUESTA DE UN PLAN PARA LA MEDICIÓN DEL RENDIMIENTO EN LA PLATAFORMA DE MONITOREO DE SEGURIDAD TECNOLÓGICA DE CANTV** ", y manifiesto que cumple con los requisitos exigidos por la Dirección de los Estudios de Postgrado de la Universidad Católica Andrés Bello: y que, por lo tanto, lo considero apto para ser evaluado por el jurado que se decida designar para tal fin.

En la ciudad de Caracas, a los 10 días del mes de Julio de 2013.

_____

Ana Julia Guillén Guédez

CARTA DE AUTORIZACIÓN CANTV

Yo, Carolina Sarmiento Gallardo, en mi carácter de Coordinadora de la unidad Monitoreo de Seguridad, adscrita a la Gerencia de Seguridad Tecnológica, Gerencia General de Seguridad Integral de CANTV, por medio de la presente autorizo al Ing. **Pedro Rafael Hernández Barrios C.I 16.578.636**, a la realización del Trabajo Especial de Grado titulado ***PROPUESTA DE UN PLAN PARA LA MEDICIÓN DEL RENDIMIENTO EN LA PLATAFORMA DE MONITOREO DE SEGURIDAD TECNOLÓGICA*** en la Universidad Católica Andrés Bello (Ucab)

Autorización que se expide a petición de la parte interesada a los 10 (diez) días del mes de Julio del Año 2013.

Atentamente.

_____

Carolina Sarmiento Gallardo

Coordinadora de Monitoreo de Seguridad.

UNIVERSIDAD CATÓLICA ANDRÉS BELLO
VICERRECTORADO ACADÉMICO
ESTUDIOS DE POSTGRADO
AREA DE CIENCIAS ADMINISTRATIVAS Y DE GESTIÓN
POSTGRADO EN GERENCIA DE PROYECTOS

TRABAJO ESPECIAL DE GRADO

PROPUESTA DE UN PLAN PARA LA MEDICIÓN DEL RENDIMIENTO EN LA PLATAFORMA DE MONITOREO DE SEGURIDAD TECNOLÓGICA DE CANTV

Autor: Hernández Barrios Pedro Rafael.
Asesor: Guillén Guédez Ana Julia.
Año: 2013.

RESUMEN

En el referido contexto, el presente Trabajo Especial de Grado aborda la problemática de seguridad tecnológica de la Compañía Anónima Nacional Teléfonos de Venezuela, CANTV. En la actualidad, las fallas presentadas en la plataforma de monitoreo de seguridad tecnológica son solventadas sólo cuando algún operador las detecta y en muchas ocasiones son detectadas luego de un largo período de haber sucedido, ya que las herramientas con las que se cuenta actualmente no permiten la detección automática de fallas en la plataforma, por lo que es de vital importancia contar un sistema que detecte de forma inmediata todas y cada una de las fallas que puedan presentarse, para así aumentar su nivel de disponibilidad. Por las razones antes expuestas se plantean aplicar las herramientas de mejores prácticas de la Gerencia de Proyectos en el área de la gestión de los riesgos y de la calidad a fin de evaluar los diversos procesos que miden la criticidad de los eventos detectados en la plataforma de Monitoreo de Seguridad Tecnológica, con miras al diseño de un sistema de medición del rendimiento para la plataforma de monitoreo de seguridad tecnológica de CANTV. De acuerdo al problema de investigación que se plantea, el cual hace referencia a la propuesta de un plan para la medición del rendimiento en la plataforma monitoreo de seguridad tecnológica y en función de sus objetivos la investigación a realizar fue de tipo Aplicada, los resultados obtenidos recomendaron la utilización de la herramienta Nagios para la medición del rendimiento en dicha plataforma, apalancada por una propuesta que permitirá la correcta medición de los parámetros de rendimiento.

Palabras clave: Plan, Medición de Rendimiento, Seguridad Tecnológica, Monitoreo.

Línea de Trabajo: Gerencia de Proyectos Tecnológicos

INDICE DE CONTENIDO

ÍNDICE DE FIGURAS Y GRÁFICOS

CONTENIDO **Página.**

ÍNDICE DE CUADROS

CONTENIDO **Página**

INTRODUCCIÓN

La Compañía Anónima Teléfonos de Venezuela (CANTV), es una empresa del estado venezolano operadora y proveedora de soluciones integrales de telecomunicaciones e informática, la Gerencia de Seguridad Tecnológica de la CANTV es la encargada de velar por el cumplimiento de las políticas de seguridad en todos y cada uno de los sistemas implantados, razón por la cual cuenta con una plataforma de monitoreo encargada de detectar anomalías a nivel de seguridad que presenten los sistemas y redes de C ANTV

Actualmente la plataforma de Monitoreo de Seguridad Tecnológica presenta una oportunidad de mejora en lo que respecta a la medición de su rendimiento, por lo que se plantea el desarrollo de una propuesta enmarcada en una investigación que consiste en recopilar información sobre cómo se está llevando a cabo la detección de las fallas actualmente en dicha plataforma, para así proponer un plan que permita automatizar la detección de fallas aumentando así la efectividad en la medición del rendimiento de la plataforma de Monitoreo de Seguridad Tecnológica de la CANTV.

El Capítulo I **"El Problema"** está compuesto por la delimitación y contextualización del problema, las interrogantes de la Investigación, los objetivos (General y específicos) y la Justificación de la Investigación.

El Capítulo II **"Marco Teórico"** detalla las bases que sustentan la investigación y está compuesto por los Antecedentes de la Investigación y las Bases Teóricas.

El Capítulo III **"Marco Metodológico"** explica la metodología a aplicar y está compuesto por el Tipo y Diseño de la Investigación, Población y Muestra y las Técnicas e Instrumentos de Recolección de Datos.

El Capítulo IV **"Marco Organizacional"** está compuesto por todos y cada uno de los aspectos organizacionales de la Compañía Anónima Teléfonos de Venezuela (CANTV), entre los que se encuentran la Misión, la Visión, Principios y Valores

Corporativos, así como los aspectos organizacionales de la Gerencia General de Seguridad Integral de CANTV.

El Capítulo v **"Desarrollo"** está compuesto por la respuesta y desarrollo de cada uno de los objetivos específicos del presente proyecto.

El capítulo VI, **"Análisis de los Resultados",** viene representado por el análisis de los resultados obtenidos en el desarrollo del Trabajo Especial de Grado.

El capítulo VII **"Lecciones Aprendidas",** viene dado por todas aquellas enseñanzas que se obtuvieron con la realización del Trabajo Especial de Grado.

El Capítulo VIII **"Conclusiones y Recomendaciones"** está compuesto por las conclusiones y recomendaciones más relevantes a las que se llegó con la realización del presente proyecto.

Por último, se presentan las **Referencias Bibliográficas** en las que se plasman todas y cada y una de las teorías y estándares involucrados en la ejecución de éste proyecto.

CAPÍTULO I. EL PROBLEMA

1.1 Delimitación y contextualización del problema

Dentro del campo de las ciencias administrativas y de gestión se inserta la gerencia de proyectos que incluye las áreas de planificación, control, dirección y organización, pero también las áreas intermedias de operaciones, finanzas, producción, recursos humanos, infraestructura, mercadeo, ventas proyectos, calidad, riesgo, conocimiento, información, activos y cambio.

Las áreas intermedias, por estar muy relacionadas entre sí, se agrupan en conjuntos de procesos gerenciales, con la finalidad de darle mayor fluidez a la incorporación de los conceptos asociados, así se tiene desempeño (calidad y riesgo), Tecnologías de Información comunicaciones TIC (Información, conocimiento, comunicaciones), elementos financieros (Finanzas, activos y auditoría), Ingeniería Industrial (Operaciones, producción, proyectos), mercadeo y ventas (mercadeo, ventas), transformación (tecnología, recursos humanos, competencias, cambio).

En el caso de la gerencia del riesgo y la gerencia de calidad se agrupan dentro de la gerencia del desempeño y responde a la lógica según la cual todo lo que se haga pase a mejorar la calidad, disminuyendo los riesgos y todo lo que se haga para prevenir y protegerse de los riesgos, aumentando la calidad del servicio prestado.

En el referido contexto, el presente Proyecto de Investigación aborda la problemática de seguridad tecnológica de la Compañía Anónima Nacional Teléfonos de Venezuela, CANTV.

La coordinación de monitoreo de seguridad tecnológica de CANTV es la encargada de garantizar la confidencialidad, integridad y disponibilidad de la Red corporativa de TI de CANTV, según los lineamientos y las políticas de seguridad de información establecidas por la gerencia de seguridad tecnológica, razón por la cual cuenta con una plataforma encargada de detectar y alertar cualquier actividad anormal en la red de

acuerdo a patrones (firmas de seguridad), para su posterior análisis y/o escalamiento a las áreas encargadas.

En la actualidad, las fallas presentadas en la plataforma de monitoreo de seguridad tecnológica son solventadas sólo cuando algún operador las detecta y en muchas ocasiones son detectadas luego de un largo período de haber sucedido, ya que las herramientas con las que se cuenta actualmente no permiten la detección automática de fallas en la plataforma, por lo que es de vital importancia contar un sistema que detecte de forma inmediata todas y cada una de las fallas que puedan presentarse, para así aumentar su nivel de disponibilidad.

Por otra parte cabe destacar que la disponibilidad de dicha plataforma es imprescindible, ya que la no presencia de algún servidor de la misma, implicaría una total o parcial desprotección del segmento de red afectado, por carecer de un sistema que permita la visualización y registro de la totalidad de eventos maliciosos, por tal razón se propone el diseño de un sistema que permita visualizar de manera automática y de acuerdo a diversos niveles de criticidad las fallas que pudieran presentarse dentro de la plataforma, con lo cual se lograrían disminuir los tiempos de respuesta en la atención de fallas y aumento de la disponibilidad.

Por las razones antes expuestas se plantean aplicar las herramientas del PMI a fin de evaluar los diversos procesos que medirán la criticidad de los eventos detectados en la plataforma de Monitoreo de Seguridad Tecnológica, con miras al diseño de un plan para la medición del rendimiento en la plataforma de monitoreo de seguridad tecnológica de CANTV.

1.2 Interrogantes de la investigación.

- ¿Cuál es el nivel de disponibilidad en el funcionamiento de la plataforma de monitoreo de seguridad tecnológica?

- ¿Cuáles son los elementos que se requieren para la gestión de la calidad y los riesgos en la plataforma de monitoreo de seguridad tecnológica?

- ¿Cómo diseñar un plan para la medición del rendimiento en la plataforma de monitoreo de seguridad tecnológica?

1.3 Objetivos.

1.3.1 General.

Proponer el Plan para la medición del rendimiento en la plataforma de monitoreo de seguridad tecnológica de CANTV.

1.3.2 Específicos.

- Analizar el estado del arte en la medición del rendimiento de plataformas de seguridad tecnológica.

- Evaluar el nivel de disponibilidad actual de la plataforma de monitoreo de seguridad tecnológica de CANTV.

- Proponer una aplicación informática que permita detectar y alertar las fallas dentro de la plataforma de monitoreo de seguridad tecnológica de CANTV.

- Diseñar el plan para la medición de la disponibilidad de los equipos y servicios de la plataforma de monitoreo de seguridad tecnológica.

1.4 Justificación.

La presente investigación es de vital importancia para la organización, ya que permitirá dar a conocer una metodología idónea para la solución a la problemática planteada anteriormente, a través de una investigación aplicada de tipo de investigación y desarrollo, contenida en el ámbito de la gestión de la calidad y los riesgos, a través de la aplicación de las herramientas dictadas por el PMI para sugestión, lo cual ayudará a determinar y clasificar la criticidad de las fallas ocurridas

dentro de la plataforma de monitoreo de seguridad tecnológica de CANTV, para mantener de esta forma una mayor disponibilidad dentro de dicha plataforma, gracias a la disminución de los tiempos de respuesta en la atención de las fallas presentadas en cualquiera de los elementos de la plataforma.

Por otra parte es importante destacar que el sistema a proponer servirá para aumentar la productividad de la empresa, debido a que ayudará a garantizar la confidencialidad, disponibilidad e integridad de la información en la red corporativa de TI de CANTV, esto debido a que servirá para ayudar a mantener la disponibilidad en la plataforma de Monitoreo de seguridad tecnológica de CANTV, lo cual se traduce en la detección, contención escalamiento inmediato y oportuno de todas y cada una de las amenazas, vulnerabilidades, virus, malwares y ataques de los que puedan ser víctima cada uno de los elementos de la red corporativa de CANTV y sus filiales.

CAPÍTULO II. MARCO TEÓRICO

2.1 Antecedentes

Giralt et al (2011), realizaron una investigación titulada “Seguridad de los documentos de archivo: estudio de caso del Archivo del Ayuntamiento de Barcelona”.

El resumen inicial del artículo señala que el crecimiento exponencial de los contenidos digitales en las organizaciones y la obligación de asegurar la preservación de la documentación hace más evidente la necesidad de disponer de mecanismos que garanticen la autenticidad, integridad y seguridad de la misma. Se presenta el caso del Archivo del Ayuntamiento de Barcelona que, a partir de la experiencia pionera del Archivo del Ayuntamiento de Ámsterdam, está implementando el sistema Hitachi Content Plataform (HCP) de Hitachi Data Sytems como repositorio de los documentos digitales. El proyecto comprende también una revisión de las pautas de trabajo actuales con el fin de establecer procedimientos y buenas prácticas de digitalización.

Al momento de realización del artículo los autores llegaron a las siguientes lecciones aprendidas:

- La parte de análisis, con un trabajo de campo en los distintos centros y previa a la implementación tecnológica, ha contribuido a tener unas líneas de actuación corporativas claras.
- El trabajo en equipo: archiveros, informáticos, gestores, etc., ha sido un aspecto clave en el avance del proyecto.
- Obviamente, hay que dimensionar el crecimiento de información para planificar el volumen de los sistemas de almacenamiento.
- Las pautas de trabajo consensuadas garantizarán la calidad de los proyectos de digitalización.

La investigación realizada por dicho autor contribuye de gran manera para la realización del proyecto, ya que gracias a ésta se puede obtener un estándar para la seguridad de los datos que se transmiten dentro de la plataforma de monitoreo de seguridad, ayudando así a obtener con mayor facilidad los parámetros incluidos en la medición del rendimiento de dicha plataforma.

Sneha (2011), presentó un artículo titulado “Un estudio literario sobre los aspectos de seguridad de los almacenes de datos”.

El objetivo de este artículo es dar una visión general de los aspectos relevantes de seguridad de los almacenes de datos, ya que se han convertido en un fenómeno esencial en el mundo de las empresas, debido a que contienen data importante y sensitiva para las mismas. Con el fin de utilizar sus datos, se debe tener la debida autorización. Los permisos de acceso en los almacenes de datos son manejados actualmente separados de las políticas de origen de la empresa. La protección de la privacidad de los datos y la confidencialidad en el que subyace el almacén están garantizadas a través de una seguridad fiable. También se proponen diferentes políticas de seguridad para garantizar la seguridad de la data.

Las conclusiones más resaltantes a las que se llegó con la investigación fueron las siguientes:

- Los almacenes de datos, data marts y otras grandes sistemas de bases de datos se han vuelto sistemas críticos dentro de las organizaciones.
- El almacenamiento de datos se ha convertido en un fenómeno en el mundo de las empresas.
- En este trabajo, se demostró cómo se mantiene la seguridad por la aplicación de diferentes políticas de seguridad.
- En los almacenes de datos, a través de transacciones SQL se puede proporcionar seguridad a los almacenes de datos.

- Sostenemos que "los datos derivados de los permisos de acceso” ofrecen importantes beneficios para la administración de bases de datos distribuidas.

- En este trabajo se presentó también el papel de los metadatos en la seguridad de almacenamiento de datos.

En la investigación anterior se lograron evidenciar los diversos aspectos en el control de acceso lógico de datos, es decir se lograron dar a conocer las diversas restricciones que deben poseer los servidores encargados de almacenar los datos sensitivos en las organizaciones, por tal razón sirvió como base para lograr maximizar el acceso a los servidores que almacenan los datos soportados en la propuesta del plan para la medición del rendimiento en la plataforma de monitoreo de seguridad.

Khodadadi et al (2006), presentaron un artículo titulado “Optimización y la gestión cuantitativa de inversiones”, el cual ofrece una breve reseña de algunas de las cuestiones clave en la construcción de una exitosa cartera de la equidad cuantitativa construcción de la plataforma, la integración de un almacén de datos, un motor de un nuevo equilibrio, un motor de back-testing, así como una metodología de reparto. Modelos de optimización y el software son elementos centrales de dicha plataforma. Ellos sirven como herramientas sofisticadas para la transferencia de las ideas de rentabilidad en exceso generados mediante la investigación y las pruebas en las carteras que mejor representan estas ideas.

Las conclusiones a las que se llegó fueron las siguientes: Un portafolio robusto y eficiente plataforma de integración de la construcción de una base de datos almacén, un motor de reequilibrio, un back-testing del motor y la atribución una metodología es esencial para la gran escala gestión de inversiones cuantitativas a gran escala. Los modelos de optimización y de software son elementos centrales de una plataforma y, por lo tanto, las herramientas vitales para la gestión cuantitativa de inversiones en su búsqueda de transferencia de las ideas de rentabilidad en exceso generados mediante la investigación y de prueba en las carteras que mejor representan estas ideas. El progreso continuo en la optimización de algoritmos y software está ampliando las

herramientas disponibles para los gestores de cartera. Además, robusto modelo de optimización son prometedores en la reducción del impacto de la estimación y errores en los modelos de carteras óptimas. Con estos y otros acontecimientos recientes, el uso generalizado de la optimización en la gestión de las inversiones puede ser de uso continuo en el futuro.

En la investigación citada anteriormente se lograron dar a conocer los diversos métodos existentes en la optimización de las plataformas, lo cual sirvió como un modelo para lograr estimar los modelos de rendimiento óptimos en la plataforma de monitoreo de seguridad tecnológica, para así obtener los parámetros adecuados en la medición de dicho rendimiento.

Burtescu (2009), presentó un artículo titulado “Implementación de seguridad en almacenes de datos”, en el cual se plantea que los almacenes de datos inicialmente fueron llevados a cabo y desarrollados por las grandes. Más tarde, debido a las tendencias económicas y de la tecnológica el progreso, los almacenes de datos también fueron implantados por las empresas medianas y pequeñas. La creación de un almacén de datos es una operación difícil y laboriosa y su seguridad es aún más difícil de lograr. Las exageraciones sobre la seguridad y sus medidas no siempre son buenas para los negocios. La literatura contiene guías y un montón de consejos en materia de seguridad de almacenamiento de datos. Un importante apoyo puede ser ofrecido por las empresas especializadas que forman parte del mercado actual.

Las conclusiones a las que se llegó con este artículo fueron las siguientes:

Los almacenes de datos son sistemas creados con el fin de ofrecer un acceso inmediato a los datos importantes y confiables que son utilizados para el análisis de decisiones, planificación y evaluación. Un almacén de datos puede facilitar mucho el trabajo pero a al mismo tiempo, puede hacer que sea más difícil. Una infravaloración de las amenazas puede llevar a un nivel bajo de protección de los datos del almacén y de negocios, por lo que aumentan las posibilidades de acceso de los intrusos. Una sobreestimación de la amenazas, a veces alcanzando valores paranoides, conduce a

un nivel de sobreprotección que garantiza una seguridad excesiva, pero será tan perjudicial como el nivel bajo de protección. En este caso, los medios de seguridad pueden ser molestos e inoperantes para la producción de la compañía. Sería ideal descubrir una manera óptima para asegurar un almacén de datos. En muchos casos, debido a la falta de fondos, las empresas pueden adoptar un nivel mínimo de medidas que no será suficiente para lograr lo que supone dicho propósito.

La investigación anterior logró dar a conocer los diversos aspectos de seguridad en los almacenes de datos, los cuales serán empleados al momento de lograr optimizar la seguridad de los datos en la plataforma de monitoreo de seguridad tecnológica de la CANTV, que es uno de los parámetros más importantes para el desempeño óptimo de los servidores que contemplan dicha plataforma.

Parra (2012), en su trabajo especial de grado titulado como el Diseño de una metodología para la gestión del proceso de la demanda estratégica de tecnología de información (IT), caso de estudio: Gerencia Corporativa de IT del Grupo Mistral.

La presente investigación se enfoca en el análisis de la gestión del proceso de la demanda estratégica que se efectúa actualmente en la Gerencia Corporativa de IT, tomando como referencia buenas prácticas ampliamente aceptadas; esto, se toma como base para definir una metodología que determine los pasos a seguir para llevar a cabo eficientemente este proceso y mejorar los aspectos que se consideren necesarios según las fortalezas y debilidades planteadas. En esta investigación consistió en la definición de una metodología que permitiese dar apoyo a la gestión de la demanda estratégica de IT como proceso que permite canalizar, seleccionar y ejecutar proyectos los cuales promueven la consecución de logros que se traducen en beneficios organizacionales. Como resultado de los análisis, se hizo notorio que el Grupo Mistral presenta fortalezas en algunos procesos que forman parte de la gestión de la demanda estratégica, presentando debilidad, principalmente, en la gestión del portafolio de proyectos. Finalmente, realizó un estudio que determinó la factibilidad de la adopción

de la metodología, estando esto supeditado a la disponibilidad del personal de acuerdo a su carga laboral. El estudio estuvo apoyado en la experticia de profesionales que evaluaron la adecuación de la metodología y orientación a buenas prácticas.

Monrroy (2011), en su trabajo especial de grado para optar al título de especialista en Gerencia de proyecto, titulado como Diseño del plan de ejecución del proyecto de actualización de la plataforma tecnológica centralizada de Banesco Banco Universal.

En esta investigación se presenta los escenarios de actualización propuestos para la Plataforma Centralizada de Banesco incluyendo las necesidades actuales y considerando los componentes tecnológicos más modernos del mercado. Así como también, la generación del Roadmap Tecnológico de Actualización que representa el tiempo de ejecución de cada uno de los cambios asociados al proceso de migración; incluyendo la representación de las necesidades de procura tanto para la adquisición de los nuevos equipos tecnológicos como para la fase de adiestramiento en la administración de los mismos; a fin de llegar a la implantación del escenario de actualización visionado.

Como producto de esta investigación se obtuvieron los insumos necesarios para cubrir la fase de Implantación y Operación; donde se pondrá en marcha la solución de acuerdo al diseño generado contemplando el seguimiento y la operacionalización correspondiente. a través del presente Trabajo Especial de Grado; logró consolidar todos los requerimientos de las diversas áreas con la finalidad de definir un escenario de actualización que evolucionara tecnológicamente; brindado la base necesaria para proveer las necesidades demandadas. Además se presenta un plan de ejecución integral para la actualización de la Plataforma Tecnológica Centralizada; incluyendo los componentes asociados a cada una de las capas: Procesamiento, Almacenamiento, R&R y Replicación.

- **Antecedentes empresariales:**

Hasta el año 2008 el monitoreo de seguridad tecnológica era llevado a cabo por una empresa externa, mediante la aplicación **Open Source Security Information Management** (OSSIM), cuyo objetivo primordial era la administración de eventos de seguridad tecnológica, a través de un motor de correlación y una colección detallada de herramientas open source las cuales servían al administrador para tener una vista de todos los aspectos relativos a la seguridad dentro de la red corporativa de CANTV.

Los elementos de software por lo que OSSIM está compuesto son los siguientes:

• Arpwatch, utilizado para detección de anomalías en direcciones MAC.

• P0f, utilizado para la identificación pasiva de OS.

• Pads, utilizado para detectar anomalías en servicios.

• Openvas , utilizado para la evaluación y correlación cruzada (Sistema de detección de intrusos vs Escaner de Vulnerablidad)

• Snort , utilizado como sistema de detección de intrusos (IDS) como también para la correlación cruzada con Nessus.

• Spade, es un motor de detección de anomalías en paquetes. Utilizado para obtener conocimiento de ataques sin firma.

• Tcptrack, utilizado para conocer la información de las sesiones, lo cual puede conceder información útil relativa a los ataques.

• Ntop , el mismo construye una impresionante base de datos con la información de la red, para la detección de anomalías en el comportamiento.

• nfSen, visor de flujos de red para la detección de anomalías de red

• Osiris, es un sistema de detección de intrusos basado en host (HIDS).

• Snare, colecciona los logs de sistemas Windows.

• OSSEC , es un sistema de detección de intrusos basado en hosts

Por otra parte la herramienta empleada para la medición del rendimiento de la plataforma de monitoreo de seguridad tecnológica era Netflow, utilizada para verificar la disponibilidad de los hosts y lo servicios de dicha plataforma, se caracteriza por ser un sistema es un sistema de monitoreo dirigido a los equipos (hardware) y servicios (software) que se especifiquen, alertando cuando el comportamiento de los mismos no sea el deseado. Entre sus características principales figuran la inclusión de servicios de red (SMTP, POP3, HTTP, SNMP...), de los recursos de sistemas hardware (carga del procesador, uso de los discos, memoria, estado de los puertos...), dicha herramienta proporciona permite consultar prácticamente cualquier parámetro de interés de un sistema, y genera alertas, que pueden ser recibidas por los responsables correspondientes mediante (entre otros medios) correo electrónico y mensajes SMS, cuando estos parámetros exceden de los márgenes definidos por el administrador de red.

A partir de Marzo del año 2008 OSSIM fue sacada de producción y migrada a otra herramienta, debido a que el monitoreo de seguridad pasó a formar parte de la empresa, pero aún no se cuenta con un sistema de medición del rendimiento que sustituya al antiguo Netflow.

2.2 Bases Teóricas.

En esta investigación se abarca los tópicos referentes al desarrollo del plan para la gerencia del proyecto en el que se tomarán en cuenta las siguientes áreas de conocimiento involucradas en la Gerencia de Proyectos: Alcance, Tiempo, Costo, Calidad, y Riesgos, de igual forma se hará referencia la planificación pre-proyecto mediante la metodología FEL, con respecto al plan para la Gerencia de Proyectos el PMI en la Guía del PMBOK (2008), señala lo siguiente:

> Desarrollar el Plan para la Dirección del Proyecto es el proceso que consiste en documentar las acciones necesarias para definir, preparar, integrar y coordinar todos los planes subsidiarios. El plan para la dirección del proyecto se convierte en la fuente primaria de información para determinar la manera en que se planificará, ejecutará, supervisará y controlará, y cerrará el proyecto. (PMI, 2008, p 50)

- **Áreas del conocimiento en la Gerencia de Proyectos**

Las distintas áreas del conocimiento en la gerencia del proyecto son las siguientes: Administración del Alcance, Tiempo, Costo, Calidad, Recursos Humanos, Comunicaciones, Riesgos, Procura e Integración, las que se emplearán en el proyecto de investigación son las siguientes:

- *Gestión del Alcance:*

El alcance es definido por Guido (1999) de la siguiente manera:

> El alcance de un proyecto conocido también como el alcance del proyecto o el alcance del trabajo, es todo el trabajo que se tiene que realizar con el fin de que el cliente quede satisfecho de que las entregas (el producto o los artículos tangibles a proporcionarle), cumplan con los requisitos o los criterios de aceptación acordados al inicio del proyecto. Por ejemplo, el alcance del proyecto pudiera ser todo el trabajo incluido en limpiar el terreno, construir una casa y preparar los jardines de acuerdo a las especificaciones acordadas entre el contratista y el comprador. (Gido, 1999) p 6)

Es decir, el alcance de los proyectos es todo aquel trabajo que debe ser realizado, mediante el cumplimiento de las especificaciones técnicas a cumplir (necesidades del cliente).

Con respecto a la gestión del alcance en proyectos el PMI señala lo siguiente: “La Gestión del Alcance del Proyecto incluye los procesos necesarios para garantizar que el proyecto incluya todo (y únicamente todo) el trabajo requerido para completarlo con éxito”. (PMI, 2008, p 95) Es decir que el objeto principal de la gestión del alcance en los proyectos es verificar lo que debería y no debería estar incluido dentro del proyecto.

- *Gestión del Tiempo*

Con respecto a la gestión del tiempo el PMI señala: “La Gestión del Tiempo del Proyecto incluye los procesos requeridos para administrar la finalización del proyecto a tiempo”.(PMI, 2008, p 116). Como cada proyecto tiene una fecha de inicio y una fecha de finalización, en la gestión del alcance se deben aplicar una serie de procesos para lograr que dicha finalización se haga a tiempo, los procesos son los siguientes:

Definir las Actividades: Es el proceso que consiste en identificar las acciones específicas a ser realizadas para elaborar los entregables del proyecto.

Secuenciar las Actividades: Es el proceso que consiste en identificar y documentar las interrelaciones entre las actividades del proyecto.

Estimar los Recursos de las Actividades: Es el proceso que consiste en estimar el tipo y las cantidades de materiales, personas, equipos o suministros requeridos para ejecutar cada actividad.

Estimar la Duración de las Actividades: Es el proceso que consiste en establecer aproximadamente la cantidad de períodos de trabajo necesarios para finalizar cada actividad con los recursos estimados.

Desarrollar el Cronograma: Es el proceso que consiste en analizar la secuencia de las actividades, su duración, los requisitos de recursos y las restricciones del cronograma para crear el cronograma del proyecto.

Controlar el Cronograma: Es el proceso por el que se da seguimiento al estado del proyecto para actualizar el avance del mismo y gestionar cambios a la línea base del cronograma.

- *Gestión de los costos*

El PMI, señala: “La Gestión de los Costos del Proyecto incluye los procesos involucrados en estimar, presupuestar y controlar los costos de modo que se complete el proyecto dentro del presupuesto aprobado”. PMI, 2008, p 145). Los procesos involucrados en la gestión de los costos son los siguientes:

Estimar los Costos: Es el proceso que consiste en desarrollar una aproximación de los recursos financieros necesarios para completar las actividades del proyecto.

Determinar el Presupuesto: Es el proceso que consiste en sumar los costos estimados de actividades individuales o paquetes de trabajo para establecer una línea base de costo autorizada.

Controlar los Costos: Es el proceso que consiste en monitorear la situación del proyecto para actualizar el presupuesto del mismo y gestionar cambios a la línea base de costo.

- *Balance Alcance-Tiempo-Costo.*

Debe existir un balance coordinado entre el alcance, el tiempo y el costo en Gerencia de proyectos, al respecto Chamoun (2002) cita lo siguiente:

> Una de las funciones más importantes del Gerente del Proyecto es lograr y mantener el equilibrio entre el Alcance-Tiempo-Costo. Debemos establecer desde un principio las fronteras de las tres áreas, para monitorearlas muy de cerca en el desarrollo de los trabajos previos al diseño, durante éste y a lo largo de la implementación hasta llegar al cierre del proyecto.(Chamoun, 2002, p 34)

- *Gestión de la Calidad:*

El PMI señala: “La Gestión de la Calidad del Proyecto incluye los procesos y actividades de la organización ejecutante que determinan responsabilidades, objetivos y políticas de calidad a fin de que el proyecto satisfaga las necesidades por la cuales fue emprendido”. (PMI, 2008, p166)

Existen 3 procesos para la gestión de la calidad dictados por el PMI en el PMBOK (2008), entre los cuales se resaltan los siguientes:

Planificar la Calidad: Es el proceso por el cual se identifican los requisitos de calidad y/o normas para el proyecto y el producto, documentando la manera en que el proyecto demostrará el cumplimiento con los mismos.

Realizar el Aseguramiento de Calidad: Es el proceso que consiste en auditar los requisitos de calidad y los resultados de las medidas de control de calidad, para asegurar que se utilicen las normas de calidad apropiadas y las definiciones operacionales.

Realizar el Control de Calidad: Es el proceso por el que se monitorean y registran los resultados de la ejecución de actividades de control de calidad, a fin de evaluar el desempeño y recomendar cambios necesarios.

Dichos procesos interactúan entre sí y de igual forma con los procesos de las otras áreas de conocimiento. Cada proceso puede implicar el esfuerzo de una o más personas o grupos de personas, dependiendo de las necesidades del proyecto. Cada proceso se ejecuta por lo menos una vez en cada proyecto y en una o más fases del proyecto, en caso de que el mismo esté dividido en fases, en la figura 1 se muestra un diagrama con el resumen de los procesos para la gestión de la calidad.

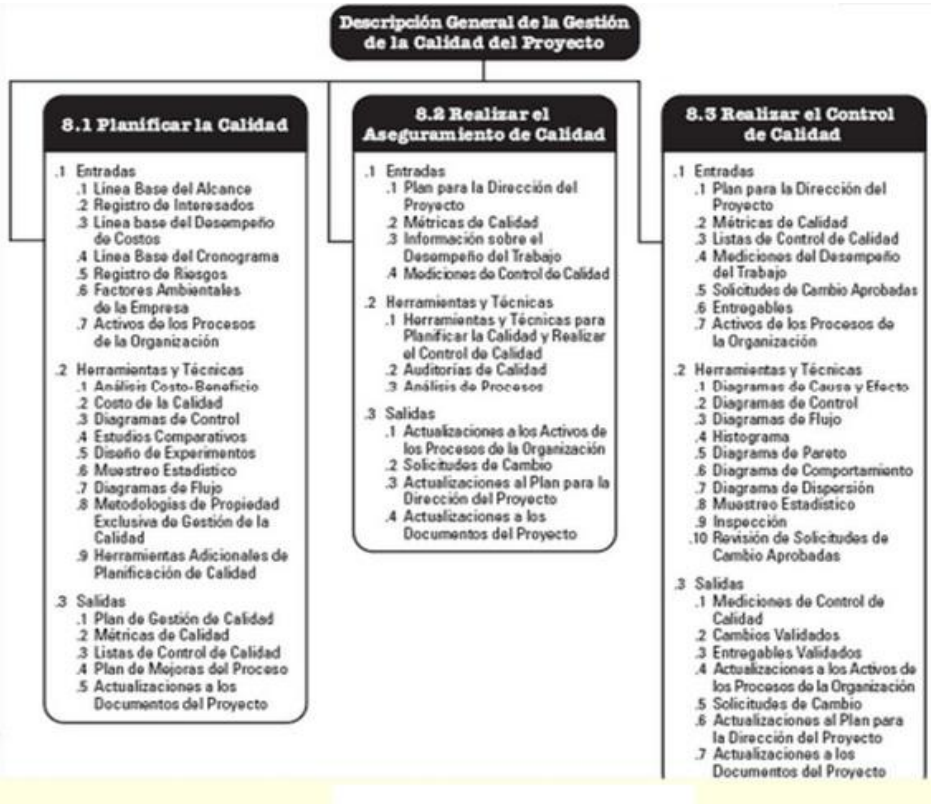


Figura 1. Panorama General de la Gestión de la Calidad.

Fuente: PMI (2008).

- Gestión de los riesgos

En lo que respecta a la gestión de los riesgos, el PMI señala lo siguiente:

> La Gestión de los Riesgos del Proyecto incluye los procesos relacionados con llevar a cabo la planificación de la gestión, la identificación, el análisis, la planificación de respuesta a los riesgos, así como su monitoreo y control en un proyecto. Los objetivos de la Gestión de los Riesgos del Proyecto son aumentar la probabilidad y el impacto de eventos positivos, y disminuir la probabilidad y el impacto de eventos negativos para el proyecto. (PMI, 2008 p234)

Los procesos para la gestión de riesgos dictados por el PMI (2008) son los siguientes:

Planificar la Gestión de Riesgos: Es el proceso por el cual se define cómo realizar las actividades de gestión de los riesgos para un proyecto.

Identificar los Riesgos: Es el proceso por el cual se determinan los riesgos que pueden afectar el proyecto y se documentan sus características.

Realizar el Análisis Cualitativo de Riesgos: Es el proceso que consiste en priorizar los riesgos para realizar otros análisis o acciones posteriores, evaluando y combinando la probabilidad de ocurrencia y el impacto de dichos riesgos.

Realizar el Análisis Cuantitativo de Riesgos: Es el proceso que consiste en analizar numéricamente el efecto de los riesgos identificados sobre los objetivos generales del proyecto.

Planificar la Respuesta a los Riesgos: Es el proceso por el cual se desarrollan opciones y acciones para mejorar las oportunidades y reducir las amenazas a los objetivos del proyecto.

Monitorear y Controlar los Riesgos: Es el proceso por el cual se implementan planes de respuesta a los riesgos, se rastrean los riesgos identificados, se monitorean los riesgos residuales, se identifican nuevos riesgos y se evalúa la efectividad del proceso contra riesgos a través del proyecto.

La figura 2 muestra un diagrama en el cual se destacan los procesos para la gestión de riesgos y su interrelación.

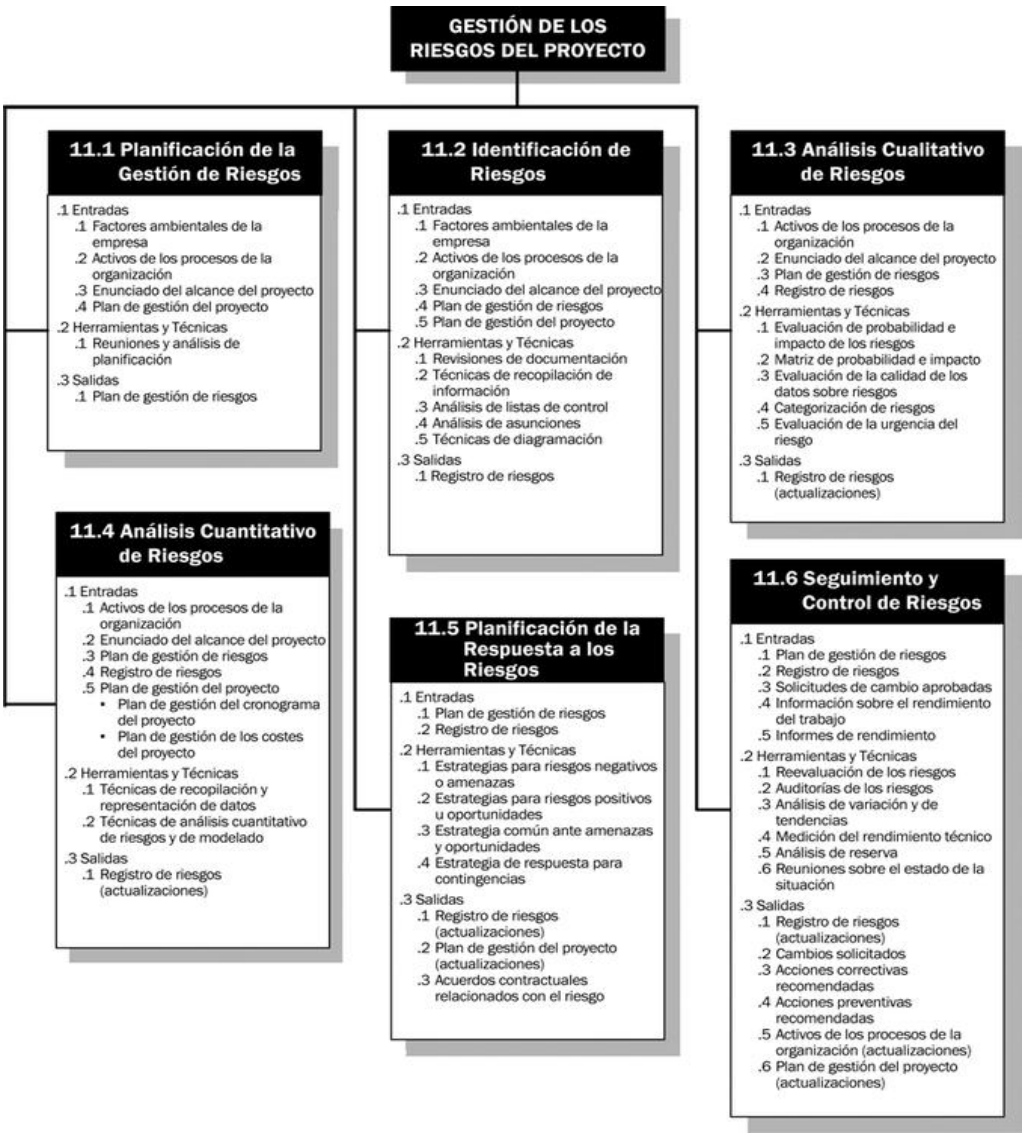


Figura 2. Panorama General de la Gestión de Riesgos.

Fuente: PMI (2008).

- **Front End Loading (FEL):**

De acuerdo al IAAP (2007)[1] en su artículo ¿Qué es la metodología FEL?

> La metodología de gestión de proyectos FEL (front end loading) es una metodología basada en el concepto de portones de aprobación, donde en cada portón se aprueba, o no, el pasaje a la siguiente etapa. Esta metodología ayuda ahorrar costos y mantener al proyecto en fecha, ya que cada fase, antes de ser iniciada, debe estar correctamente planificada y aprobada.

El Instituto de Construcción e Industria presenta ésta metodología en tres fases que son visualizar, conceptualizar y definir, en la figuras 1 y 2 muestran una analogía entre el ciclo de vida del proyecto y la metodología FEL propuesta por el instituto de Construcción e Industria (CII).

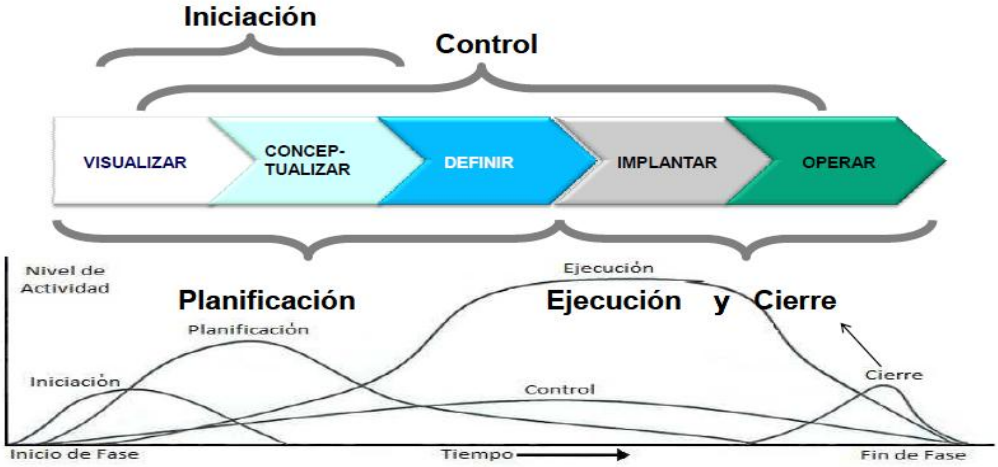


Figura 3. Ciclo de Vida del Proyecto

Fuente: CII (2008)

1 http://iaap.wordpress.com/2007/06/26/%C2%BFque-es-la-metodologia-fel/

Figura 4. Fases de la Metodología FEL
Fuente: CII (2008).

- Visualizar: Es la etapa sobre la cual se generan un conjunto de ideas y se plantea un escenario a futuro de ¿Qué quiero? ¿Cómo será? ¿Qué tendrá? ¿Cómo lo haré? ¿Qué hay a mi alcance? ¿Quién soy y que deseo?

- Conceptualizar: Es la siguiente etapa del ciclo de desarrollo de un proyecto, luego de la visualización debemos ser más específicos, aclarar las ideas y convertirlas en objetivos claros. Este proceso nos permite descartar y sugerir nuevos esquemas, planteamientos y actividades que permitirán la continuidad de desarrollo del objetivo inicial y fundamental considerado en la visualización.

- Definir: La fase de definición representa el análisis detallado de nuestros objetivos anteriores para la puesta en marcha o implementación del proyecto, en ella nos dedicamos a profundizar y analizar las situaciones más sencillas y complejas de acción, que nos permitirán definir el plan de ejecución para el desarrollo de nuestro alcance inicial, sin duda alguna debemos dedicar tiempo a fin de evaluar todas las posibles alternativas que se hagan más corto el camino para la llegada al estado final, en esta etapa en materia económica y presupuestaria entregamos el estimado de costos definitivo y anclado en la

realidad actual, denominado estimado clase II, en el se sabrá exactamente ¿cual el gasto de nuestra inversión?, ¿cuál será la tasa interna de retorno y nuestro valor agregado?, los beneficios que obtendremos a futuro y por supuesto la solución a los por menores con los que tendremos que lidiar.

Por otra parte se presentan las bases que sustentarán la medición del rendimiento en la plataforma de monitoreo de seguridad, entre lo que se puede mencionar los conceptos básicos para el aseguramiento de los sistemas que son la Confidencialidad, Disponibilidad e Integridad, así como también los diversos parámetros utilizados para gestionar los riesgos a nivel de seguridad de información que son: las vulnerabilidades, amenazas y ataques.

- **Confidencialidad, integridad y disponibilidad**:

Al respecto EC-COUNCIL a. (2012), señala lo siguiente:

> La confidencialidad se refiere a la prevención de accesos no autorizados, revelación y uso de la información, y es una parte de un concepto más amplio que se conoce como privacidad. La confidencialidad se mantiene por medio de la autenticación de los usuarios y control de acceso.
>
> La autenticación de usuarios asegura que la persona que está intentando acceder a la data es la autorizada. El control de acceso es el proceso de definir que usuarios y grupos deben tener acceso a los datos. (EC-COUNCIL, 2012, p13)

Por lo tanto la confidencialidad es un proceso que se refiere a la protección de la data del acceso de usuarios no autorizados.

Por otra parte EC-COUNCIL A. (2012), señala:

> La integridad, se refiere a la confiabilidad y fidelidad de la información. La integridad de los datos se refiere a la necesidad conservar o preservar la información (sin alteración ni corrupción) desde la fuente hacia el destino. La integridad de la fuente se refiere al proceso de verificación que está envuelto en asegurar que los datos provienen de la fuente correcta y no de un impostor.
> La disponibilidad de la información es crítica para las compañías que confían de los datos electrónicos y comunicaciones. Como la integridad de la red, la disponibilidad es una función del departamento de tecnologías de la información. (EC-COUNCIL, 2012, p13)

- **Vulnerabilidad, amenazas y ataques:**

Con respecto a estos tópicos EC-COUNCIL B. (2012) señala los siguientes aspectos:

> Una vulnerabilidad es una falla o debilidad en los sistemas. Si es explotada puede resultar en eventos indeseables que comprometerían la seguridad, permitiendo violación de la integridad de los sistemas. las vulnerabilidades más comunes en las redes son las siguientes: contraseñas débiles, bugs en los software, virus y malwares, inyección de códigos.
>
> Una amenaza es un evento, persona o circunstancia que tiene la habilidad de dañar el sistema alterando, borrando o revelando información confidencial.
>
> Un ataque es una acción deliberada que causa daños a los sistemas de computación, mediante la explotación de vulnerabilidades y amenazas conocidas. (EC-COUNCIL, 2012, p14).

Por otra parte en lo que respecta a la calidad en la Gerencia de Proyectos tecnológicos Pressman (2002), señala lo siguiente

> Un atributo de un elemento, la calidad se refiere a las características mensurables cosas que se pueden comparar con estándares conocidos como longitud, color, propiedades eléctricas, maleabilidad, etc. Sin embargo, el software en su gran extensión, como entidad intelectual, es más difícil de caracterizar que los objetos físicos. No obstante, sí existen las medidas de características de un programa. (Pressman, R, 2002, p132).

- **Garantía de calidad**

La garantía de calidad consiste en la auditoría y las funciones de información de la gestión. El objetivo de la garantía de calidad es proporcionar la gestión para informar de los datos necesarios sobre la calidad del producto, por lo que se va adquiriendo una visión más profunda y segura de que la calidad del producto está cumpliendo sus objetivos. Por supuesto, si los datos proporcionados mediante la garantía de calidad identifican problemas, es responsabilidad de la gestión afrontar los problemas y aplicar los recursos necesarios para resolver aspectos de calidad.

- **Pruebas de aceptación en fábrica (FAT)**

Las pruebas de aceptación de fábrica o Factory Acceptance Test (FAT) por sus siglas en inglés son diversos protocolos de prueba necesarios para la puesta en producción de aplicaciones informáticas, al respecto Safeprod (2006) señala lo siguiente:

> El objetivo principal de FAT es poner a prueba la seguridad del sistema (evaluando el código y el software de manera conjunta). Las pruebas son normalmente ejecutadas durante la fase final del diseño y fase de ingeniería, antes de la instalación final en planta . Las FAT son un procedimiento personalizado para poner a prueba la seguridad del sistema y funciones, de acuerdo a los requerimientos de seguridad de fábrica (Safeprod, 2006, p6).

La figura 5 muestra el proceso FAT, especificando las etapas en las cuales son realizadas las diversas pruebas.

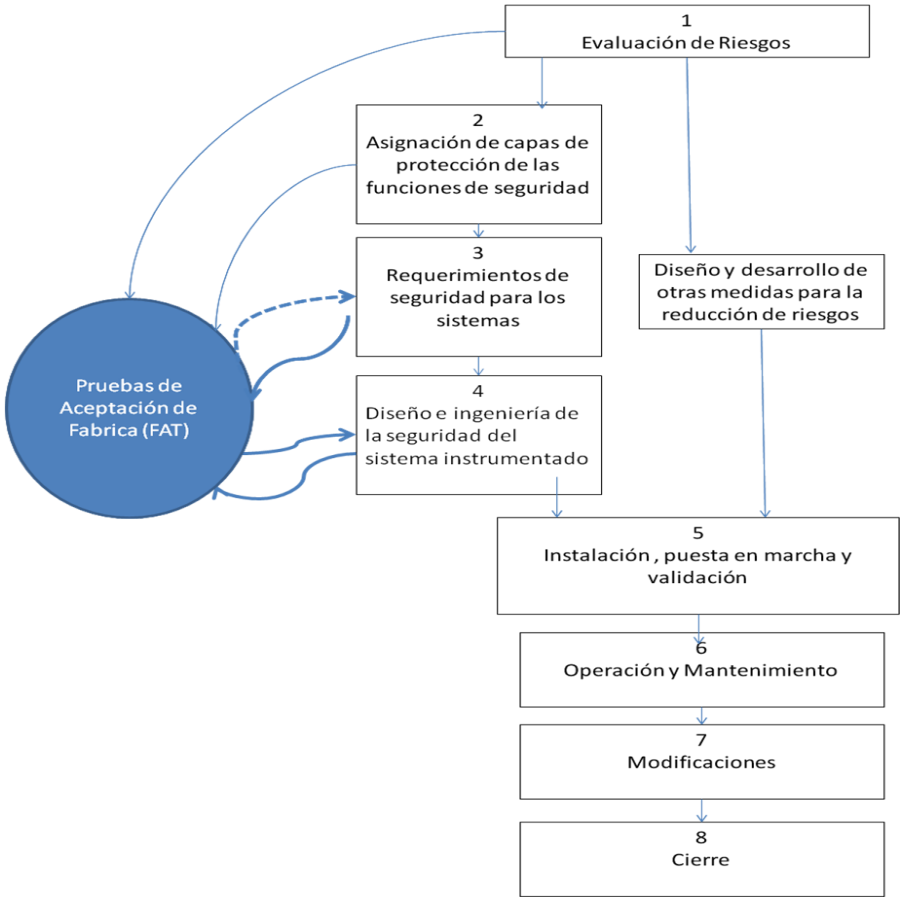


Figura 5. Proceso FAT (Factory Acceptance Test).
Fuente: Adaptado de Safeprod (2006).

En el proceso FAT se revelan las debilidades en la fase de diseño e ingeniería o en la fase de especificaciones y requerimientos de seguridad, dichas fallas o debilidades son tratadas de acuerdo al resultado de las FAT, luego de que sean subsanadas se vuelve a realizar el procedimiento de pruebas, para verificar la operatividad y seguridad del sistema y software.

- **Pruebas de aceptación en Sitio (SAT)**

Las pruebas de aceptación en sitio, Site Acceptance Test (SAT) por sus siglas en ingles se refieren a un conjunto de pruebas realizadas por el cliente a fin de que el sistema a adquirir cumpla con los requerimientos de la empresa. Sobre este tema Viryanet (2013)[2], en su artículo Site Acceptance Testing., señala lo siguiente:

> Es la etapa en la que el cliente lleva a cabo pruebas para los componentes suministrados en virtud del alcance del proyecto y pone a prueba la conformidad de la solución entregada al documento de la definición de soluciones y especificaciones funcionales. La etapa de prueba de aceptación del sitio incluye 3 partes: pruebas de integración, pruebas de rendimiento y pruebas de aceptación del usuario. Esta fase de pruebas también utiliza los planes de pruebas y escenarios creados anteriormente en el ciclo de vida del proyecto por el equipo de atención al cliente.

Por otra parte, es importante destacar que la integración, rendimiento, pruebas de aceptación, plan documentado y datos para representar situaciones reales de negocio son usados durante la fase de diseño.

Análisis del modo y Efectos de Falla (AMEF).

Sobre la metodología AMEF SPC Consulting Group [3]en su artículo AMEF Análisis del Modo y Efecto de Falla, señala lo siguiente

> AMEF o Análisis del Modo y Efectos de Fallas, es una metodología utilizada durante el desarrollo del producto y del proceso, para asegurar que se han considerado los problemas que potencialmente se puede presentar y que pueden afectar la calidad del producto y/o su desempeño. Como tal, surge la necesidad de elaborar los AMEF´s durante el proceso de Planeación Avanzada de la Calidad (APQP), y proporcionar información de entrada para el desarrollo del Plan de Control. Esta herramienta también es conocida por ser parte de las Core Tools del sector automotriz y un requerimiento de la especificación técnica ISO/TS 16949.

2 http://www.viryanet.com/services/implementation/site-acceptance-testing/

3 http://spcgroup.com.mx/amef/

> Hay dos tipos de AMEF: de Diseño y de Proceso. El AMEF es una herramienta para mejorar la confiabilidad del producto, y se puede describir de manera general como un método para identificar la severidad de los efectos potenciales de fallas y para estimar la probabilidad de ocurrencia de las causas de las fallas. Proporciona así una base para implementar medidas que reduzcan los riesgos.

Es importante señalar que es de vital importancia en proyectos en los cuales se requiera realizar una gestión de la calidad de manera eficiente contar con este tipo de herramientas que permiten predecir con gran facilidad cualquier falla que se pueda presentar en los procesos o el diseño, lo cual puede garantizar el éxito o no del producto final.

CAPÍTULO III. MARCO METODOLÓGICO

3.1 Tipo y diseño de la Investigación

De acuerdo al problema que se plantea, el cual hace referencia a la propuesta de un plan para la medición del rendimiento en la plataforma monitoreo de seguridad tecnológica y en función de sus objetivos la investigación a realizar será de tipo documental y de carácter descriptivo.

La investigación es documental debido a que se basará en un proceso de búsqueda y análisis de datos secundarios, es decir aquellos que provienen de otras fuentes documentales, en este caso la empresa CANTV, posee diversos registros históricos con información de la plataforma de Seguridad Tecnológica, según Arias (2004), "La investigación Documental es un proceso basado en la búsqueda, recuperación, análisis, crítica e interpretación de datos secundarios.

Por otra parte, se considera descriptiva, ya que con la investigación se busca mediante el análisis de datos, el entendimiento de todas y cada una de las fallas que inciden en la disponibilidad de la plataforma de monitoreo de seguridad tecnológica para lograr el diseño de un sistema para la medición de su rendimiento, al respecto Arias (2004), señala "La investigación descriptiva consiste en la caracterización de un hecho, fenómeno, individuo o grupo, con el fin de establecer su estructura o comportamiento." Con lo cual se comprueba su carácter descriptivo" (p 24).

Asimismo la investigación está orientado por un diseño de tipo no experimental, debido a que no existe manipulación de variable alguna, ya que las variables presentes se respetan de acuerdo a su entorno natural, con lo cual se adquiere una característica longitudinal, ya que la información es tomada durante períodos de tiempo delimitado. En cuanto a su carácter longitudinal, Balestrini (2002), señala: "permiten la recolección de los datos en un período de tiempo delimitado, tomando en cuenta determinados momentos previamente especificado, a fin de establecer los cambios producidos en

relación a las variables estudiadas, las consecuencias de estos y los factores determinantes de los mismos" (p 133).

3.2 Población y muestra

El universo de estudio en la presente investigación sobre la propuesta de un plan para la medición del rendimiento en la plataforma de Monitoreo de Seguridad Tecnológica son todos aquellos que integran la plataforma de monitoreo de seguridad tecnológica, entre los cuales se encuentran los 13 Sensores que fungen como Sistemas de detección de Intrusos presentes en dicha plataforma, así como los 3 servidores para las aplicaciones de gestión de la coordinación.

3.3Técnicas e Instrumentos de Recolección de Datos.

En función de los objetivos definidos en la investigación, en la cual se propone el diseño de un sistema para la medición del rendimiento de la plataforma de monitoreo de seguridad tecnológica de CANTV se emplearán técnicas de tipo encuesta escrita, empleando instrumentos como lo son las guías de encuesta, que constan de una ficha con una serie de preguntas a los operadores de la plataforma de monitoreo de seguridad tecnológica, de igual forma técnicas de análisis documental empleando como instrumentos las diferentes bases de datos en donde se almacenan los registros históricos de las fallas presentes en la plataforma de monitoreo de seguridad tecnológica de CANTV.

3.4 Fases de la investigación

El desarrollo del presente proyecto será plasmado en 5 fases que se describen a continuación:

- **Fase I. Detección del problema:** Esta fase consistió en la detección y análisis de las situaciones que conllevaron a determinar la problemática existente en la plataforma de monitoreo de seguridad tecnológica de CANTV, en la que están

incluidos la contextualización y delimitación del problema, los objetivos general y específicos, así como también la justificación de la investigación.

- **Fase II. Investigación documental:** Está conformada por todos y cada uno de los procesos que se llevan a cabo para obtener la información inicial con respecto a los aspectos más relevantes de la problemática detectada, allí van incluidas las bases teóricas y antecedentes de la investigación.

- **Fase III. Métodos y técnicas.** Durante esta fase se lograron determinar las diversas metodologías, técnicas y herramientas empleadas para el desarrollo y conclusiones del proyecto

- **Fase IV. Desarrollo.** Se tomarán en cuenta todos los procesos que regirán el la realización del proyecto para dar respuesta a la problemática planteada en la fase I.

- **Fase V. Conclusiones:** Durante esta fase se emitirán una serie de conclusiones y recomendaciones de los resultados obtenidos en la fase IV.

3.5 Estructura Desagregada de Trabajo

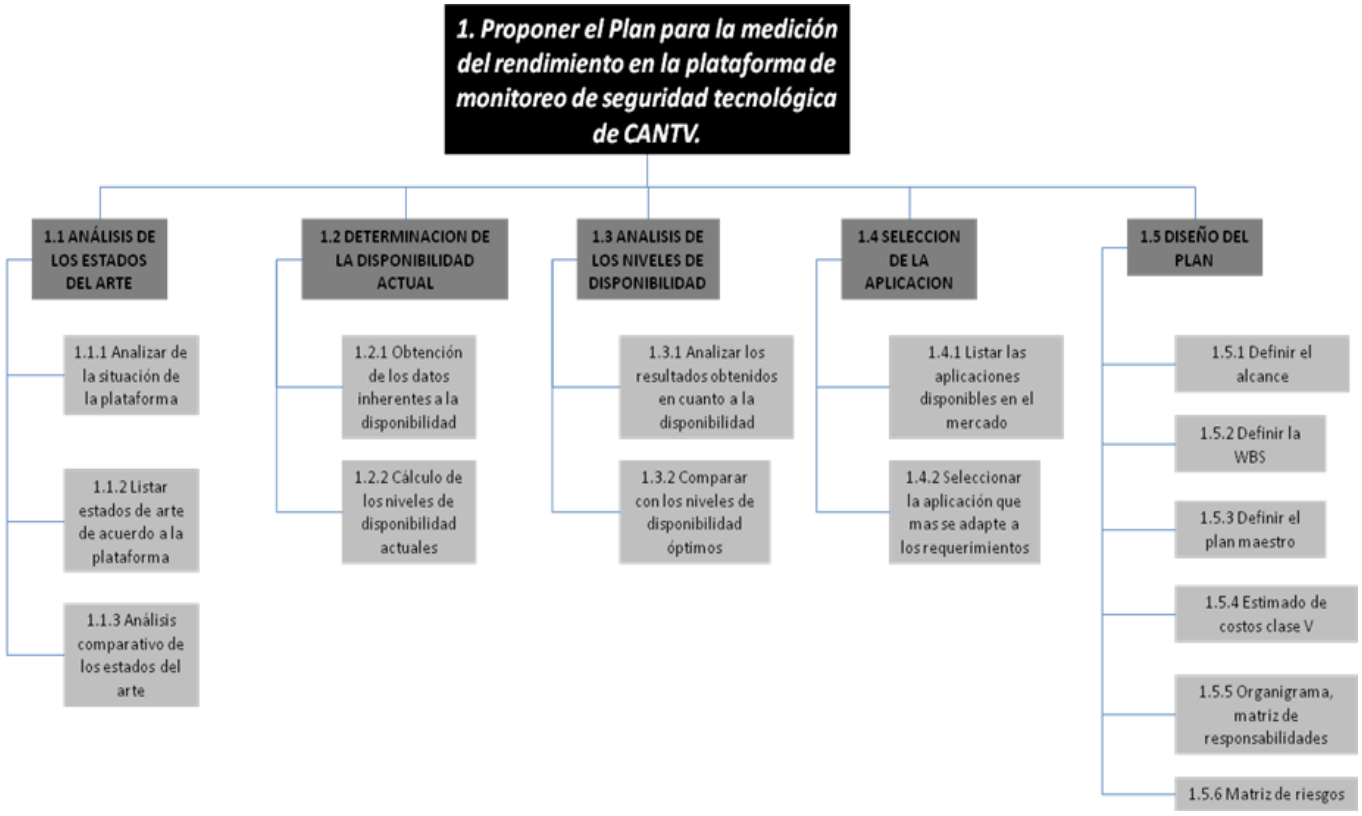


Figura 6. Estructura Desagregada de Trabajo
Fuente: CANTV (2013)

3.6 Operacionalización de las variables

Para Hurtado (2008) “La Operacionalización (sic) es un proceso que le permite al investigador identificar aquellos aspectos perceptibles de un evento que hacen posible dar cuenta de la presencia o intensidad de éste.” (p.131). Mediante este proceso los investigadores definen los indicadores que dan respuestas a las variables y a los objetivos que dan pautas a la presente investigación.

El cuadro 1 muestra las variables involucradas en el desarrollo del presente proyecto.

Cuadro 1. Operacionalización de las variables.

Evento	Sinergia	indicios	Indicador	Instrumento/ herramienta	Fuente
Propuesta de un Plan para la medición del rendimiento en la plataforma de monitoreo de seguridad tecnológica de CANTV.	Análisis del estado del arte en la medición del rendimiento de plataformas de seguridad tecnológica.	Continuidad Operativa Seguridad Integridad Tiempo de respuesta	Eficiencia Eficacia Economicidad productividad	Revisión documental Análisis comparativo	Secundaria CANTV
	Evaluar el nivel de disponibilidad actual de la plataforma de monitoreo de seguridad tecnológica de CANTV.	Continuidad Operativa Seguridad Integridad Tiempo de respuesta	Eficiencia Eficacia Economicidad productividad	Tabla de medición del impacto/efecto Dimensiones de la calidad de los datos	
	Propuesta de una aplicación informática que permita detectar y alertar las fallas dentro de la plataforma de monitoreo de seguridad tecnológica de CANTV.	Continuidad Operativa Seguridad Integridad Tiempo de respuesta	Eficiencia Eficacia Economicidad productividad	Evaluación de tecnología	
	Diseño del plan para la medición de la disponibilidad de los equipos y servicios de la plataforma de monitoreo de seguridad tecnológica.	Definición de Documento de Alcance del Proyecto.	Documento de Requerimientos	Documento de Alcance del Proyecto.	
		Definición de Estructura Desagregada de Trabajo (WBS)	Documento de Requerimientos	Estructura Desagregada de Trabajo (WBS)	
		Definición de Plan Maestro de Ejecución del Proyecto	Tiempo Costo Alcance	Plan Maestro de Ejecución del Proyecto	
		Definición de Estimado de Presupuesto Clase V	Costos	Estimado de Presupuesto Clase V	
		Definición de Organigrama del Proyecto.	Recursos	Organigrama del Proyecto.	
		Definición de Matriz de Roles y Responsabilidades del Proyecto.	RRHH	Matriz de Roles y Responsabilidades del Proyecto.	
		Definición de Matriz de Riesgos	Riesgos	Matriz de Riesgos Plan contingencia	

Fuente: CANTV (2013).

3.7 Consideraciones Éticas.

Se considera como confidencial, toda aquella información que la organización estime de su propiedad y que no sea del conocimiento público.

Por tratarse de un trabajo de investigación y profesional, en el campo de la gerencia de proyectos, se seguirá el código de ética del Project Management Institute (PMI, 2008), el cual especifica lo siguiente:

- Mantenimiento de altos estándares de integridad y de conducta profesional.
- Responsabilidad por cada una de las acciones.
- Práctica continua de la justicia y la honestidad.
- Mejora continua del conocimiento, las capacidades y las habilidades profesionales.
- Respeto y protección de la propiedad intelectual.
- Cumplimiento de las obligaciones éticas y legales pertinentes.

CAPÍTULO IV.MARCO REFERENCIAL

El contexto organizacional en el cual se desarrolla el proyecto está enmarcado por la Compañía Anónima Nacional Teléfonos Venezuela (CANTV), a continuación se presenta una descripción de sus principales atributos.

4.1 Misión

Somos la empresa estratégica del estado venezolano operadora y proveedora de soluciones integrales de telecomunicaciones e informática, corresponsable de la soberanía y transformación de la nación, que potencia el poder popular y la integración de la región, capaz de servir con calidad, eficiencia y eficacia, y con la participación protagónica del pueblo, contribuyendo a la suprema felicidad social

4.2 Visión

Ser una empresa socialista operadora y proveedora de soluciones integrales de telecomunicaciones e informática, reconocida por su capacidad innovadora, habilitadora del desarrollo sustentable y de la integración nacional y regional, comprometida con la democratización del conocimiento, el bienestar colectivo, la eficiencia del estado y la soberanía nacional.

4.3 Principios y Valores Corporativos

- **Eficiencia**

Nos orientamos al cumplimiento oportuno de nuestros objetivos y metas, enfocándonos en la obtención de resultados basados en la rentabilidad social y asegurando la viabilidad económica de la Corporación.

Cumplimos con los compromisos que establecemos y respondemos profesionalmente por nuestras acciones, realizando las actividades con altos niveles de excelencia, calidad y productividad.

Impulsamos la optimización de los procesos, hacemos uso adecuado de los recursos y mejoramos continuamente lo que hacemos y como lo hacemos.

Profundizamos en el conocimiento y el autodesarrollo que nos permita brindar un soporte adecuado a las propuestas que realizamos.

Propiciamos la innovación, la aplicación de nuevas ideas, la generación de servicios y prácticas que contribuyan al cumplimiento de la Misión y Visión.

- **Honestidad**

Nos comportamos con probidad y actuamos de manera congruente entre lo que somos, decimos y hacemos.

Actuamos con transparencia, facilitando el acceso a información veraz y oportuna del ejercicio de nuestra función pública, a todos los relacionados con las actividades que realizamos.

Promovemos el uso responsable, claro y racional de los recursos públicos que disponemos para realizar nuestras funciones.

- **Igualdad**

Promovemos la inclusión de todas y todos, sin distinciones de etnia, edad, orientación sexual, salud, género, credo, condición social o política, jerarquía o cualquier otra que menoscabe la dignidad humana.

Establecemos relaciones basadas en la justicia social con nuestras usuarias, usuarios, trabajadoras, trabajadores, jubiladas, jubilados, comunidades, proveedores y aliados de la Corporación.

Propiciamos la igualdad en el disfrute de los beneficios a nuestras trabajadoras y trabajadores.

Impulsamos el acceso a las telecomunicaciones de todas y todos como un derecho fundamental.

- **Solidaridad:**

Somos parte de la nueva sociedad en construcción y contribuimos activamente con su desarrollo. Nos esforzamos en ayudar a otros y actuamos en función del bienestar colectivo.

Propiciamos el intercambio con las comunidades para conocer sus necesidades, intereses, sentimientos, preocupaciones y contribuir a la mejora de su calidad de vida.

Valoramos nuestra contribución como trabajadoras y trabajadores al desarrollo y transformación de la sociedad.

- **Participación Protagónica:**

Nos comprometemos en el diseño, desarrollo, ejecución, evaluación y control de las iniciativas y actividades de la Corporación, de manera sistemática y sostenida en el tiempo.

Mantenemos una actitud optimista, creativa, positiva y emprendedora, enfocada en la generación de acciones y/o propuestas que demuestren compromiso y contribuyan con la gestión eficiente de la Corporación.

Somos agentes de transformación, influyendo e inspirando a otros y orientándonos a compartir experiencias y aprendizajes con nuestro entorno laboral y con la sociedad.

Creamos y compartimos espacios directos de comunicación e intercambio para fortalecer la participación popular.

Somos corresponsables de la seguridad, defensa y soberanía de la nación, y de la preservación y resguardo de la Corporación.

- **Vocación de Servicio:**

Sentimos satisfacción y pasión por brindar la mejor atención y calidad de servicio, teniendo claro nuestro rol como servidores públicos.

Nos comprometemos a “entender, atender y resolver” las necesidades de aquellos a los que servimos, orientándonos permanentemente a su satisfacción y a superar sus expectativas.

Atendemos con cordialidad, humanidad, rapidez y sentido de oportunidad los planteamientos de nuestras usuarias y usuarios.

Estamos en constante desarrollo, mejoramiento de nuestras capacidades y abiertos al aprendizaje de nuevos conocimientos, con la finalidad de prestar nuestro mejor servicio.

- **Esfuerzo Colectivo:**

Compartimos la Misión, Visión, Principios, Valores, Objetivos y nos sentimos parte de la Corporación y de la Nación.

Practicamos la cooperación y la complementariedad, propiciando el esfuerzo colectivo, como medio fundamental para alcanzar y superar, con pasión, los objetivos y las metas comunes con altos niveles de excelencia.

Valoramos y promovemos el espíritu colectivo, los resultados integrales y el intercambio de saberes, cumpliendo nuestros compromisos y apoyando a otros en el logro de los objetivos y metas comunes.

Nos basamos en el respeto, la confianza y la comunicación de nuestras ideas, siendo autocríticos, escuchando y compartiendo con humildad las recomendaciones, las oportunidades de mejora y los logros.

- **Ética Socialista:**

Somos humanistas, orientamos nuestras acciones basados en el amor y el respeto por los semejantes, la justicia social, el desprendimiento, la solidaridad humana y la importancia de lo colectivo.

Desarrollamos relaciones armónicas con el ambiente, mitigando el impacto de las operaciones en la transformación de nuestro entorno.

Propiciamos el intercambio de saberes con la sociedad, contribuyendo en el proceso de formación y modelaje de conductas, facilitando la transferencia de poder y conocimiento para la toma de decisiones por el pueblo.

Somos tolerantes manejando las diferencias, basados en nuestra capacidad de comprensión y escucha, identificando y valorando todas las opiniones y creencias

Promovemos nuevas relaciones de producción y de propiedad social.

- **Responsabilidad:**

Nos enfocamos en el cumplimiento de nuestros objetivos y actividades alineados con la Orientaciones Estratégicos y Planes Operativos.

Honramos con el cumplimiento nuestros compromisos adquiridos de manera oportuna y con altos estándares de calidad.

Somos responsables en nuestra capacidad de dar respuesta a todas las solicitudes que tengamos de nuestros clientes, compañeros, proveedores.

Asumimos con humildad el impacto de nuestras decisiones y las consecuencias de nuestros actos, aprendiendo de ellas con disposición de mejorar y aplicar correctivos inmediatos.

4.4 Gerencia General de Seguridad Integral de CANTV.

El proyecto de investigación se llevará a cabo en la Gerencia General de Seguridad Integral de CANTV, de dicha gerencia cabe resaltar lo siguiente:

- **Misión**

Somos la Gerencia General dirigida a garantizar la Seguridad Integral de CANTV y sus empresas filiales, a través de la corresponsabilidad y participación protagónica, mitigando los riesgos, aplicando inteligencia estratégica, protegiendo activos, controlando el ciclo de ingresos de la operación, investigando y brindando apoyo a la continuidad operativa y la rentabilidad social, en aras de contribuir con la satisfacción de las necesidades de las comunidades, haciendo nuestro aporte en la transformación del Estado y la preservación de la Soberanía Nacional.

- **Visión**

Ser la Gerencia General de CANTV y sus empresas filiales, reconocida por su capacidad innovadora en Seguridad Integral, privilegiando y habilitando la cultura de prevención y resguardo de los activos, aportando en la eficiencia del Estado y la Soberanía Nacional.

CAPITULO V. DESARROLLO

5.1Introducción

En este capítulo se muestran los resultados y su respectivo análisis sobre la propuesta del plan para la medición del rendimiento en la plataforma de monitoreo de Seguridad tecnológica de CANTV por cada objetivo especifico ejecutado.

Para el análisis de los resultados se emplearon diversas evaluaciones entre las que destacan el juicio de expertos en el área, dichos expertos se destacan a continuación:

Cuadro 2. Expertos del área

Cargo	Experiencia	Certificaciones
Asesor de Seguridad tecnológica CANTV	Manejo de bases de datos, monitoreo de disponibilidad en plataformas de seguridad, administración de plataformas Linux, Windows y solaris, análisis de tráfico.	• CISA: Certified Information System Auditor. • CISM: Certified Information Security Manager. • CEH/CHFI, Certified Ethical Hacker /Computer Hacking Forensic Investigator
Consultor de Seguridad tecnológica CANTV	Manejo de bases de datos, monitoreo de disponibilidad en plataformas de seguridad, administración de plataformas Linux, Windows y solaris, análisis de tráfico.	• CEH/CHFI, Certified Ethical Hacker /Computer Hacking Forensic Investigator. • CISSP: Certified Information Systems Security Professional

5.2 Analizar el estado del arte en la medición del rendimiento de plataformas de seguridad tecnológica.

Una red de datos consta de una serie de elementos computacionales interconectados entre si que tienen por objeto la compartición de recursos, equipos, información y programas que se encuentran localmente (Redes de área local) o dispersos geográficamente (Redes de área amplia). Otro de los objetivos de las redes es brindar la mayor seguridad a los datos que viajan sobre ella aportándole los tres parámetros del triángulo de seguridad: disponibilidad, confidencialidad e integridad

La confidencialidad se refiere a garantizar que la información está accesible únicamente a personal autorizado.

La disponibilidad de un equipo o sistema es una medida que nos indica cuánto tiempo está ese equipo o sistema operativo disponible con respecto a la duración total en el periodo planificado de funcionamiento.

La integridad se refiere a que la información no sea alterada mientras viaja por un sistema de información y garantiza que la información que se transmite sea la misma que se recibe.

- **Evaluación de indicadores:**

La medición del rendimiento en una plataforma se refiere a realizar un monitoreo constante de los parámetros que determinan la disponibilidad de un equipo o sistema. En la actualidad existen ciertos estados del arte basados en una gran gama de herramientas utilizadas para medir el rendimiento en redes y servidores, éstas son empleadas para detectar problemas de configuración y seguridad. Existen varias herramientas que son de amplio uso a nivel mundial, unas que son de carácter comercial propiamente, y otras Open Source o Software libre, que son aprovechables en términos económicos, cabe destacar que para decidir cual herramienta será la más idónea para la medición del rendimiento se evaluaron 4 indicadores que son eficiencia, eficacia, economicidad y productividad, cada indicador representa el 25% del valor total de decisión, es decir que con la suma de los cuatro indicadores se obtiene un total del

100 %, por tal razón el estado que se aproxime al 100% sería el más adecuado para el proyecto, la escala para la medición se enmarcó en el juicio de expertos quienes son ingenieros y técnicos del área de seguridad tecnológica de CANTV con experiencia en redes y en medición de parámetros de rendimiento y seguridad con certificaciones internacionales que avalan la decisión para cada indicador, las escalas para cada indicador se representan de la siguiente forma:

0% = Bajo

15% = Medio

25% = Alto

A continuación se muestra la descripción técnica y evaluación de indicadores para cada herramienta:

- **Proyecto Ntop**

Ntop es una herramienta open source de medición y monitoreo de tráfico en redes, soporta varias actividades de administración, incluyendo optimización y planeamiento, así como la detección de violaciones en las políticas de seguridad de redes.

Empleando la información técnica del fabricante obtenida del sitio web http://www.ntop.org/wp-content/uploads/2011/09/ntop-overview.pdf en donde se evidencia toda la información técnica del producto e información registrada por parte de las Pruebas de Aceptación de Fábrica (FAT por sus siglas en inglés), se obtuvieron las siguientes especificaciones:

Características técnicas

Medición de Tráfico:

- Datos enviados y recibidos: Volumen y paquetes que son clasificados de acuerdo a protocolos IP y de Red

- Historial de sesiones de transmisión de datos (TCP).
- Análisis y medición del ancho de banda.
- Monitoreo de protocolos de voz sobre IP.

Monitoreo de Tráfico:

- Flujos en la Red.
- Utilización de protocolos.
- Matriz de tráfico de Red.
- Protocolos ARP e ICMP.
- Detección de la mayoría de los protocolos P2P más populares.

Indicadores

El cuadro 3 muestra los resultados obtenidos en la evaluación de los indicadores de eficiencia, eficacia, economicidad y productividad a juicio de expertos para el Proyecto NTOP, obteniéndose los siguientes resultados:

Cuadro 3. Indicadores Proyecto NTOP

Eficiencia	Eficacia	Economicidad	Productividad	Total
Altamente eficiente por maximizar los recursos utilizados, lo cual equivale al **25% Eficiente.**	Para la plataforma de Monitoreo de Seguridad de Cantv sería poco eficaz, debido a que no realiza la medición de los procesos a nivel de plataformas, sino a nivel de tráfico de red, resultando un **0% eficiente**	Altamente económica por ser software libre y no generar gastos de licenciamiento. Resultando en un **25% Económico**	Baja. **0% Productiva**	**50%**

2. Nagios

Nagios es un sistema open source de monitoreo de redes encargado de vigilar y controlar los equipos (hardware) y servicios (software) que sean especificados, informando cuando el comportamiento de los mismos no sea el deseado. Entre las características principales están el monitoreo de servicios de red (SMTP, POP3, HTTP, SNMP...), el monitoreo de los recursos de sistemas hardware (carga del procesador, uso de los discos, memoria, estado de los puertos...), independencia de sistemas operativos, posibilidad de monitorización remota mediante túneles SSL cifrados o SSH, y la posibilidad de programar plugins específicos para nuevos sistemas. De acuerdo a lo expresado por el fabricante en la página web http://nagios.sourceforge.net/docs/nagioscore/3/en/toc.html en donde se evidencia toda la información técnica del producto e información registrada por parte de las Pruebas de Aceptación de Fábrica (FAT por sus siglas en inglés), se obtuvieron las siguientes especificaciones:

Características Técnicas.

- Monitoreo de Servicios de Red (SMTP, POP3, HTTP, NNTP, PING, etc.)
- Monitoreo de los recursos de los servidores(carga del procesador, uso de disco, etc.)
- Chequeo de servicios en paralelo.
- Capacidad para definir la jerarquía de los equipos de la red.
- Notificaciones cuando el servicio o el equipo presenta algún tipo de conflicto (vía email, pager, o cualquier otro método que defina el administrador)
- Rotación de logs automática
- Soporte para implementar equipos de monitoreo redundante
- Interfaz web opcional.

Indicadores.

El cuadro 4 muestra los resultados obtenidos en la evaluación de los indicadores de eficiencia, eficacia, economicidad y productividad a juicio de expertos para el Proyecto Nagios, obteniéndose los siguientes resultados:

Cuadro 4. Indicadores Nagios

Eficiencia	Eficacia	Economicidad	Productividad	Total
Altamente eficiente por maximizar los recursos utilizados. **25% Eficiente**	Altamente eficaz para la plataforma de monitoreo de seguridad por contar con módulos para el control de equipos (hardware). **25% Eficaz**	Altamente económica por ser software libre y no generar gastos de licenciamiento. **25% Económico**	Altamente productivo para la plataforma de monitoreo de seguridad. **25% Productivo**	**100%**

3. Cacti

De acuerdo a lo expresado por el fabricante en la página web http://docs.cacti.net/manual:087, en donde se evidencia toda la información técnica del producto e información registrada por parte de las Pruebas de Aceptación de Fábrica (FAT por sus siglas en inglés), se obtuvieron las siguientes especificaciones:

Es una solución open source para la generación de gráficos en red, . Esta herramienta, desarrollada en PHP, provee un pooler ágil, plantillas de gráficos avanzadas, múltiples métodos para la recopilación de datos, y manejo de usuarios. Tiene una interfaz de usuario fácil de usar, que resulta conveniente para instalaciones del tamaño de una LAN, así como también para redes complejas con cientos de dispositivos.

Indicadores

El cuadro 5 muestra los resultados obtenidos en la evaluación de los indicadores de eficiencia, eficacia, economicidad y productividad a juicio de expertos para la herramienta Cacti, obteniéndose los siguientes resultados:

Cuadro 5. Indicadores Cacti

Eficiencia	Eficacia	Economicidad	Productividad	Total
Altamente eficiente por maximizar los recursos utilizados. **25% Eficiente**	Medianamente eficaz para la plataforma de monitoreo de seguridad, ya que almacena gráficas de comportamiento en los servidores (hardware). **15% Eficaz**	Altamente económica por ser software libre y no generar gastos de licenciamiento. **25% Económico**	Medianamente productivo para la plataforma de monitoreo de seguridad. **15% Productivo**	**80%**

4. NetFlow

Es un protocolo de red desarrollado por Cisco Systems para recolectar información sobre tráfico IP. Netflow se ha convertido en un estándar de la industria para

monitorización de tráfico de red, y actualmente se está soportado para varias plataformas además de Cisco IOS y NXOS, como por ejemplo en dispositivos de fabricantes como Juniper, Enterasys recolectar datos NetFlow/IPFIX. De acuerdo a lo expresado por el fabricante en la página web http://www.cisco.com/cisco/web/psa/default.html?mode=tech, en donde se evidencia toda la información técnica del producto e información registrada por las Pruebas de Aceptación de Fábrica (FAT por sus siglas en inglés), se obtuvieron las siguientes especificaciones:

Características técnicas

Medición de los siguientes parámetros:

- Los equipos que transmiten más datos en la red
- Los equipos que transmiten más datos con algún otro equipo
- Las aplicaciones que generan más tráfico en la red
- Volumen de datos por entidad
- Velocidades de transmisión por entidad
- Marcado de ToS (Tipo de Servicio) por aplicación o entidad.

Indicadores

El cuadro 6 muestra los resultados obtenidos en la evaluación de los indicadores de eficiencia, eficacia, economicidad y productividad a juicio de expertos para la herramienta Netflow, obteniéndose los siguientes resultados:

Cuadro 6. Indicadores Netflow

Eficiencia	Eficacia	Economicidad	Productividad	Total
Poco eficiente. **0% Eficiente**	Para la plataforma de Monitoreo de Seguridad de Cantv sería poco eficaz, debido a que no realiza la medición de los procesos a nivel de plataformas, sino a nivel de tráfico de red. **0% Eficaz.**	Poco económica por ser software que requerir de inversión monetaria para su instalación. **0% Económico**	Baja. **0% productiva**	**0%**

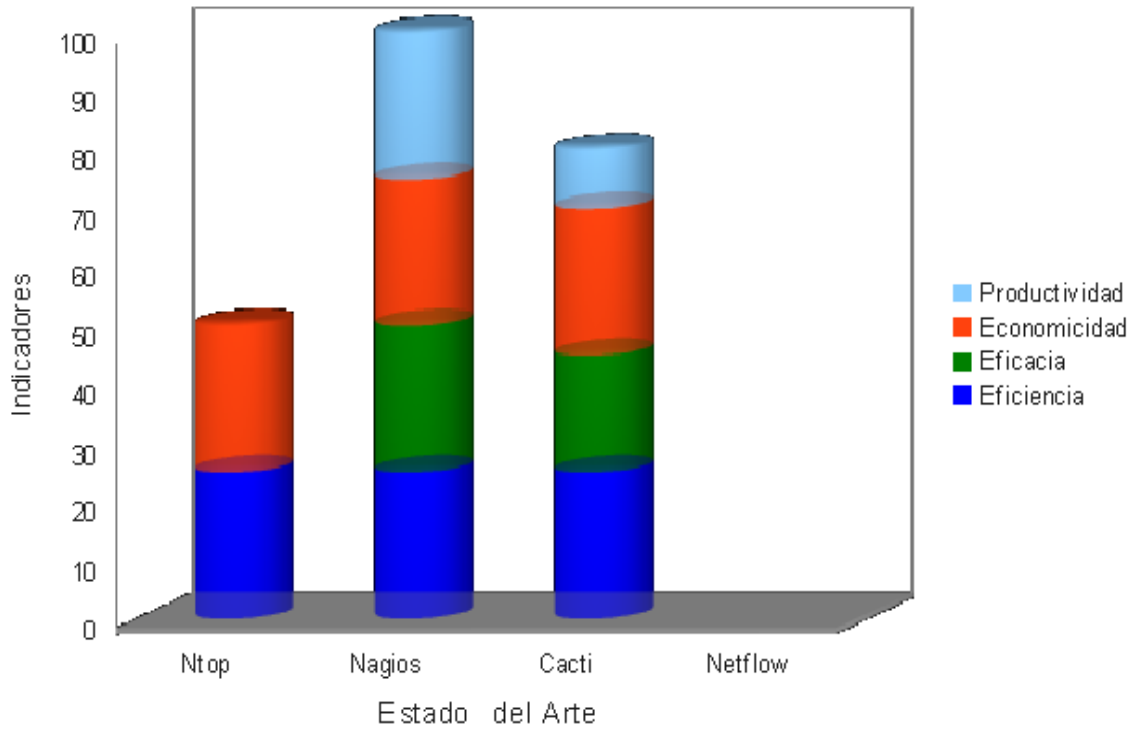
En el cuadro 7 se muestra un resumen de los resultados obtenidos en el análisis del estado del arte en la medición de rendimiento en plataformas de seguridad tecnológica.

Cuadro 7. Resumen Indicadores de estado del arte.

Herramientas	Eficiencia	Eficacia	Economicidad	Productividad	Total
Proyecto Ntop	Altamente eficiente por maximizar los recursos utilizados.	Para la plataforma de Monitoreo de Seguridad de Cantv sería poco eficaz, debido a que no realiza la medición de los procesos a nivel de plataformas, sino a nivel de tráfico de red.	Altamente económica por ser software libre y no generar gastos de licenciamiento.	Baja.	50%
Nagios	Altamente eficiente por maximizar los recursos utilizados.	Altamente eficaz para la plataforma de monitoreo de seguridad por contar con módulos para el control de equipos (hardware)	Altamente económica por ser software libre y no generar gastos de licenciamiento.	Altamente productivo para la plataforma de monitoreo de seguridad.	100%
Cacti	Altamente eficiente por maximizar los recursos utilizados.	Medianamente eficaz para la plataforma de monitoreo de seguridad, ya que almacena gráficas de comportamiento en los servidores (hardware)	Altamente económica por ser software libre y no generar gastos de licenciamiento.	Medianamente productivo para la plataforma de monitoreo de seguridad.	80%
Netflow	Poco eficiente	Para la plataforma de Monitoreo de Seguridad de Cantv sería poco eficaz, debido a que no realiza la medición de los procesos a nivel de plataformas, sino a nivel de tráfico de red.	Poco económica por ser software requerir inversión para su instalación	Baja	0%

El gráfico 1 muestra la representación de los datos recabados anteriormente para cada una de las herramientas enmarcadas en el análisis del estado del arte en plataformas de seguridad tecnológica.

Gráfico 1. Evaluación del estado del arte.



Al observar los resultados obtenidos, se evidencia que de acuerdo a las necesidades actuales de la CANTV, el estado del arte que mejor se adapta a los requerimientos es el que está dado por el uso de la herramienta **Nagios**, por cumplir al 100% con los parámetros de Eficiencia, eficacia, economicidad y productividad, dados de acuerdo a la escala de juicio de expertos, en donde se evaluaron dichos indicadores en cada una de las herramientas.

5.3 Desarrollo del objetivo específico Nº 2. Evaluar el nivel de disponibilidad actual la plataforma de monitoreo de seguridad tecnológica de CANTV.

Actualmente la plataforma de monitoreo de seguridad tecnológica cuenta con un total de 15 servidores desplegados a lo largo de la red corporativa de CANTV, de los cuales 13 corresponden a los sensores IDS y 2 corresponden a las consolas de visualización de eventos de seguridad snort y LML, a continuación se describe el funcionamiento de dichos servidores:

- **Sensores IDS:** Son los dispositivos encargados de registrar todo el tráfico que circula en las diversas redes de CANTV, que luego analiza y compara de acuerdo a diversos patrones de tráfico malicioso para generar las diversas alertas de seguridad que son almacenadas en las consolas de visualización de eventos de seguridad snort y LML.

- **Consolas de visualización de eventos de seguridad:** En la consola snort se muestran las alertas de virus y ataques informáticos en contra de las redes y elementos de Tecnologías de Información de la CANTV, mientras que en la consola LML se muestran las alertas generadas en los logs de los dispositivos informáticos instalados en la red de CANTV y empresas filiales

El cuadro 8 muestra el listado de servidores que comprenden la plataforma de monitoreo de Seguridad Tecnológica:

Cuadro 8. Servidores plataforma de monitoreo de seguridad tecnológica.

Servidor	Función
Consola Snort	Consolas de visualización de eventos de seguridad
Consola LML	
IDS_CNT GESTIÒN	Sistemas de Detección de Intrusos, dispositivos en los que se almacena y analiza el tráfico de red
IDS_FW CORPORATIVO	
IDS_PROXYS	
IDS_CHACAO GESTIÒN	
IDS_FW CORPORATIVO 2	
IDS_XPERT	
IDS_MOVILNET	
IDS_CET	
IDS_LPG GESTIÓN	
IDS_LOS CORTIJOS	
IDS_BBO	
IDS_BOSS 01	
IDS_BOSS 02	

En la figura 7 correspondiente al diagrama de la plataforma de Monitoreo de Seguridad Tecnológica, se muestra la ubicación lógica de cada uno de los 15 servidores.

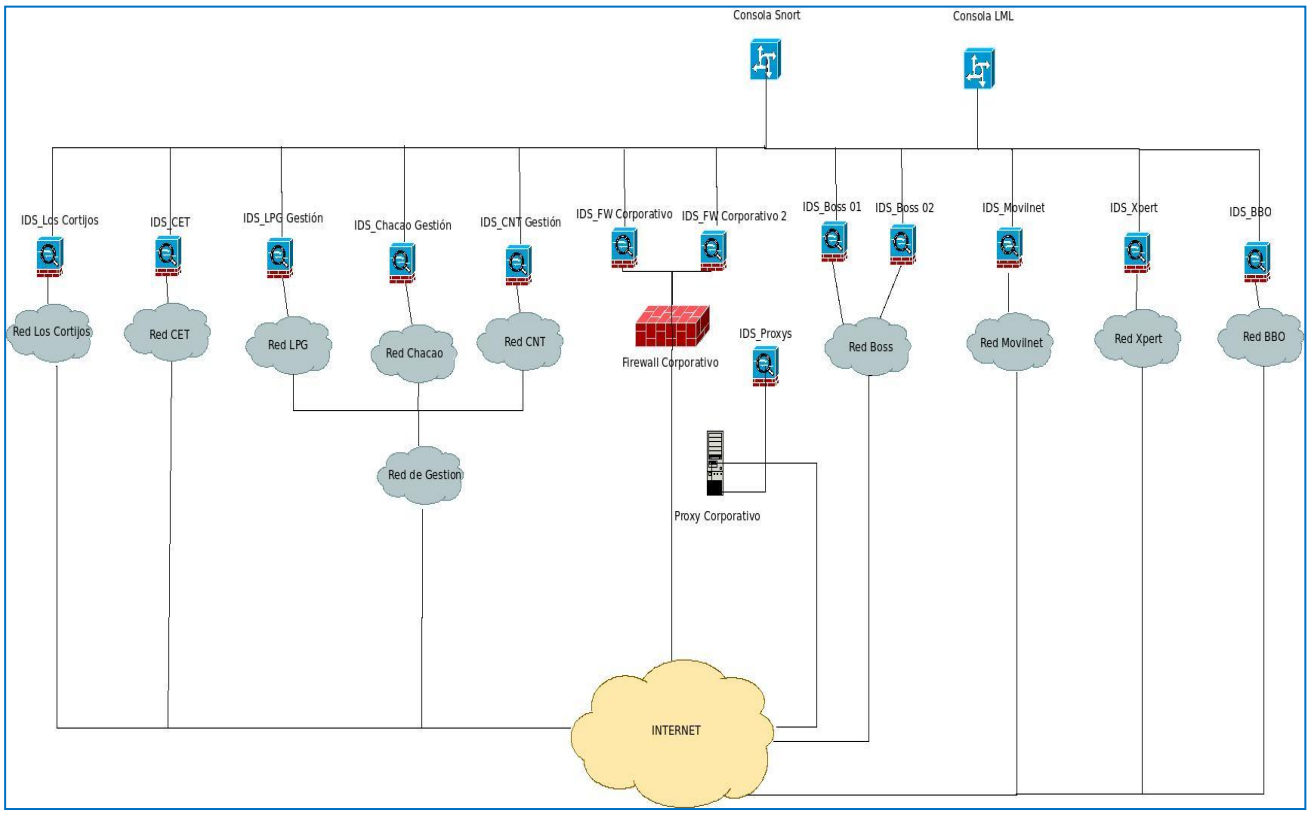


Figura 7. Diagrama de la plataforma de Monitoreo de Seguridad Tecnológica

El cuadro 9 muestra las fallas de cada uno de los servidores de acuerdo a su fecha de ocurrencia, asimismo se evidencia si la falla afectó o no el servicio del equipo y la cantidad de horas que permaneció el servidor fuera de línea a causa de la falla.

Cuadro 9. Lista de fallas en los servidores plataforma de monitoreo de seguridad tecnológica.

Fecha de la falla	Servidor	Afectó el servicio s/n	Cantidad de horas offline
09/12/12	Consola LML	s	5
06/12/12	Consola snort	s	1
14/12/12	Consola snort	s	3
23/01/13	IDS_BACKBONE OPERACIONAL	s	2
25/01/13	IDS_BBO	n	0
27/01/13	IDS_BOSS 02	s	6
28/01/13	IDS_BOSS 03	s	4
15/01/13	IDS_CET	n	0
22/01/13	IDS_CET	n	0
15/12/12	IDS_CNT GESTIÓN	s	2
19/12/12	IDS_CNT GESTIÓN	s	4
30/12/12	IDS_FW CORPORATIVO_1	s	6
03/01/13	IDS_FW CORPORATIVO_2	s	4
31/01/13	IDS_LOS CORTIJOS	s	2
19/01/13	IDS_LPG GESTIÓN	s	3
05/01/13	IDS_MOVILNET	s	2
08/01/13	IDS_MOVILNET	s	1
22/12/12	IDS_XPERT	s	1
28/12/12	IDS_XPERT	n	0

El siguiente diagrama causa-efecto muestra las causas más comunes por las cuales existen fallas en la plataforma:

Figura 8. Diagrama Causa-Efecto.

A continuación se describen las causas mostradas en el diagrama anterior:

- **Base de Datos sobrecargada:** Este tipo de falla se presenta cuando la base de datos alcanza un tamaño muy grande, debido a la alta cantidad de datos almacenados, lo cual causa degradación en el servicio teniendo como consecuencia pérdida en la disponibilidad de los equipos.

- **Procesos Corruptos:** Son aquellos procesos informáticos que causan mal funcionamiento de los servidores, a causa de que los datos fueron alterados debido a alguna falla en su transmisión.

- **Duplicación de procesos:** Cuando existe duplicación de procesos los datos de los servidores se corrompen, teniendo como resultado degradación del servicio.

- **Fallas de energía:** Fallas en el suministro eléctrico de los centros de datos donde se albergan los servidores, lo cual ocasiona degradación en el servicio y afectación de la disponibilidad.

- **Fallas de hardware:** Son diversas las fallas del hardware, que pueden ocasionar afectación del servicio, como lo son fan coolers dañados, discos duros, memoria ram, entre otros.

- **Fallas de red:** Son intermitencias en la conexión de la red corporativa que ocasionan afectación del servicio

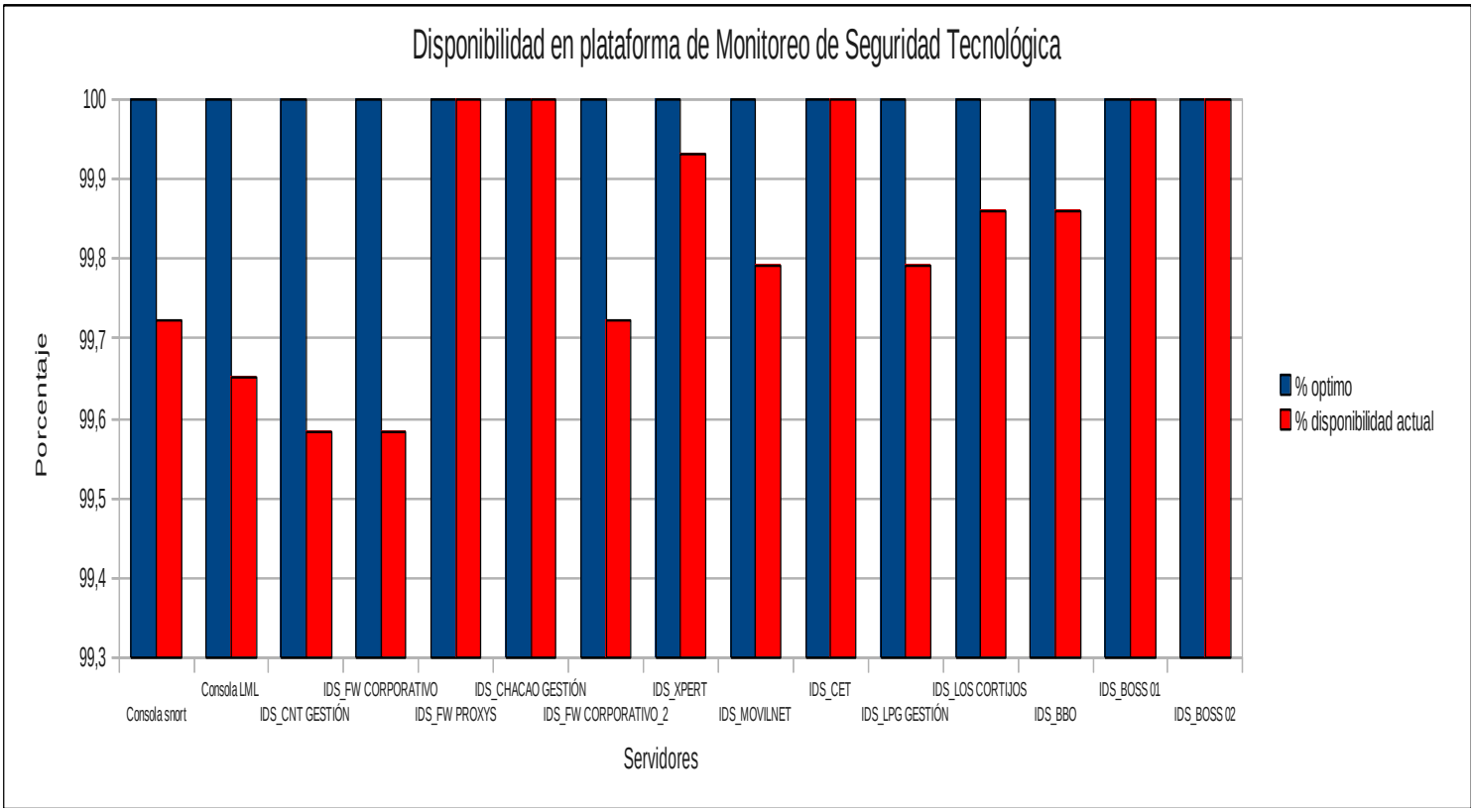
Los niveles de disponibilidad fueron determinados de acuerdo a la cantidad de fallas que han interrumpido el desempeño y funcionamiento de los servidores durante los meses de Diciembre de 2012 y Enero de 2013, dicha disponibilidad fue medida por la cantidad de tiempo (horas) que cada servidor se mantuvo fuera de línea en dicho período de tiempo, comparando la disponibilidad actual con los niveles óptimos de disponibilidad (100%), a continuación se muestran los datos obtenidos:

Cuadro 10. Porcentaje de disponibilidad en los servidores de la plataforma de monitoreo de seguridad tecnológica

Servidor	Disponibilidad optima (h)	Horas de falla	% optimo	% disponibilidad actual
Consola snort	1440	4	100	99,72
Consola LML	1440	5	100	99,65
IDS_CNT GESTIÓN	1440	6	100	99,58
IDS_FW CORPORATIVO	1440	6	100	99,58
IDS_FW PROXYS	1440	0	100	100
IDS_CHACAO GESTIÓN	1440	0	100	100
IDS_FW CORPORATIVO_2	1440	4	100	99,72
IDS_XPERT	1440	1	100	99,93
IDS_MOVILNET	1440	3	100	99,79
IDS_CET	1440	0	100	100,00
IDS_LPG GESTIÓN	1440	3	100	99,79
IDS_LOS CORTIJOS	1440	2	100	99,86
IDS_BBO	1440	2	100	99,86
IDS_BOSS 01	1440	0	100	100
IDS_BOSS 02	1440	0	100	100

El gráfico 2 muestra la disponibilidad de cada uno de los servidores con respecto a los niveles óptimos de disponibilidad (100%)

Gráfico 2. Disponibilidad en la plataforma de monitoreo de seguridad tecnológica.



La gráfica anterior muestra los niveles de disponibilidad de todos y cada uno de los servidores que conforman la plataforma de monitoreo de seguridad tecnológica con respecto al porcentaje óptimo (100%), de acuerdo a los resultados obtenidos se evidencia que en los últimos 2 meses los servidores con mayor tiempo fuera de línea fueron los IDS_CNT_GESTION e IDS_FW_CORPORATIVO, esto es debido a diversos cortes de energía en la zona que interrumpieron su funcionamiento, cabe destacar que es importante la reducción en los tiempos de falla, ya que los tiempos que los servidores permanecieron caídos están en la magnitud de horas, debido a que no se cuenta con una herramienta que permita la visualización de las fallas al instante, lo

cual le permite a los técnicos solventarlas de manera expedita y reducción en los tiempos de fallas.

5.4 Desarrollo del objetivo específico Nº 3. Proponer una aplicación informática que permita detectar y alertar las fallas dentro de la plataforma de monitoreo de seguridad tecnológica de CANTV.

De acuerdo a los resultados obtenidos anteriormente en la evaluación de los estados del arte de las diversas tecnologías ligadas a la medición del rendimiento en plataformas de seguridad en las que se evaluaron de acuerdo a juicio de expertos diversos indicadores de eficacia, eficiencia, economicidad y productividad y a las diversas pruebas y protocolos enmarcados en las SAT (Pruebas de aceptación en Sitio), los usuarios que realizaron las pruebas fueron los analistas de seguridad tecnológica encargados de realizar el monitoreo de la plataforma, con experiencia en el área de redes de datos y análisis de tráfico de red, dichas pruebas constaron de lo siguiente:

- **Pruebas de Integración:** Realizadas para asegurar que todos los puntos de integración están funcionando como se especifica en los requisitos por parte de CANTV y la documentación técnica presentadas por el fabricante.
- **Pruebas de desempeño:** Las pruebas de desempeño del sistema se realizan en un entorno adecuado para asegurar el cumplimiento de todos a los requisitos de desempeño por parte de CANTV. Esta prueba garantiza que el rendimiento de la aplicación se encuentra dentro de la tolerancia, basado en el volumen de pedidos y usuarios.
- **Pruebas de aceptación del usuario (UAT):** Validan que la solución es compatible con la CANTV en sus operaciones del día a día y procesos de negocio de extremo a extremo. En la fase UAT, los usuarios seleccionados

realizan las pruebas referentes a los procesos de negocio y afectación de los servicios.

Los resultados arrojados en cada una de las pruebas mencionadas anteriormente lograron evidenciar que la tecnología ligada a la herramienta Nagios es la que mejor se adapta a las redes y plataformas de Monitoreo de Seguridad Tecnológica de CANTV, debido a que cumple con los indicadores de Efiencia, Eficacia, Economicidad y productividad, de acuerdo a los juicios de expertos presentados con anterioridad y las pruebas SAT, debido a que con dicha aplicación se pueden controlar y monitorear los equipos (hardware) y servicios (software) deseados, informando cuando el comportamiento de los mismos no cumpla con los parámetros adecuados de funcionamiento, a continuación se presentan los datos correspondientes a la evaluación de la aplicación en la que se presentan la las aplicaciones empleadas para la medición del rendimiento en plataformas de seguridad de acuerdo a los indicadores de productividad, eficacia, eficiencia y economicidad, tal como se indicó anteriormente cada indicador representa el 25% del valor total de decisión, es decir que con la suma de los cuatro indicadores se obtiene un total del 100%, por tal razón el estado que se aproxime al 100% sería el más adecuado para el proyecto, la escala para la medición se enmarcó en el juicio de expertos quienes son ingenieros y técnicos del área de seguridad tecnológica de CANTV con experiencia en redes y en medición de parámetros de rendimiento y seguridad con certificaciones internacionales que avalan la decisión para cada indicador, las escalas se representan de la siguiente forma:

0% = Bajo

15% = Medio

25% = Alto

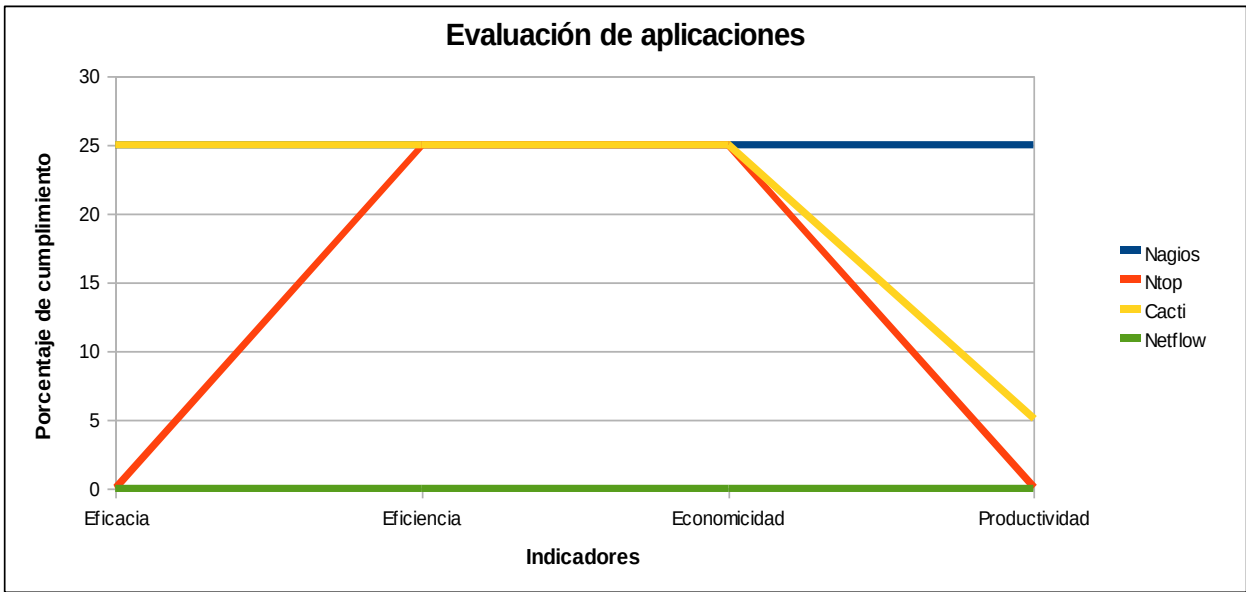
Los resultados obtenidos se muestran en el cuadro 11.

Cuadro 11. Evaluación de las aplicaciones informáticas.

	Porcentaje de cumplimiento (%)			
Aplicaciones	Nagios	Ntop	Cacti	Netflow
Eficacia	25	0	25	0
Eficiencia	25	25	25	0
Economicidad	25	25	25	0
Productividad	25	0	5	0
Total	**100**	**50**	**80**	**0**

La siguiente gráfica un resumen de la evaluación de las aplicaciones de acuerdo a los indicadores de eficacia, eficiencia, productividad y economicidad.

Gráfico 3. Evaluación de las aplicaciones informáticas.



Tal como lo indica la gráfica anterior, la aplicación que mejor se adapta a la plataforma de Monitoreo de Seguridad Tecnológica de CANTV es **NAGIOS**, debido a que obtuvo un total del 100% de porcentaje de cumplimiento de los indicadores de medición, es decir se observó que para cada uno de los indicadores su valor fue de un 25%, por lo que al observar la gráfica se evidencia una línea recta en 25%, lo cual comprueba lo mencionado anteriormente, que para cada indicador el valor fue de 25% (máximo permitido), mientras que el resto de aplicaciones muestra un comportamiento en forma de trapecio o línea recta en 0%, lo cual indica que de acuerdo a la escala propuesta no cumplen con los indicadores presentados.

5.5 Desarrollo del objetivo específico Nº 4. Diseñar el plan para la medición de la disponibilidad de los equipos y servicios de la plataforma de monitoreo de seguridad tecnológica:

Definición de Documento de Alcance del Proyecto:

A continuación se presenta el alcance preliminar del proyecto en donde se desarrollan los diversos parámetros y requisitos iniciales necesarios para la implantación del plan para la medición de la disponibilidad de los equipos y servicios de la plataforma de monitoreo de seguridad tecnológica.

- **Justificación**

Se requiere Diseñar un plan para la medición del rendimiento en la plataforma de Monitoreo de Seguridad Tecnológica de CANTV, con el fin de disminuir el tiempo de las fallas presentadas en dicha plataforma

- **Descripción del Producto**

- Aumento de los niveles de disponibilidad en los servidores de la plataforma de monitoreo de seguridad tecnológica de CANTV en un lapso de 3 meses.
- Detección de las posibles fallas dentro de la plataforma de monitoreo seguridad tecnológica.

- **Entregables finales**

- Estado del arte en la medición del rendimiento de plataformas de seguridad tecnológica.
- Nivel de disponibilidad actual de la plataforma de monitoreo de seguridad tecnológica de CANTV.
- Aplicación informática para detectar y alertar las fallas dentro de la plataforma de monitoreo de seguridad tecnológica de CANTV.
- Plan para la medición de la disponibilidad de los equipos y servicios de la plataforma de monitoreo de seguridad tecnológica.

- **Requisitos (premisas)**

- Detectar y corregir las fallas en la plataforma de monitoreo de seguridad tecnológica de CANTV en menor tiempo.
- Contar con un sistema de medición del rendimiento en los equipos (hardware) y servicios (software) de la plataforma de monitoreo de seguridad tecnológica de CANTV, alertando cuando el comportamiento de los mismos no sea el adecuado.
- Aumentar los niveles de protección de los activos de la corporación.

- **Restricciones**

- Entregar el plan en 3 meses antes del 28 de Febrero de 2013.
- Se deben aprovechar al máximo los servidores que actualmente se encuentran desincorporados en otros departamentos de seguridad.
- Cada servidor debe contar con protección mediante firewalls, antivirus, antimalware, HIDS, entre otros.
- La instalación de los servidores se debe realizar en ambientes seguros con los servidores de producción.

- El diseño debe estar basado en software libre para la instalación de las aplicaciones.
- El presupuesto disponible es de 300000 Bs para la compra de servidores y mantenimiento del software.

Definición de Estructura Desagregada de Trabajo (WBS):

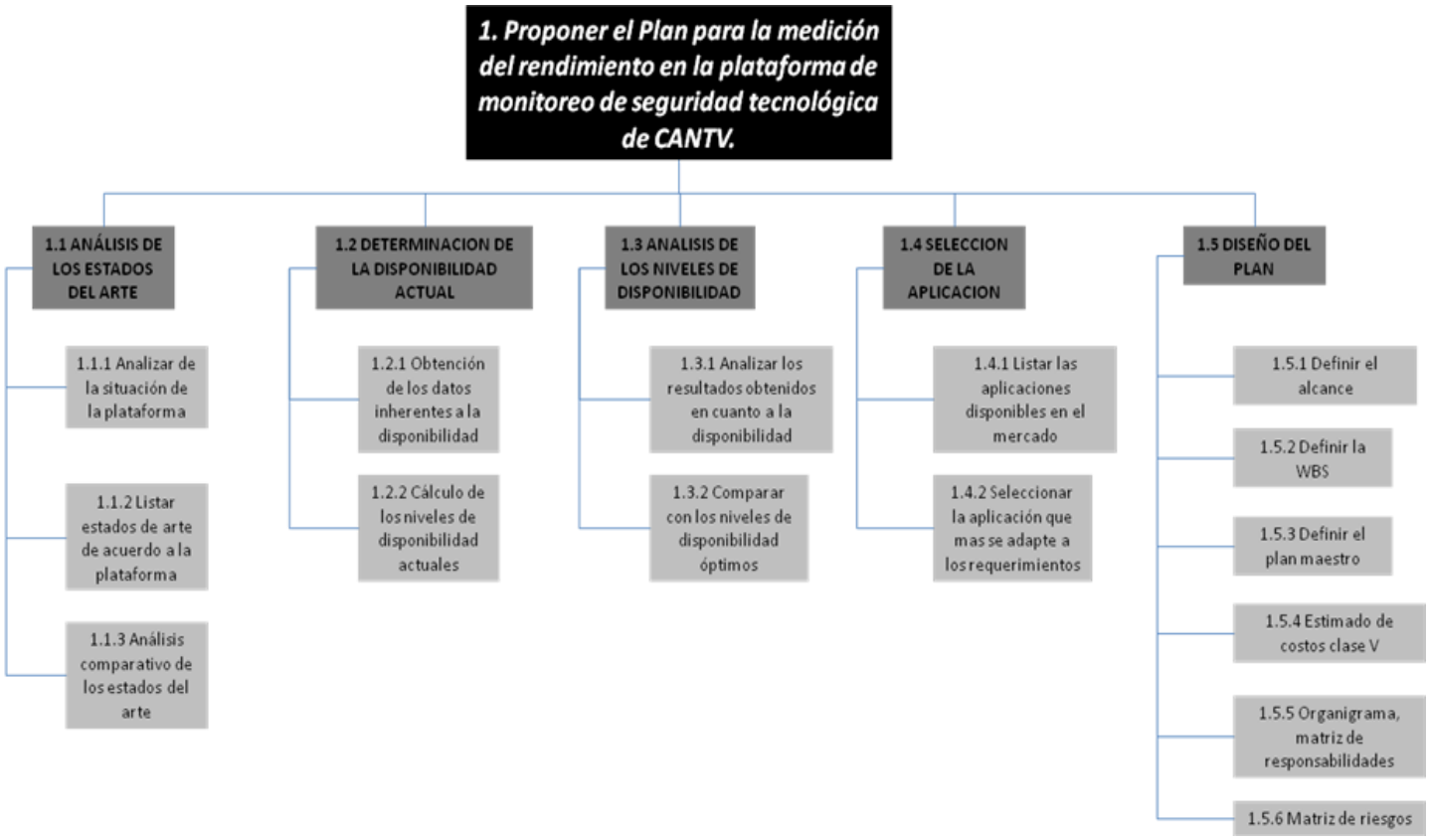


Figura 9. Estructura desagregada de trabajo.

Diccionario de la EDT

A continuación se presenta el esquema que define el diccionario de la EDT:

<u>TITULO DEL PROYECTO</u>: "PROPUESTA DE UN PLAN PARA LA MEDICIÓN DE RENDIMIENTO EN LA PLATAFORMA DE MONITOREO DE SEGURIDAD TECNOLÓGICA DE CANTV".

Cuadro 12. Diccionario de la EDT.

1.1	**Análisis del Estado del Arte**
Descripción	Evaluación las diversas tecnologías para la medición del rendimiento en plataformas de seguridad
Actividades	1. Analizar de la situación de la plataforma 2. Listar estados de arte de acuerdo a la plataforma 3. Análisis comparativo de los estados del arte
Duración	5 días hábiles.
Responsable	Equipo del Proyecto.

1.2	**Determinación de la disponibilidad actual**
Descripción	Investigar el estado de la plataforma para verificar cual es el nivel de disponibilidad en cada uno de los servidores que la componen
Actividades	1. Obtención de los datos inherentes a la disponibilidad. 2. Cálculo de los niveles de disponibilidad actuales
Duración	3 días hábiles.
Responsable	Analistas de seguridad tecnológica.

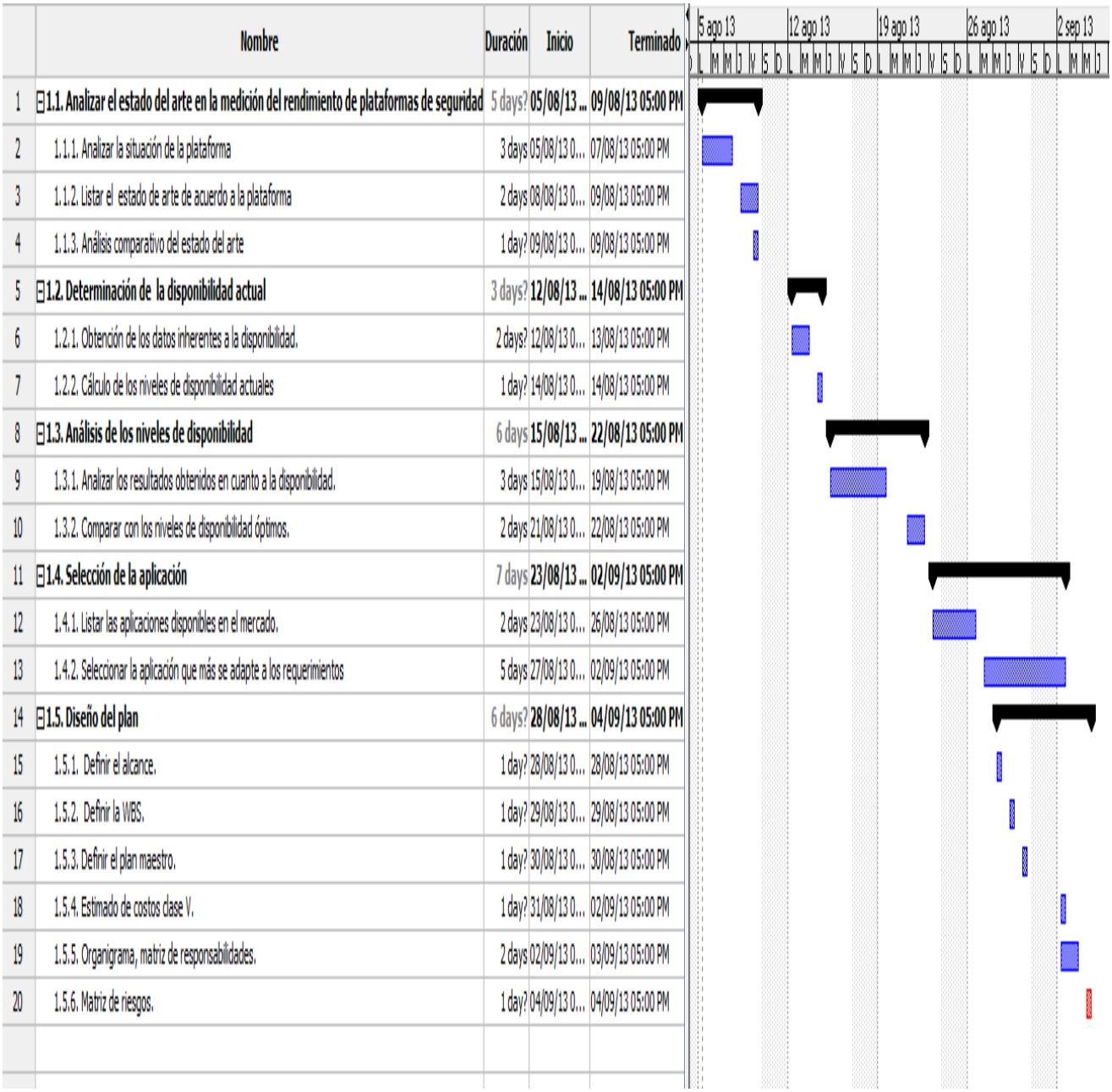
1.3	**Análisis de los niveles de disponibilidad**
Descripción	Analizar el estado de las fallas presentes en la plataforma de monitoreo de seguridad tecnológica y como afectan su disponibilidad.
Actividades	1. Analizar los resultados obtenidos en cuanto a la disponibilidad. 2. Comparar con los niveles de disponibilidad óptimos.
Duración	6 días hábiles.
Responsable	Consultor de seguridad tecnológica.

1.4	Selección de la aplicación
Descripción	De acuerdo a los análisis realizados, elegir cual aplicación se adapta a los requerimientos de CANTV
Actividades	1. Listar las aplicaciones disponibles en el mercado. 2. Seleccionar la aplicación que más se adapte a los requerimientos
Duración	7 días hábiles.
Responsable	Consultor de seguridad tecnológica.

1.5	Diseño del plan
Descripción	Diseñar el plan para la ejecución del proyecto.
Actividades	1. Definir el alcance. 2. Definir la WBS. 3. Definir el plan maestro. 4. Estimado de costos clase V. 5. Organigrama, matriz de responsabilidades. 6. Matriz de riesgos.
Duración	7 días hábiles.
Responsable	Consultor de seguridad tecnológica.

Cronograma del Proyecto

Cuadro 13. Cronograma del Proyecto



	Nombre	Duración	Inicio	Terminado
1	1.1. Analizar el estado del arte en la medición del rendimiento de plataformas de seguridad	5 days?	05/08/13 ...	09/08/13 05:00 PM
2	1.1.1. Analizar la situación de la plataforma	3 days	05/08/13 0...	07/08/13 05:00 PM
3	1.1.2. Listar el estado de arte de acuerdo a la plataforma	2 days	08/08/13 0...	09/08/13 05:00 PM
4	1.1.3. Análisis comparativo del estado del arte	1 day?	09/08/13 0...	09/08/13 05:00 PM
5	1.2. Determinación de la disponibilidad actual	3 days?	12/08/13 ...	14/08/13 05:00 PM
6	1.2.1. Obtención de los datos inherentes a la disponibilidad.	2 days?	12/08/13 0...	13/08/13 05:00 PM
7	1.2.2. Cálculo de los niveles de disponibilidad actuales	1 day?	14/08/13 0...	14/08/13 05:00 PM
8	1.3. Análisis de los niveles de disponibilidad	6 days	15/08/13 ...	22/08/13 05:00 PM
9	1.3.1. Analizar los resultados obtenidos en cuanto a la disponibilidad.	3 days	15/08/13 0...	19/08/13 05:00 PM
10	1.3.2. Comparar con los niveles de disponibilidad óptimos.	2 days	21/08/13 0...	22/08/13 05:00 PM
11	1.4. Selección de la aplicación	7 days	23/08/13 ...	02/09/13 05:00 PM
12	1.4.1. Listar las aplicaciones disponibles en el mercado.	2 days	23/08/13 0...	26/08/13 05:00 PM
13	1.4.2. Seleccionar la aplicación que más se adapte a los requerimientos	5 days	27/08/13 0...	02/09/13 05:00 PM
14	1.5. Diseño del plan	6 days?	28/08/13 ...	04/09/13 05:00 PM
15	1.5.1. Definir el alcance.	1 day?	28/08/13 0...	28/08/13 05:00 PM
16	1.5.2. Definir la WBS.	1 day?	29/08/13 0...	29/08/13 05:00 PM
17	1.5.3. Definir el plan maestro.	1 day?	30/08/13 0...	30/08/13 05:00 PM
18	1.5.4. Estimado de costos clase V.	1 day?	31/08/13 0...	02/09/13 05:00 PM
19	1.5.5. Organigrama, matriz de responsabilidades.	2 days	02/09/13 0...	03/09/13 05:00 PM
20	1.5.6. Matriz de riesgos.	1 day?	04/09/13 0...	04/09/13 05:00 PM

Plan Maestro de Ejecución del Proyecto

Cuadro 14. Plan maestro del proyecto.

PROPUESTA / PRIORIDAD	INMEDIATO (0-6 meses)	CORTO PLAZO (6 meses-1 año)	ACTIVIDADES	RESPONSABLES
Análisis de los estados del arte en la medición del desempeño en plataformas de monitoreo de seguridad tecnológica	X		Comparar y analizar todas las tecnologías ligadas a la medición del desempeño en plataformas de seguridad tecnológica.	Gerente del proyecto
Determinación de los niveles de disponibilidad actual de la plataforma de monitoreo de seguridad tecnológica de CANTV	X		Analizar el estado de la plataforma de monitoreo de seguridad tecnológica de CANTV con respecto a la disponibilidad de los servicios críticos de la misma y comparar con los patrones adecuados de funcionamiento	Gerente del proyecto
Detección de fallas en la plataforma de Monitoreo de Seguridad tecnológica de CANTV	X		Detectar aquellos patrones de comportamiento no adecuado en los servicios de la plataforma de monitoreo de seguridad tecnológica	Analistas de Seguridad tecnológica
Selección de la aplicación informática para la medición del desempeño en la plataforma de monitoreo e seguridad tecnológica de CANTV	X		Seleccionar un software que se adapte a los requerimientos de la plataforma y que logre alarmar aquellos estados y comportamientos no adecuados en los servicios de dicha plataforma	Consultores de Seguridad Tecnológica
Instalación del hardware		x	Instalar los servidores que contemplarán los sistemas para la medición del rendimiento en plataforma	Analistas de Seguridad tecnológica
Instalación del software		x	Instalar la aplicación informática seleccionada	Analistas de Seguridad tecnológica

Estimado de Presupuesto Clase V

El presupuesto base es calculado de acuerdo a un estimado de costos Clase V que se presenta a continuación:

Cuadro 15. Estimado de costos clase V.

Elemento de Costos	Bs.
Servidor de Alto Rendimiento	20000
Licencias del software	5000
Aplicativo para la medición del rendimiento	300
Mantenimiento (anual)	1000
Total	26.300

El presente estimado de costos se ajusta a lo estipulado por CANTV en el presupuesto de inversión para el año 2013, el cual es de Bs 30.000.

Organigrama del Proyecto.

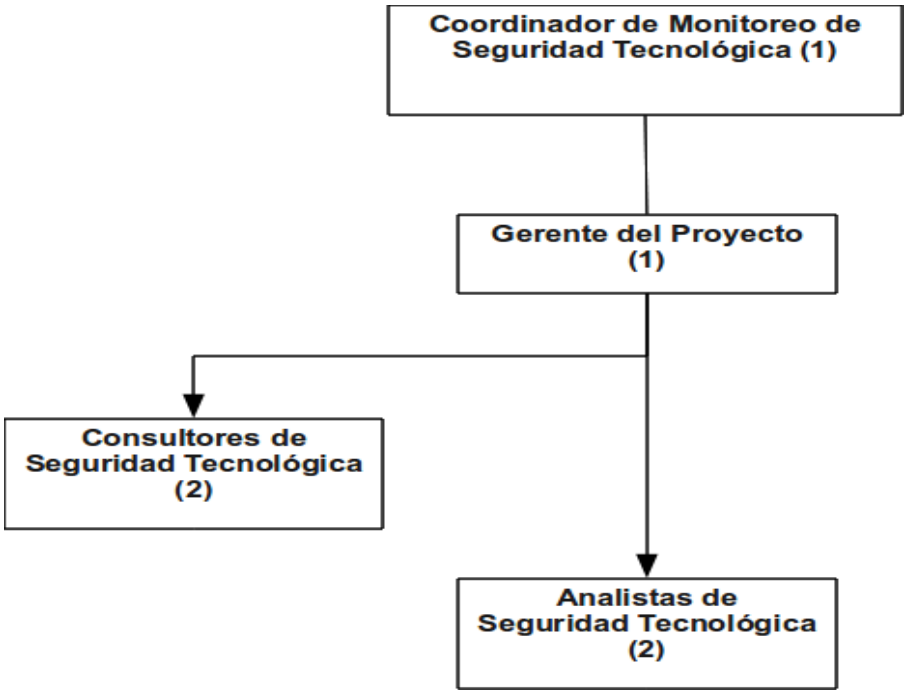


Figura 10. Organigrama. Del proyecto

Matriz de Roles y Responsabilidades del Proyecto.

Cuadro 16. Matriz de roles y responsabilidades.

Actividades	Coordinador de Monitoreo de Seguridad tecnológica	Gerente del Proyecto	Consultor de Seguridad Tecnológica 1	Consultor de Seguridad Tecnológica 2	Analista de Seguridad Tecnológica 1	Analista de Seguridad Tecnológica 2
Seguimiento del Proyecto	I	R				
Diseño del Plan	AI	RE	A	A		
Determinación de los niveles de disponibilidad actuales	I	R	A	A	E	E
Detección de las fallas en la plataforma	I	I			RE	RE
Selección de la aplicación	I	I	R	R		
Instalación del hardware	I	I	A	AR	RE	RE
Instalación del software	I	I	AR	A	RE	RE
I: Informado R: Responsable E: Ejecuta A: Asesora						

Matriz de Riesgos

La matriz de riesgo a utilizar está enmarcada en la plantilla de la Unidad de política interinstitucional y proyectos del gobierno de Tasmania, en la cual se emplea la relación entre la probabilidad y severidad al momento de afrontar un posible incidente o riesgo los siguientes cuadros señalan la explicación de cómo aplicar la relación entre probabilidad y severidad, para obtener el grado y a partir de allí ejecutar las acciones de mitigación, que se muestran en el cuadro 18.

Cuadro 17. Clasificación de la probabilidad y severidad de cada riesgo.

Clasificación de la probabilidad y severidad de cada riesgo			
L	Bajo	E	Extremo (solo severidad)
M	Medio	NA	No aplica
H	Alto		

Fuente: CANTV (2013).

Cuadro 18. Efecto combinado de la probabilidad / Severidad.

Grado: Efecto combinado de la probabilidad / Severidad					
	Severidad				
Probabilidad		Bajo	Medio	Alto	Extremo
	Bajo	N	D	C	A
	Medio	D	C	B	A
	Alto	C	B	A	A

Cuadro 19. Acciones recomendadas para los grados de riesgo.

Acciones recomendadas para los grados de riesgo	
Grado	**Acciones de mitigación de riesgo**
A	Las acciones de mitigación para reducir l probabilidad severidad, deben identificarse y aplicarse antes del inicio del proyecto como una prioridad.
B	Las acciones de mitigación para reducir la probabilidad y severidad, deben identificarse y aplicarse durante la ejecución del proyecto.
C	Las acciones de mitigación, para reducir la probabilidad y la gravedad, deben ser aplicadas sólo si lo permite el presupuesto.
D	No se requiere acción alguna a menos que se incremente el grado de riesgo con el tiempo
N	Para señalar - no se requiere ninguna acción a menos que los riesgos aumenten con el tiempo

Cuadro 20. Matriz de Riesgos

Nº	Descripción del riesgo	Impacto en el proyecto	Probabilidad	Severidad	Grado
1	**Cronograma sumamente ajustado**	Retrasos en la ejecución y entrega del proyecto	M	M	C
2	**Restricciones presupuestarias**	Suspensión del proyecto o modificaciones en el alcance por carencia de presupuesto	L	H	C
3	**Rotación de personal**	Retrasos en la ejecución y entrega del proyecto	M	M	C
4	**Cambios**	Retrasos, asignación de nuevas responsabilidades al equipo del proyecto	M	H	B
5	**Virus**	Retrasos en la ejecución del proyecto, pérdida de integridad en equipos informáticos del proyecto	M	H	B

Plan de Contingencia

Cuadro 21. Plan de Contingencia.

Descripción del riesgo	Estrategia de mitigación	Responsable	Fecha	Recursos
Cronograma sumamente ajustado	Realizar ajustes de recursos con el fin de cumplir con las expectativas de los stakeholders	Gerente del proyecto	06/08/2013	30 Horas hombre
Restricciones presupuestarias	Ajustar el alcance del proyecto y comunicar la situación a los stakeholders con el fin de aprobar dichos ajustes.	Gerente del proyecto	08/08/2013	6 Horas hombre
Rotación de personal	Poseer memoria descriptiva y documentación de cada una de las actividades a realizar a fin de que el personal nuevo pueda comprender rápidamente el proyecto	Consultores de seguridad tecnológica	13/08/2013	10 Horas hombre
Cambios	Realizar modificaciones en los recursos (humanos y monetarios) a fin de ajustarse a los cambios realizados.	Gerente de proyecto	09/08/2013	5 Horas hombre
Virus	Poseer respaldos periódicos de los sistemas con el fin de recuperarlos en caso de presentarse algún virus que corrompa dichos sistemas, así como mantener actualizado los antivirus.	Analistas de seguridad tecnológica	11/08/2013	8 Horas hombre

CAPÍTULO VI. ANÁLISIS DE LOS RESULTADOS.

6.1 Resultados obtenidos

En esta sección se realizará el Plan de Ejecución del proyecto PEP en el que se presentará la propuesta para la medición del rendimiento en la plataforma de monitoreo de Seguridad Tecnológica de CANTV de acuerdo a lo presentado capítulo V, dicho plan está representado por la integración de los siguientes planes:

Plan del alcance.

Plan del manejo del tiempo.

Plan de Gestión del personal.

Plan del manejo de costos.

Plan de respuesta a los riesgos.

6.2 Plan de Ejecución del proyecto

En el cuadro 22 se presenta un resumen del plan de ejecución del proyecto, el mismo fue tomado de la plantilla de la Unidad de política interinstitucional y proyectos del gobierno de Tasmania.

Cuadro 22. Plan de ejecución del Proyecto

Plan	Descripción
Plan del alcance	El plan del alcance viene dado por la definición del documento del alcance, en el cual se presentó el alcance preliminar del proyecto conformado por la justificación, descripción del producto, los entregables finales, los requisitos y las restricciones para elaborar la propuesta, de igual forma se describió la estructura desagregada de trabajo (EDT), adicionalmente se tomaron en cuenta todas y cada uno de los indicios necesarios para la ejecución del plan que involucran al personal y recursos disponibles.
Plan de manejo del tiempo	De acuerdo a lo presentado en la EDT realizada en el plan de gestión del alcance, se elaboró un cronograma con una lista de actividades necesarias para dar cumplimiento al plan de gestión y manejo del tiempo, en el cual se determinó la duración y precedencia de cada una de ellas, de igual forma se elaboró el plan maestro del proyecto en el que se establecieron las prioridades de cada actividad macro del proyecto.
Plan de Gestión del personal.	Se estableció la matriz de roles y responsabilidades de cada uno de los integrantes del proyecto, así como el organigrama en el que se presentó el cargo y/o rol de los integrantes del proyecto
Plan del manejo de costos.	Se elaboró un estimado de costos clase V en el que se representó el valor monetario aproximado de toda la plataforma tecnológica necesaria para la implantación de la propuesta de medición del rendimiento en la plataforma de monitoreo de seguridad tecnológica de CANTV
Plan de respuesta a los riesgos.	En esta sección se elaboró una matriz de riesgos, junto con su plan de contingencia en el que se le dio respuesta a todas y cada una de las posibles incidencias que pudieran influir en la realización del proyecto.
Acuerdos con los stakeholders	Se elaboró un plan para la medición del rendimiento para la plataforma de Monitoreo de Seguridad Tecnológica de CANTV, el cual permitirá la implantación de una aplicación en donde se cotejarán de manera automática los niveles de fallas y disponibilidad de dicha plataforma

Fuente: CANTV (2013).

CAPÍTULO VII. LECCIONES APRENDIDAS

En esta sección se presentan el conjunto de éxitos y errores que se lograron manejar y sortear durante la realización del Trabajo Especial de Grado, los mismos se enumeran a continuación:

Objetivo 01:

En el análisis del estado de arte en la medición del rendimiento de plataformas de seguridad tecnológica, se evaluaron varias tecnologías que apoyaron la problemática planteada, pero no todas se adaptaron a los requerimientos de la plataforma, sin embargo se pudo obtener en una tecnología el cumplimiento de todos los requerimientos.

Objetivo 02

Al evaluar el nivel de disponibilidad actual de la plataforma de monitoreo de seguridad tecnológica de CANTV se lograron determinar las fallas más frecuentes a las que fue sometida la plataforma en los últimos dos meses.

Objetivo 03

Al proponer una aplicación informática para detectar y alertar las fallas dentro de la plataforma de monitoreo de seguridad tecnológica de CANTV se encontró que la más idónea fue la herramienta Nagios.

Objetivo 04

El plan para la medición de la disponibilidad de los equipos y servicios de la plataforma de monitoreo de seguridad tecnológica, se llevó a cabo por medio de la elaboración del plan de ejecución del proyecto en el que se contemplaron planes para la gestión del tiempo, recursos humanos, alcance, costos y riesgos.

CAPÍTULO VIII. CONCLUSIONES Y RECOMENDACIONES

8.1 Conclusiones.

A continuación se presentan las conclusiones a las que se llegó en el desarrollo del presente proyecto:

- Con el desarrollo del Trabajo Especial de Grado, se lograron entender los niveles más altos de desarrollo en tecnologías empleadas para la medición de rendimiento en plataformas de monitoreo de Seguridad Tecnológica, a través del análisis de los estados del arte.

- Se logró medir y evaluar el nivel de disponibilidad actual de la plataforma de monitoreo de seguridad tecnológica de CANTV.

- Se propuso una aplicación informática que permitirá detectar y alertar automáticamente y de manera oportuna las fallas dentro de la plataforma de monitoreo de seguridad tecnológica de CANTV.

- Se logró el diseño de un plan para la medición de la disponibilidad de los equipos y servicios de la plataforma de monitoreo de seguridad tecnológica, que permitirá el análisis y agilización del proceso de detección y corrección de fallas en la plataforma de monitoreo de Seguridad Tecnológica de CANTV.

- Se realizó una investigación documental y de carácter descriptivo para lograr a cabalidad los objetivos planteados inicialmente.

- Al llevar a cabo la presente investigación se logró identificar la importancia que tiene para la productividad de CANTV el correcto mantenimiento de la plataforma de monitoreo de seguridad Tecnológica, ya que dicha plataforma

aporta un valor agregado a la seguridad de la empresa, disminuyendo los riesgos en la operatividad.

8.2 Recomendaciones

- Debe existir un compromiso por parte del personal involucrado de dar continuidad al plan propuesto para mejorar los niveles de disponibilidad.
- Se recomienda seguir con la instalación de hardware y software necesarios para la medición del rendimiento en la plataforma de monitoreo de Seguridad Tecnológica de CANTV.
- Efectuar el mantenimiento preventivo y correctivo de la plataforma de manera periódica para evitar fallas en la operación.
- Contar al personal adecuado para dar continuidad y seguimiento del plan propuesto.

REFERENCIAS BIBLIOGRÁFICAS.

Arias, F (2004). *El Proyecto de Investigación. Introducción a la Metodología científica*. Venezuela, Editorial: Episteme.

Ballestrini, M (2002). *Como se Elabora el Proyecto de Investigación. Venezuela. Editorial: BL Consultores Asociados.*

Burtescu (2009). *Implementación de seguridad en almacenes de datos.*

Cacti. *The complete rrdtool-based graphing solution*. http://www.cacti.net/what_is_cacti.php. [Consulta: 2013, Enero 10].

Chamoun, Y (2002). *Administración Profesional de Proyectos La Guía. Editorial: Mc Graw Hill.*

Cisco. *Cisco IOS NetFlow. http://www.cisco.com/en/US/products/ps6601/products_ios_protocol_group_home.htm.* [Consulta: 2012, Noviembre 8].

EC-COUNCIL A (2012). *Certified Ethical Hacker Version 7*. Estados Unidos de Norteamérica.

EC-COUNCIL B (2012). *Certified Incident Handler Version 1*. Estados Unidos de Norteamérica.

Giralt, Vidal y Pérez (2011). *Seguridad de los documentos de archivo: estudio de caso del Archivo del Ayuntamiento de Barcelona*.

Hurtado, J (2008). *El proyecto de Investigación*. Caracas. Quirón-Sypal

IAAP (2007). Que es la Metodología FEL. Disponible http://iaap.wordpress.com/2007/06/26/%C2%BFque-es-la-metodologia-fel/ [Consulta: 2012, Junio 17].

Khodadadi, Tutuncu y Zangari (2006). *Optimización y la gestión cuantitativa de inversiones.*

Mcnab, C *(2008). Seguridad de Redes.* Madrid. Ediciones Anaya Multimedia *S.A.*

Monrroy (2011). *Diseño del plan de ejecución del proyecto de actualización de la plataforma tecnológica centralizada de Banesco Banco Universal.* Universidad Católica Andrés Bello. Caracas, Venezuela.

Nagios. *Nagios Is The Industry Standard In IT Infrastructure Monitoring.* http://www.nagios.org/. [Consulta: 2013, Enero 5].

Ntop. *Ntop Knowledge Base.* http://www.ntop.org/support/kb. [Consulta: 2012, Diciembre 6].

Parra, M. (2012). *Diseño de una metodología para la gestión del proceso de la demanda estratégica de tecnología de información (IT), caso de estudio: Gerencia Corporativa de IT del Grupo Mistral*. Universidad Católica Andrés Bello. Caracas, Venezuela.

PMI (2006). *Practice Standard for Work Breakdown Structure*. Estados Unidos.

PMI (2008). *Guía de los fundamentos para la dirección de proyectos (guía del PMBOK)*, Estados Unidos. Editorial Global Standard.

Pressman, R (2002). *Ingeniería del Software, un enfoque práctico*. España. Editorial: Mc Graw Hill.

Safeprod (2006). *Factory Acceptance Test Guideline.*

SPC Consulting Group. *Análisis del Modo y Efecto de Falla.* http://spcgroup.com.mx/amef/. [Consulta: 2013, Julio 6].

Sneha (2011). *Un estudio literario sobre los aspectos de seguridad de los almacenes de datos*.

Tasmania Inter Agency Policy and Projects Unit (2008). *Project Execution Plan Template & Guide.*

Tasmania Inter Agency Policy and Projects Unit (2008). *Project Risk Register Template & Guide.*

Viryanet (2013). *Site Acceptance Testing* http://www.viryanet.com/services/implementation/site-acceptance-testing. . [Consulta: 2013, Julio 6].